Dd Wrt Setup Guide

Introduces Linux concepts to programmers who are familiar with other operating systems such as Windows XP Provides comprehensive coverage of the Pentium assembly language

Now in its third Canadian edition, the market-leading Social Research Methods is an engaging and straightforward introduction to conducting quantitative and qualitative research in the social sciences. Building on the success of previous editions, the authors deftly guide students through allaspects of the research process, while providing useful tips on how to effectively collect, analyze, and interpret data, and disseminate those findings to others. With a brand new chapter on ethics and extensive updates throughout, this new edition continues to be an essential guide to theconceptual foundations, methodological approaches, and practical

This book was first published in 2015. Since then, the Wi-Fi technology has evolved tremendously. This 2020 edition has important updates about security. Once hackers take control of your Wi-Fi router, they can attack connected devices such as phones, laptops, computers! Fortunately, it is easy to harden the defense of your home network. There are important steps you should take in order to protect your connected devices. An exhaustive catalog of the latest home security devices has been updated in this 2020 edition. Why would you spend a lot of money to have a home security system installed when you can do it yourself! A chapter about health risks has also been added. Are EMF radiations safe? We regularly post updates on our site http://mediastimulus.com such as security alerts and the latest in Wi-Fi technology. Your feedback is always welcome http://mediastimulus.com/contact/

This soup-to-nuts collection of recipes covers everything you need to know to perform your job as a Linux network administrator, whether you're new to the job or have years of experience. With Linux Networking Cookbook, you'll dive straight into the gnarly hands-on work of building and maintaining a computer network. Running a network doesn't mean you have all the answers. Networking is a complex subject with reams of reference material that's difficult to keep straight, much less remember. If you want a book that lays out the steps for specific tasks, that clearly explains the commands and configurations, and does not tax your patience with endless ramblings and meanderings into theory and obscure RFCs, this is the book for you. You will find recipes for: Building a gateway, firewall, and wireless access point on a Linux network Building a VoIP server with Asterisk Secure remote administration with SSH Building secure VPNs with OpenVPN, and a Linux PPTP VPN server Single sign-on with Samba for mixed Linux/Windows LANs Centralized network directory with OpenLDAP Network monitoring with Nagios or MRTG Getting acquainted with IPv6 Setting up hands-free networks installations of new systems Linux system administration via serial console And a lot more. Each recipe includes a clear, hands-on solution with tested code, plus a discussion on why it works. When you need to solve a network problem without delay, and don't have the time or patience to comb through reference books or the Web for answers, Linux Networking Cookbook gives you exactly what you need.

Essential Skills for a Successful IT Career Written by CompTIA certification and training expert Mike Meyers, this instructive, full-color guide will help you pass CompTIA Network+ exam N10-005 and become an expert networking technician. Mike Meyers' CompTIA Network+ Guide to Managing and Troubleshooting Networks, Third Edition is completely up to date with the new CompTIA Network+ standards. From McGraw-Hill—a Gold-Level CompTIA Authorized Partner, this book offers Authorized CompTIA Approved Quality Content. Inside, you'll find helpful on-the-job tips, end-of-chapter practice questions, and hundreds of photographs and illustrations. End-of-chapter solutions and answers are only available to instructors and do not appear in the book. Learn how to: Build a network with the OSI and TCP/IP models Configure network hardware, topologies, and cabling Connect multiple Ethernet components Install and configure routers and switches Work with TCP/IP applications and network protocols Configure IPv6 routing protocols Set up clients and servers for remote access Configure wireless networks Secure networks with firewalls, NAT, port filtering, packet filtering, and other methods Implement virtualization Build a SOHO network Manage and troubleshoot networks The CD-ROM features: Two full practice exams Video presentation from Mike Meyers One hour of video training A new collection of Mike's favorite shareware and freeware networking tools and utilities Adobe Digital Editions free eBook download (subject to Adobe's system requirements) Each chapter includes: Learning objectives Photographs and illustrations Real-world examples Try This! and Cross Check exercises Key terms highlighted Tech Tips, Notes, and Warnings Exam Tips End-of-chapter quizzes and lab projects

Discusses how to configure and manage Microsoft Server 2012's expanded capabilities, covering data management, user permissions, networking tools, and data integrity.

Complete Administrator's User Guide to daloRADIUS Platform.daloRADIUS is an advanced RADIUS web platform aimed at managing hotspots and general-purpose ISP deployments. It features user management, graphical reporting, accounting, and integration with GoogleMaps for geo-locating. daloRADIUS integrates with FreeRADIUS's database to provide centralized management and control for RADIUS deployments.Those who would find daloRADIUS to be of use are most notably RADIUS operators and administrators, network and systems administrators, integration engineers and NOC departments. Companies or individuals running hotspot captive portals or remote access technologies such as VPNs are likely to find daloRADIUS a great fit to manage their users database records.

