

IP ADDRESS MANAGEMENT



IEEE Press
445 Hoes Lane
Piscataway, NJ 08854

IEEE Press Editorial Board

Lajos Hanzo, *Editor in Chief*

R. Abari	M. El-Hawary	S. Nahavandi
J. Anderson	B. M. Hammerli	W. Reeve
F. Canavero	M. Lanzerotti	T. Samad
T. G. Croda	O. Malik	G. Zobrist

Kenneth Moore, *Director of IEEE Book and Information Services (BIS)*

Technical Reviewers:

Greg Rabil
Paul Vixie

Books in the IEEE Press Series on Network Management

Telecommunications Network Management Into the 21st Century, edited by Thomas Plevyak and Salah Aidarous, 1994

Telecommunications Network Management: Technologies and Implementations, edited by Thomas Plevyak and Salah Aidarous, 1997

Fundamentals of Telecommunications Network Management, by Lakshmi Raman, 1999

Security for Telecommunications Management Network, by Moshe Rozenblit, 2000

Integrated Telecommunications Management Solutions, by Graham Chen and Quinzheng Kong, 2000

Managing IP Networks: Challenges and Opportunities, edited by Thomas Plevyak and the late Salah Aidarous, 2003

Next-Generation Telecommunications Networks, Services, and Management, edited by Thomas Plevyak and Veli Sahin, 2010

Introduction to IP Address Management, by Timothy Rooney, 2010

IP Address Management: Principles and Practices, by Timothy Rooney, 2011

IP ADDRESS MANAGEMENT

Principles and Practice

Timothy Rooney



Thomas Plevyak and
Veli Sahin, *Series Editors*



A JOHN WILEY & SONS, INC., PUBLICATION

Copyright © 2011 by the Institute of Electrical and Electronics Engineers, Inc.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey. All rights reserved

Published simultaneously in Canada

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permission>.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Cataloging-in-Publication Data:

Rooney, Tim.

IP address management : principles and practice / Tim Rooney.

p. cm.

Includes bibliographical references and index.

ISBN 978-0-470-58587-0 (cloth : alk. paper)

1. Internet addresses. 2. Internet domain names. I. Title.

TK5105.8835.R66 2011

004'67'8--dc22

2010010791

Printed in Singapore

oBook ISBN: 978-0-470-88065-4

ePDF ISBN: 978-0-470-88064-7

10 9 8 7 6 5 4 3 2 1

In memory of my father, Patrick Rooney

CONTENTS



Preface	xi
Acknowledgments	xv

PART I IP ADDRESSING

1 THE INTERNET PROTOCOL	3
1.1 Highlights of Internet Protocol History	3
1.2 IP Addressing	7
1.3 Classless Addressing	13
1.4 Special Use Addresses	14
2 INTERNET PROTOCOL VERSION 6 (IPv6)	15
2.1 Introduction	15
2.2 IPv6 Address Allocations	21
2.3 IPv6 Address Autoconfiguration	30
2.4 Neighbor Discovery	30
2.5 Reserved Subnet Anycast Addresses	33
2.6 Required Host IPv6 Addresses	34
3 IP ADDRESS ALLOCATION	35
3.1 Address Allocation Logic	38
3.2 IPv6 Address Allocation	49
3.3 IPAM Worldwide's IPv6 Allocations	53

3.4 Internet Registries	57
3.5 Multihoming and IP Address Space	62
3.6 Block Allocation and IP Address Management	63

PART II DHCP

4 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)	67
4.1 Introduction	67
4.2 DHCP Overview	68
4.3 DHCP Servers and Address Assignmen	75
4.4 DHCP Options	78
4.5 Other Means of Dynamic Address Assignment	89
5 DHCP FOR IPv6 (DHCPv6)	90
5.1 DHCP Comparison: IPv4 Versus IPv6	91
5.2 DHCPv6 Address Assignment	92
5.3 DHCPv6 Prefix Delegation	93
5.4 DHCPv6 Support of Address Autoconfiguration	94
5.5 Device Unique Identifiers	97
5.6 Identity Associations	99
5.7 DHCPv6 Options	99
6 DHCP APPLICATIONS	109
6.1 Multimedia Device Type Specific Configuration	110
6.2 Broadband Subscriber Provisioning	111
6.3 Related Lease Assignment or Limitation Applications	115
6.4 Preboot Execution Environment Clients	115
7 DHCP SERVER DEPLOYMENT STRATEGIES	118
7.1 DHCP Server Platforms	118
7.2 Centralized DHCP Server Deployment	119
7.3 Distributed DHCP Server Deployment	120
7.4 Server Deployment Design Considerations	122
7.5 DHCP Deployment on Edge Devices	125