Machinery's Handbook has been the most popular reference work in metalworking, design, engineering and manufacturing facilities, and in technical schools and colleges throughout the world for nearly 100 years. It is universally acknowledged as an extraordinarily authoritative, comprehensive, and practical tool, providing its users with the most fundamental and essential aspects of sophisticated manufacturing practice. The 29th edition of the "Bible of the Metalworking Industries" contains major revisions of existing content, as well as new material on a variety of topics. It is the essential reference for Mechanical, Manufacturing, and Industrial Engineers, Designers, Draftsmen, Toolmakers, Machinists, Engineering and Technology Students, and the serious Home Hobbyist. New to this edition ? micromachining, expanded material on calculation of hole coordinates, an introduction to metrology, further contributions to the sheet metal and presses section, shaft alignment, taps and tapping, helical coil screw thread inserts, solid geometry, distinguishing between bolts and screws, statistics, calculating thread dimensions, keys and keyways, miniature screws, metric screw threads, and fluid mechanics. Numerous major sections have been extensively reworked and renovated throughout, including Mathematics, Mechanics and Strength of Materials, Properties of Materials, Dimensioning, Gaging and Measuring, Machining Operations, Manufacturing Process, Fasteners, Threads and Threading, and Machine Elements. The metric content has been greatly expanded. Throughout the book, wherever practical, metric units are shown adjacent to the U.S. customary units in the text. Many formulas are now presented with equivalent metric expressions, and additional metric examples have been added. The detailed tables of contents located at the beginning of each section have been expanded and fine-tuned to make finding topics easier and faster. The entire text of this edition, including all the tables and equations, has been reset, and a great many of the figures have been redrawn. The page count has increased by nearly 100 pages, to 2,800 pages. Updated Standards.

Social Research Methods
Building Virtual Machine Labs
IBM Tivoli Netcool/OMNIbus V7.2 Implementation
Ad-Hoc, Mobile and Wireless Networks
Wireless Networking in the Developing World
The Water Footprint Assessment Manual
PC Magazine
The Independent Guide to IBM-standard Personal Computing
9th International Conference, ADHOC-NOW 2010, Edmonton, AB, Canada, August 20-22, 2010, Proceedings
R Cookbook
Guide to Assembly Language Programming in Linux
The .NET Developer's Guide to Directory Services Programming
Machine Learning

“If you have any interest in writing .NET programs using Active Directory or ADAM, this is the book you want to read.” —Joe Richards, Microsoft MVP, directory services Identity and Access Management are rapidly gaining importance as key areas of practice in the IT industry, and directory services provide the fundamental building blocks that enable them. For enterprise developers struggling to build directory-enabled .NET applications, The .NET Developer’s Guide to Directory Services Programming will come as a welcome aid. Microsoft MVPs Joe Kaplan and Ryan Dunn have written a practical introduction to programming directory services, using both versions 1.1 and 2.0 of the .NET Framework. The extensive examples in the book are in C#; a companion Web site includes both C# and Visual Basic source code and examples. Readers will Learn to create, rename, update, and delete objects in Active Directory and ADAM Learn to bind to and search directories effectively and efficiently Learn to read and write attributes of all types in the directory Learn to use directory services within ASP.NET applications Get concrete examples of common programming tasks such as managing Active Directory and ADAM users and groups, and performing authentication Experienced .NET developers—those building enterprise applications or simply interested in learning about directory services—will find that The .NET Developer’s Guide to Directory Services Programming unravels the complexities and helps them to avoid the common pitfalls that developers face.

Dive into the world of advanced network penetration tests to survey and attack wireless networks using your Android device and zANTI2 About This Book Understand the basics of wireless penetration testing and its importance Learn the techniques to perform penetration testing on your wireless networks, such as scanning, detecting vulnerabilities in your victim, and then attacking This simple and intriguing guide takes a step-by-step approach that will help you get to grips with network pentesting using just your Android device and zANTI2 Who This Book Is For The book is intended for those who want to know more about network penetration tests and have no prior experience, as well as for those who are experienced in network systems and are curious to discover more about this topic. Since zANTI2 features an extremely intuitive and easy to control interface, it doesn't require any special skills. What You Will Learn Understand the importance of penetration testing throughout systems Take a run through zANTI2's interface and understand the requirements to the app Perform advanced scanning/network mapping and discover the various types of scans used on a target Discover and remotely connect to open ports on a target, thereby accessing a target's files and folders remotely Detect vulnerabilities on a target, learn how to remotely exploit them, and discover ways to protect your self from these exploits Understand what an MITM attack is and how it works, and apply this knowledge to perform attacks on network targets Learn to hijack sessions, identify victim's passwords, replace images on websites, inject scripts, and more Use this knowledge to protect yourself from all of the attacks you will study In Detail A penetration test is one of the most important methods to secure a network or any individual machine. Having knowledge of these methods can enable a user to protect himself/herself from any kinds of attacks. Penetration tests can also be used to discover flaws or loop holes in one's security system, which if not fixed, can be exploited by an unwanted entity. This book starts off with an introduction to what penetration testing is, and how it can be performed on Android using zANTI2. Once you are aware of the basics, we move on to teach you the different types of scans that can be performed to search for targets. You will then learn how to connect to open ports and intrude into an unsecured computer. From here you will explore vulnerabilities and their usage, including ShellShock and SSL Poodle vulnerability. When connected to an open network, a user is susceptible to password and session hijacking, and a number of other cyber attacks. The book therefore ends with one of the main aspects of cyber security: the Man in the Middle attack. You will get to know everything about the MITM attack, how it works, and how one can be protected against it. Style and approach The book follows a step-by-step approach with each of the parts explained in an easy-to-follow style. Most of the methods showcased can be tried out immediately on almost any network.

Covers the most important and common configuration scenarios and features which will put you on track to start implementing ASA firewalls right away.

Discover over 90 practical and exciting recipes that leverage the power of OpenVPN 2.4 to help you obtain a reliable and secure VPN About This Book Master the skills of configuring, managing, and securing your VPN using the latest OpenVPN Gain expertise in establishing IPv6 connections and understand PolarSSL using the latest version of OpenVPN This book contains enticing recipes about OpenVPN functionalities that cater to mission critical applications Who This Book Is For This book is for system administrators who have a basic knowledge of OpenVPN and are eagerly waiting to build, secure, and manage VPNs using the latest version. This book assumes some prior knowledge of TCP/IP networking and OpenVPN and you must have network administration skills to get the most out of this book. What You Will Learn Determine the best type of OpenVPN setup for your networking needs Get to grips with the encryption, authentication, and certifications features of OpenSSL. Integrate an OpenVPN server into the local IT infrastructure with the scripting features of OpenVPN Ease the integration of Windows clients into the VPN using Windows-specific client-side configuration Understand the authentication plugins for PAM and LDAP Get to know the difference between TUN-style and TAP-style networks and when to use what Troubleshoot your VPN setup Establish a connection via IPv6 along with demonstrations In Detail OpenVPN provides an extensible VPN framework that has been designed to ease site-specific customization, such as providing the capability to distribute a customized installation package to clients, and supporting alternative authentication methods via OpenVPN's plugin module interface. This book provides you with many different recipes to help you set up, monitor, and troubleshoot an OpenVPN network. You will learn to configure a scalable, load-balanced VPN server farm that can handle thousands of dynamic connections from incoming VPN clients. You will also get to grips with the encryption, authentication, security, extensibility, and certifications features of OpenSSL. You will also get an understanding of IPv6 support and will get a demonstration of how to establish a connection via IPv64. This book will explore all the advanced features of OpenVPN and even some undocumented options, covering all the common network setups such as point-to-point networks and multi-client TUN-style and TAP-style networks. Finally, you will learn to manage, secure, and troubleshoot your virtual private networks using OpenVPN 2.4. Style and approach This practical, recipe-based book covers the core functionalities of OpenVPN ending with troubleshooting, performance tuning and making the readers inquisitive about the advanced features.

Take a practioner’s approach in analyzing the Internet of Things (IoT) devices and the security issues facing an IoT architecture. You’ll review the architecture's central components, from hardware communication interfaces, such as UARTand SPI, to radio protocols, such as BLE or ZigBee. You'll also learn to assess a device physically by opening it, looking at the PCB, and identifying the chipsets and interfaces. You'll then use that information to gain entry to the device or to perform other actions, such as dumping encryption keys and firmware. As the IoT rises to one of the most popular tech trends, manufactures need to take necessary steps to secure devices and protect them from attackers. The IoT Hacker's Handbook breaks down the Internet of Things, exploits it, and reveals how these devices can be built securely. What You’ll Learn Perform a threat model of a real-world IoT device and locate all possible attacker entry points Use reverse engineering of firmware binaries to identify security issues Analyze,assess, and identify security issues in exploited ARM and MIPS based binaries Sniff, capture, and exploit radio communication protocols, such as Bluetooth Low Energy (BLE), and ZigBee Who This Book is For Those interested in learning about IoT security, such as pentesters working in different domains, embedded device developers, or IT people wanting to move to an Internet of Things security role.

Best-practice QoS designs for protecting voice, video, and critical data while mitigating network denial-of-service attacks Understand the service-level requirements of voice, video, and data applications Examine strategic QoS best practices, including Scavenger-class QoS tactics for DoS/worm mitigation Learn about QoS tools and the various interdependencies and caveats of these tools that can impact design considerations Learn how to protect voice, video, and data traffic using various QoS mechanisms Evaluate design recommendations for protecting voice, video, and multiple classes of data while mitigating DoS/worm attacks for the following network infrastructure architectures: campus LAN, private WAN, MPLS VPN, and IPSec VPN Quality of Service (QoS) has already proven itself as the enabling technology for the convergence of voice, video, and data networks. As business needs evolve, so do the demands for QoS. The need to protect critical applications via QoS mechanisms in business networks has escalated over the past few years, primarily due to the increased frequency and sophistication of denial-of-service (DoS) and worm attacks. End-to-End QoS Network Design is a detailed handbook for planning and deploying QoS solutions to address current business needs. This book goes beyond discussing available QoS technologies and considers detailed design examples that illustrate where, when, and how to deploy various QoS features to provide validated and tested solutions for voice, video, and critical data over the LAN, WAN, and VPN. The book starts with a brief background of network infrastructure evolution and the subsequent need for QoS. It then goes on to cover the various QoS features and tools currently available and comments on their evolution and direction. The QoS requirements of voice, interactive and streaming video, and multiple classes of data applications are presented, along with an overview of the nature and effects of various types of DoS and worm attacks. QoS best-practice design principles are introduced to show how QoS mechanisms can be strategically deployed end-to-end to address application requirements while mitigating network attacks. The next section focuses on how these strategic design principles are applied to campus LAN QoS design. Considerations and detailed design recommendations specific to the access, distribution, and core layers of an enterprise campus network are presented. Private WAN QoS design is discussed in the following section, where WAN-specific considerations and detailed QoS designs are presented for leased-lines, Frame Relay, ATM, ATM-to-FR Service Interworking, and ISDN networks. Branch-specific designs include Cisco® SAFE recommendations for using Network-Based Application Recognition (NBAR) for known-worm identification and policing. The final section covers Layer 3 VPN QoS design-for both MPLS and IPSec VPNs. As businesses are migrating to VPNs to meet their wide-area networking needs at lower costs, considerations specific to these topologies are required to be reflected in their customer-edge QoS designs. MPLS VPN QoS design is examined from both the enterprise and service provider's perspectives. Additionally, IPSec VPN QoS designs cover site-to-site and teleworker contexts. Whether you are looking for an introduction to QoS principles and practices or a QoS planning and deployment guide, this book provides you with the expert advice you need to design and implement comprehensive QoS solutions.

The problem of privacy-preserving data analysis has a long history spanning multiple disciplines. As electronic data about individuals becomes increasingly detailed, and as technology enables ever more powerful collection and curation of these data, the need increases for a robust, meaningful, and mathematically rigorous definition of privacy, together with a computationally rich class of algorithms that satisfy this definition. Differential Privacy is such a definition. The Algorithmic Foundations of Differential Privacy starts out by motivating and discussing the meaning of differential privacy, and proceeds to explore the fundamental techniques for achieving differential privacy, and the application of these techniques in creative combinations, using the query-release problem as an ongoing example. A key point is that, by rethinking the computational goal, one can often obtain far better results than would be achieved by methodically replacing each step of a non-private computation with a differentially private implementation. Despite some powerful computational results, there are still fundamental limitations. Virtually all the algorithms discussed herein maintain differential privacy against adversaries of arbitrary computational power -- certain algorithms are computationally intensive, others are efficient. Computational complexity for the adversary and the algorithm are both discussed. The monograph then turns from fundamentals to applications other than query-release, discussing differentially private methods for mechanism design and machine learning. The vast majority of the literature on differentially private algorithms considers a single, static, database that is subject to many analyses. Differential privacy in other models, including distributed databases and computations on data streams, is discussed. The Algorithmic Foundations of Differential Privacy is meant as a thorough introduction to the problems and techniques of differential privacy, and is an invaluable reference for anyone with an interest in the topic.

*Penetration testers simulate cyber attacks to find security weaknesses in networks, operating systems, and applications. Information security experts worldwide use penetration techniques to evaluate enterprise defenses. In Penetration Testing, security expert, researcher, and trainer Georgia Weidman introduces you to the core skills and techniques that every pentester needs. Using a virtual machine–based lab that includes Kali Linux and vulnerable operating systems, you’ll run through a series of practical lessons with tools like Wireshark, Nmap, and Burp Suite. As you follow along with the labs and launch attacks, you’ll experience the key stages of an actual assessment—including information gathering, finding exploitable vulnerabilities, gaining access to systems, post exploitation, and more. Learn how to: * Crack passwords and wireless network keys with brute-forcing and wordlists * Test web applications for vulnerabilities * Use the Metasploit Framework to launch exploits and write your own Metasploit modules * Automate social-engineering attacks * Bypass antivirus software * Turn access to one machine into total control of the enterprise in the post exploitation phase You’ll even explore writing your own exploits. Then it’s on to mobile hacking—Weidman’s particular area of research—with her tool, the Smartphone Pentest Framework. With its collection of hands-on lessons that cover key tools and strategies, Penetration Testing is the introduction that every aspiring hacker needs.*

Windows Server 2012: Up and Running
WiFi User Guide 2020 Edition
Linksys WRT54G Ultimate Hacking
Step-by-Step Practical Configuration Guide Using the Cli for Asa V8.x and V9.x
The GNU Source-level Debugger
A Hands-On Guide
Machinery's Handbook
Mathematics Into Type
IMS Performance and Tuning Guide
An Internet Service Model Perspective
Technical, Commercial and Regulatory Challenges of QoS
Linux Networking Cookbook
The Discrete Charm of the Machine

This IBM® Redbooks® publication discusses in detail the facilities of DB2® for z/OS®, which allow complete monitoring of a DB2 environment. It focuses on the use of the DB2 instrumentation facility component (IFC) to provide monitoring of DB2 data and events and includes suggestions for related tuning. We discuss the collection of statistics for the verification of performance of the various components of the DB2 system and accounting for tracking the behavior of the applications. We have intentionally omitted considerations for query optimization; they are worth a separate document. Use this book to activate the right traces to help you monitor the performance of your DB2 system and to tune the various aspects of subsystem and application performance.

This edition, updated by Arlene O'Sean and Antoinette Schleyer of the American Mathematical Society, brings Ms. Swanson's work up to date, reflecting the more technical reality of publishing today. While it includes information for copy editors, proofreaders, and production staff to do a thorough, traditional copyediting and proofreading of a manuscript and proof copy, it is increasingly more useful to authors, who have become intricately involved with the typesetting of their manuscripts.

This book will teach the reader how to make the most of their WRT54G series hardware. These handy little inexpensive devices can be configured for a near endless amount of networking tasks. The reader will learn about the WRT54G's hardware components, the different third-party firmware available and the differences between them, choosing the firmware that is right for you, and how to install different third-party firmware distributions. Never before has this hardware been documented in this amount of detail, which includes a wide-array of photographs and complete listing of all WRT54G models currently available, including the WRTSL54GS. Once this foundation is laid, the reader will learn how to implement functionality on the WRT54G for fun projects, penetration testing, various network tasks, wireless spectrum analysis, and more! This title features never before seen hacks using the WRT54G. For those who want to make the most out of their WRT54G you can learn how to port code and develop your own software for the OpenWRT operating system. Never before seen and documented hacks, including wireless spectrum analysis Most comprehensive source for documentation on how to take advantage of advanced features on the inexpensive wrt54g platform Full coverage on embedded device development using the WRT54G and OpenWRT

A comprehensive introduction to machine learning that uses probabilistic models and inference as a unifying approach. Today's Web-enabled deluge of electronic data calls for automated methods of data analysis. Machine learning provides these, developing methods that can automatically detect patterns in data and then use the uncovered patterns to predict future data. This textbook offers a comprehensive and self-contained introduction to the field of machine learning, based on a unified, probabilistic approach. The coverage combines breadth and depth, offering necessary background material on such topics as probability, optimization, and linear algebra as well as discussion of recent developments in the field, including conditional random fields, L1 regularization, and deep learning. The book is written in an informal, accessible style, complete with pseudo-code for the most important algorithms. All topics are copiously illustrated with color images and worked examples drawn from such application domains as biology, text processing, computer vision, and robotics. Rather than providing a cookbook of different heuristic methods, the book stresses a principled model-based approach, often using the language of graphical models to specify models in a concise and intuitive way. Almost all the models described have been implemented in a MATLAB software package—PMTK (probabilistic modeling toolkit)—that is freely available online. The book is suitable for upper-level undergraduates with an introductory-level college math background and beginning graduate students.

WiFi User Guide 2020 EditionWebolicus

Virtualization is a skill that most IT or security pros take for granted. The sheer number of choices and requirements can be a daunting challenge to face for beginners and veterans alike. With this book, you'll learn how to build a robust, customizable virtual environments suitable for both a personal home lab, as well as a dedicated office training environment. You will learn how to: - Understand the mechanics of virtualization and how they influence the design of your lab - Build an extensive baseline lab environment on any one of five commonly used hypervisors (VMware vSphere Hypervisor, VMware Fusion, VMware Workstation, Oracle Virtualbox, and Microsoft Client Hyper-V) - Harden your lab environment against VM escapes and other security threats - Configure the pfSense firewall distribution to provide security, segmentation, and network services to your virtual lab - Deploy either Snort or Suricata open-source IDS platforms in IPS mode to further enhance the flexibility, segmentation and security of your lab network - Deploy Splunk as a log management solution for your lab - Reconfigure the provided baseline lab environment to better suit your individual needs Easy to follow steps and illustrations provide detailed, comprehensive guidance as you build your custom-tailored lab. Both IT and security professionals need practice environments to better hone their craft. Learn how to build and maintain your own with Building Flexible Virtual Machine Labs

With more than 200 practical recipes, this book helps you perform data analysis with R quickly and efficiently. The R language provides everything you need to do statistical work, but its structure can be difficult to master. This collection of concise, task-oriented recipes makes you productive with R immediately, with solutions ranging from basic tasks to input and output, general statistics, graphics, and linear regression. Each recipe addresses a specific problem, with a discussion that explains the solution and offers insight into how it works. If you're a beginner, R Cookbook will help get you started. If you're an experienced data programmer, it will jog your memory and expand your horizons. You'll get the job done faster and learn more about R in the process. Create vectors, handle variables, and perform other basic functions Input and output data Tackle data structures such as matrices, lists, factors, and data frames Work with probability, probability distributions, and random variables Calculate statistics and confidence intervals, and perform statistical tests Create a variety of graphic displays Build statistical models with linear regressions and analysis of variance (ANOVA) Explore advanced statistical techniques, such as finding clusters in your data "Wonderfully readable, R Cookbook serves not only as a solutions manual of sorts, but as a truly enjoyable way to explore the R language—one practical example at a time."—Jeffrey Ryan, software consultant and R package author

This open access book gives a complete and comprehensive introduction to the fields of medical imaging systems, as designed for a broad range of applications. The authors of the book first explain the foundations of system theory and image processing, before highlighting several modalities in a dedicated chapter. The initial focus is on modalities that are closely related to traditional camera systems such as endoscopy and microscopy. This is followed by more complex image formation processes: magnetic resonance imaging, X-ray projection imaging, computed tomography, X-ray phase-contrast imaging, nuclear imaging, ultrasound, and optical coherence tomography.

Understanding Linux Network Internals
A Reference Book for the Mechanical Engineer, Designer, Manufacturing Engineer, Draftsman, Toolmaker, and Machinist
Why the World Became Digital
The IoT Hacker's Handbook
A Practical Guide to Planning and Building
Cisco IOS Cookbook
Penetration Testing
Proven Recipes for Data Analysis, Statistics, and Graphics
Effective Communication of Scientific Information
A Probabilistic Perspective
Medical Imaging Systems
OpenVPN Cookbook
Wireless Home Networking For Dummies

Rely on this practical, end-to-end guide on cyber safety and online security written expressly for a non-technical audience. You will have just what you need to protect yourself—step by step, without judgment, and with as little jargon as possible. Just how secure is your computer right now? You probably don't really know. Computers and the Internet have revolutionized the modern world, but if you're like most people, you have no clue how these things work and don't know the real threats. Protecting your computer is like defending a medieval castle. While moats, walls, drawbridges, and castle guards can be effective, you'd go broke trying to build something dragon-proof. This book is not about protecting yourself from a targeted attack by the NSA; it's about armoring yourself against common hackers and mass surveillance. There are dozens of no-brainer things we all should be doing to protect our computers and safeguard our data—just like wearing a seat belt, installing smoke alarms, and putting on sunscreen. Author Carey Parker has structured this book to give you maximum benefit with minimum effort. If you just want to know what to do, every chapter has a complete checklist with step-by-step instructions and pictures. The book contains more than 150 tips to make you and your family safer. It includes: Added steps for Windows 10 (Spring 2018) and Mac OS X High Sierra Expanded coverage on mobile device safety Expanded coverage on safety for kids online More than 150 tips with complete step-by-step instructions and pictures What You'll Learn Solve your password problems once and for all Browse the web safely and with confidence Block online tracking and dangerous ads Choose the right antivirus software for you Send files and messages securely Set up secure home networking Conduct secure shopping and banking online Lock down social media accounts Create automated backups of all your devices Manage your home computers Use your smartphone and tablet safely Safeguard your kids online And more! Who This Book Is For Those who use computers and mobile devices, but don't really know (or frankly care) how they work. This book is for people who just want to know what they need to do to protect themselves—step by step, without judgment, and with as little jargon as possible.

Wireless home networks are better than ever! The emergence of new industry standards has made them easier, more convenient, less expensive to own and operate. Still, you need to know what to look for (and look out for), and the expert guidance you'll find in Wireless Home Networks For Dummies, 3rd Edition helps you ensure that your wire-free life is also a hassle-free life! This user-friendly, plain-English guide delivers all of the tips, tricks, and knowledge you need to plan your wireless home network, evaluate and select the equipment that will work best for you, install and configure your wireless network, and much more. You'll find out how to share your Internet connection over your network, as well as files, printers, and other peripherals. And, you'll learn how to avoid the "gotchas" that can creep in when you least expect them. Discover how to: Choose the right networking equipment Install and configure your wireless network Integrate Bluetooth into your network Work with servers, gateways, routers, and switches Connect audiovisual equipment to your wireless network Play wireless, multiuser computer games Establish and maintain your network's security Troubleshoot networking problems Improve network performance Understand 802.11n Whether you're working with Windows PCs, Mac OS X machines, or both Wireless Home Networking For Dummies, 3rd Edition, makes it fast and easy to get your wireless network up and running—and keep it that way!

Thoroughly revised and expanded, this second edition adds sections on MPLS, Security, IPv6, and IP Mobility and presents solutions to the most common configuration problems.

The genesis of the digital idea and why it transformed civilization A few short decades ago, we were informed by the smooth signals of analog television and radio; we communicated using our analog telephones; and we even computed with analog computers. Today our world is digital, built with zeros and ones. Why did this revolution occur? The Discrete Charm of the Machine explains, in an engaging and accessible manner, the varied physical and logical reasons behind this radical transformation. The spark of individual genius shines through this story of innovation: the stored program of Jacquard's loom; Charles Babbage's logical branching; Alan Turing's brilliant abstraction of the discrete machine; Harry Nyquist's foundation for digital signal processing; Claude Shannon's breakthrough insights into the meaning of information and bandwidth; and Richard Feynman's prescient proposals for nanotechnology and quantum computing. Ken Steiglitz follows the progression of these ideas in the building of our digital world, from the internet and artificial intelligence to the edge of the unknown. Are questions like the famous traveling salesman problem truly beyond the reach of ordinary digital computers? Can quantum computers transcend these barriers? Does a mysterious magical power reside in the analog mechanisms of the brain? Steiglitz concludes by confronting the moral and aesthetic questions raised by the development of artificial intelligence and autonomous robots. The Discrete Charm of the Machine examines why our information technology, the lifeblood of our civilization, became digital, and challenges us to think about where its future trajectory may lead.

If your household harbors more than one computer, you've probably wondered about home networking. Maybe you've gone so far as to start setting up a network and given up in frustration. Well, now you can relax. Home Networking All-In-One Desk Reference For Dummies has come to the rescue! A network will make your life easier, and Home Networking All-In-One Desk Reference For Dummies makes it easier to create one. It shows you how to choose the right hardware, add user accounts, get different operating systems to work together, secure your network, exchange files, add wireless devices, and even use Wi-Fi out in public. Seven individual, self-contained minibooks cover: What a network will do for you, including a low-tech explanation of how it works Choosing a network type that will work best for your needs, and planning what equipment you'll need Installing and configuring your computers and networking gear Upgrading your equipment with the manufacturer's updates The ins and outs of using particular versions of operating systems — Windows, Mac, and Linux — with your network Step-by-step directions on connecting to networks, sharing files and printers, checking connection status, and much more Discovering networking accessories and gadgets to get the most out of your network Finding and using Wi-Fi hotspots, plus setting up your own You'll even find troubleshooting tips to help find and fix common problems. Home Networking All-In-One Desk Reference For Dummies will be your personal network assistant!

Master building and integrating secure private networks using OpenVPN About This Book Discover how to configure and set up a secure OpenVPN Enhance user experience by using multiple authentication methods Delve into better reporting, monitoring, logging, and control with OpenVPN Who This Book Is For If you are familiar with TCP/IP networking and general system administration, then this book is ideal for you. Some knowledge and understanding of core elements and applications related to Virtual Private Networking is assumed. What You Will Learn Identify different VPN protocols (IPSec, PPTP, OpenVPN) Build your own PKI and manage certificates Deploy your VPN on various devices like PCs, mobile phones, tablets, and more Differentiate between the routed and bridged network Enhance your VPN with monitoring and logging Authenticate against third-party databases like LDAP or the Unix password file Troubleshoot an OpenVPN setup that is not performing correctly In Detail Security on the internet is increasingly vital to both businesses and individuals. Encrypting network traffic using Virtual Private Networks is one method to enhance security. The internet, corporate, and "free internet" networks grow more hostile every day. OpenVPN, the most widely used open source VPN package, allows you to create a secure network across these systems, keeping your private data secure. The main advantage of using OpenVPN is its portability, which allows it to be embedded into several systems. This book is an advanced guide that will help you build secure Virtual Private Networks using OpenVPN. You will begin your journey with an exploration of OpenVPN, while discussing its modes of operation, its clients, its secret keys, and their format types. You will explore PKI: its setting up and working, PAM authentication, and MTU troubleshooting. Next, client-server mode is discussed, the most commonly used deployment model, and you will learn about the two modes of operation using "tun" and "tap" devices. The book then progresses to more advanced concepts, such as deployment scenarios in tun devices which will include integration with back-end authentication, and securing your OpenVPN server using iptables, scripting, plugins, and using OpenVPN on mobile devices and networks. Finally, you will discover the strengths and weaknesses of the current OpenVPN implementation, understand the future directions of OpenVPN, and delve into the troubleshooting techniques for OpenVPN. By the end of the book, you will be able to build secure private networks across the internet and hostile networks with confidence. Style and approach An easy-to-follow yet comprehensive guide to building secure Virtual Private Networks using OpenVPN. A progressively complex VPN design is developed with the help of examples. More advanced topics are covered in each chapter, with subjects grouped according to their complexity, as well as their utility.

WithFriendzy: Pre-K Fun Pad, kids can have fun mastering key concepts from anywhere. The convenient format is perfect for the car, waiting rooms, restaurants, and more. Plus, with dozens of colorful, game-based activities covering the alphabet, numbers, colors, shapes, and more, kids will be engaged and interested in learning. And they'll love the colorful sticker sheet!

Technical, Commerical and Regulatory Challenges of QoS provides a comprehensive examination of Internet QoS theory, standards, vendor implementation and network deployment from the practitioner's point of view, including extensive discussion of related economic and regulatory issues. Written in a technology-light way so that a variety of professionals and researchers in the information and networking industries can easily grasp the material. Includes case studies based on real-world experiences from industry. The author starts by discussing the economic, regulatory and technical challenges of the existing QoS model. Key coverage includes defining a clear business model for selling and buying QoS in relation to current and future direction of government regulation and QoS interoperability (or lack thereof) between carriers and networking devices. The author then demonstrates how to improve the current QoS model to create a clear selling point, less regulation uncertainty, and higher chance of deployment success. This includes discussion of QoS re-packaging to end-users; economic and regulatory benefits of the re-packaging; and the overall benefits of an improved technical approach. Finally, the author discusses the future evolution of QoS from an Internet philosophy perspective and lets the reader draw the conclusions. This book is the first QoS book to provide in depth coverage on the commercial and regulatory aspects of QoS, in addition to the technical aspect. From that, readers can grasp the commercial and regulatory issues of QoS and their implications on the overall QoS business model. This book is also the first QoS book to provide case studies of real world QoS deployments, contributed by the people who did the actual deployments. From that, readers can grasp the practical issues of QoS in real world. This book is also the first QoS book to cover both wireline QoS and wireless QoS. Readers can grasp the QoS issues in the wireless world. The book was reviewed and endorsed by a long list of prominent industrial and academic figures. Discusses QoS technology in relation to economic and regulatory issues Includes case studies based on real-world examples from industry practitioners Provides unique insight into how to improve the current QoS model to create a clear selling point, less regulatory uncertainty, and higher chance of deployment success

Debugging with GDB
From Asterisk to Zebra with Easy-to-Use Recipes
Firewalls Don't Stop Dragons
Mastering OpenVPN
Home Networking All-in-One Desk Reference For Dummies
Setting the Global Standard
End-to-end Qos Network Design
DaloRADIUS User Guide
Learning zANTI2 for Android Pentesting
An Introductory Guide
Subsystem and Transaction Monitoring and Tuning with DB2 11 for z/OS
A Hands-On Introduction to Hacking
A Step-by-Step Guide to Computer Security for Non-Techies

Provides instructions on how to build low-cost telecommunications infrastructure. Topics covered range from basic radio physics and network design to equipment and troubleshooting, a chapter on Voice over IP (VoIP), and a selection of four case studies from networks deployed in Latin America. The text was written and reviewed by a team of experts in the field of long distance wireless networking in urban, rural, and remote areas. Contents: 1) Where to Begin. 2) A Practical Introduction to Radio Physics. 3) Network Design. 4) Antennas & Transmission Lines. 5) Networking Hardware. 6) Security & Monitoring. 7) Solar Power. 8) Building an Outdoor Node. 9) Troubleshooting. 10) Economic Sustainability. 11) Case Studies. See the website for translations, including French, Spanish, Portuguese, Italian, Arabic, and others, and additional case studies, training course material, and related information

First Published in 2011. Routledge is an imprint of Taylor & Francis, an informa company.

In the time since the second edition of The ACS Style Guide was published, the rapid growth of electronic communication has dramatically changed the scientific, technical, and medical (STM) publication world. This dynamic mode of dissemination is enabling scientists, engineers, and medical practitioners all over the world to obtain and transmit information quickly and easily. An essential constant in this changing environment is the requirement that information remain accurate, clear, unambiguous, and ethically sound. This extensive revision of The ACS Style Guide thoroughly examines electronic tools now available to assist STM writers in preparing manuscripts and communicating with publishers. Valuable updates include discussions of markup languages, citation of electronic sources, online submission of manuscripts, and preparation of figures, tables, and structures. In keeping current with the changing environment, this edition also contains references to many resources on the internet. With this wealth of new information, The ACS Style Guide's Third Edition continues its long tradition of providing invaluable insight on ethics in scientific communication, the editorial process, copyright, conventions in chemistry, grammar, punctuation, spelling, and writing style for any STM author, reviewer, or editor. The Third Edition is the definitive source for all information needed to write, review, submit, and edit scholarly and scientific manuscripts.

A Do-It-Yourself Guide To Troubleshooting and Repairing Your EASY, comprehensive technology troubleshooter! PCs, smartphones, tablets, networks, cameras, home theater and more—all in one book! We all use technology—and we all have problems with it. Don't get frustrated... and don't waste money on costly repair or support calls! Solve the problems yourself, with the one guide that makes it easy: The PC and Gadget Help Desk. Using clear pictures, handy "symptom tables," and easy-to-use flowcharts, Mark Edward Soper walks you step-by-step through identifying, solving, and preventinghundreds of today's most aggravating tech problems. Soper covers all your major platforms: iPhones, iPads, Android devices, Windows systems, and more. He even helps you fix the weird problems that happen when you use them together! Regain lost Internet access and fix broken Wi-Fi connections Solve problems with viewing and sharing media or other files Track down power problems wherever they arise Troubleshoot printing problems and print from smartphones or tablets Fix missing video or audio on your HDTV or home theater system Get syncing working right on your Apple or Android device Improve your PC's 3D gaming performance Identify and replace flaky memory chips Prevent overheating that can damage your equipment Solve common problems with digital cameras and DV camcorders Troubleshoot iOS or Android antennas, updates, screens, and connectivity Get FaceTime working right on your iPhone or iPad Troubleshoot eReaders and display your eBooks on additional devices Sensibly decide whether to upgrade, repair, or replace Mark Edward Soper has spent 30 years as an instructor and corporate trainer, helping thousands of people work more happily with personal technology. He is the author of PC Help Desk in a Book, and is the co-author of Leo Laporte's PC Help Desk, as well as more than 25 other books on Windows, digital imaging, networking, the Internet, IT certification, and computer troubleshooting. Soper is a CompTIA A+ Certified computer technician and Microsoft Certified Professional. BONUS ONLINE VIDEOS: Includes access to free, studio-quality how-to videos that make troubleshooting and repair even easier!

Benvenuti describes the relationship between the Internet's TCP/IP implementation and the Linux Kernel so that programmers and advanced administrators can modify and fine-tune their network environment.

This IBM Redbooks publication provides IMS performance monitoring and tuning information. This book differs from previous IMS performance and tuning IBM Redbooks in that there is less emphasis on the internal workings of IMS and more information about why and how certain options can affect the performance of IMS. Most of the information in the previous book IMS Version 7 Performance Monitoring and Tuning Update, SG24-6404, is still valid, and in most cases, continues to be valid in any future versions of IMS. This book is not an update or rewrite but instead attempts to be more of a guide than a reference. As such, the team gathered experiences and data from actual production environments as well as from IBM benchmarks and solicited input from experts in as many areas as possible. You should be able to find valuable new information and perhaps validate things you might have questioned. Hardware and software characteristics are constantly changing, but hopefully the information that you find here provides a basis to help you react to change and to keep your IMS running efficiently. In this book, we introduce methods and tools for monitoring and tuning IMS systems, and in addition to IMS TM and DB system-wide performance considerations, we dedicate separate chapters for application considerations, IMS and DB2 interoperability, the Parallel Sysplex environment, and On Demand considerations.

A Practical Guide to Hacking the Internet of Things
ACS Style Guide
Certification Guide Series
A Do-It-Yourself Guide To Troubleshooting and Repairing
Mike Meyers' CompTIA Network+ Guide to Managing and Troubleshooting Networks, 3rd Edition (Exam N10-005)
The Algorithmic Foundations of Differential Privacy
Cisco Asa Firewall Fundamentals

The PC and Gadget Help Desk