8	DHCP AND NETWORK ACCESS SECURITY	127
8.1	Network Access Control	127
8.2	Alternative Access Control Approaches	132
8.3	Securing DHCP	137
PART III	DNS	
9	THE DOMAIN NAME SYSTEM (DNS) PROTOCOL	143
9.1	DNS Overview—Domains and Resolution	143
9.2	Name Resolution	145
9.3	Zones and Domains	148
9.4	Resolver Configuration	159
9.5	DNS Message Format	161
10	DNS APPLICATIONS AND RESOURCE RECORDS	176
10.1	Introduction	176
10.2	Name–Address Lookup Applications	178
10.3	Email and Antispam Management	191
10.4	Security Applications	205
10.5	Experimental Name–Address Lookup Records	217
10.6	Resource Record Summary	218
11	DNS SERVER DEPLOYMENT STRATEGIES	223
11.1	General Deployment Guidelines	224
11.2	General Deployment Building Blocks	224
11.3	External–External Category	226
11.4	External–Internal Category	231
11.5	Internal–Internal Category	232
11.6	Internal–External Category	237
11.7	Cross-Role Category	243
11.8	Putting it All Together	253
12	SECURING DNS (PART I)	254
12.1	DNS Vulnerabilities	254
12.2	Mitigation Approaches	258
12.3	Non-DNSSEC Security Records	259

13	SECURING DNS (PART II): DNSSEC	264
13.1	Digital Signatures	265
13.2	DNSSEC Overview	266
13.3	Configuring DNSSEC	268
13.4	The DNSSEC Resolution Process	290
13.5	Key Rollover	297
PART IV IPAM INTEGRATION		
14	IP ADDRESS MANAGEMENT PRACTICES	305
14.1	FCAPS Summary	306
14.2	Common IP Management Tasks	307
14.3	Configuration Management	307
14.4	Fault Management	324
14.5	Accounting Management	334
14.6	Performance Management	338
14.7	Security Management	340
14.8	Disaster Recovery/Business Continuity	340
14.9	ITIL Process Mappings	342
14.10	Conclusion	346
15	IPv6 DEPLOYMENT AND IPv4 COEXISTENCE	347
15.1	Introduction	347
15.2	Dual-Stack Approach	349
15.3	Tunneling Approaches	353
15.4	Translation Approaches	368
15.5	Application Migration	374
15.6	Planning the IPv6 Deployment Process	374
	BIBLIOGRAPHY	383
	GLOSSARY	392
	RFC INDEX	394
	INDEX	408

PREFACE



The practice of IP address management (IPAM) entails the application of network management disciplines to Internet Protocol (IP) address space and associated network services, namely Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS). The linkages among an IP address plan and configurations of DHCP and DNS servers are inseparable. A change of an IP address affects DNS information and perhaps DHCP as well. These services provide the foundation for today's converged services IP networks, which offer ad hoc anytime, anyplace communications.

If end-user devices such as laptops or voice-over IP (VoIP) phones cannot obtain an IP address via DHCP, they will be rendered unproductive and users will call the help desk. Likewise, if DNS is improperly configured, application navigation by name, phone number, or web address will likewise impair productivity and induce help desk calls.

Effective IPAM practice is a key ingredient in an enterprise or service-provider IP network management strategy. As such, IPAM addresses configuration, change control, auditing, reporting, monitoring, trouble resolution, and related functions as applied to the three foundational IPAM technologies

1. **IP Address Subnetting and Tracking (IPv4/IPv6 Addressing):** Maintenance of a cohesive IP address plan that promotes route summarization, maintains accurate IP address inventory, and provides an automated individual IP address assignment and tracking mechanism. This tracking of individual IP address assignments on each subnet includes those assigned by hard-coding, for example, routers or servers, and others assigned dynamically, for example, laptops and VoIP phones.
2. **DHCP:** Automated IP address and parameter assignment relevant to location and device type. This requires tracking address assignments configured on devices and setting aside dynamically allocated address pools. These address pools can be configured on DHCP servers in order to enable devices to request an IP address, and receive a location-relevant address in reply.
3. **DNS:** Lookup or resolution of hostnames, for example, www entries to IP addresses. This third key aspect of IP address management deals with simplifying IP communications for humans through the use of names, not IP addresses, to establish IP communications. After all, the mapped IP addresses must be consistent with the IP address plan.

The technologies comprising these three core functions are discussed in the first three parts of this book. The practice of IPAM in the fourth part* explains their interrelationships and practices for managing them cohesively. Most IP networks are constantly changing, with the daily demands of the business new stores are opened, offices are closed or moved, companies are acquired, and new devices and device types need IP addresses. These and other changes impacting the IP network can have major repercussions on the existing IP address plan. As the number of users and IP addresses increases, along with the number of subnets or sites, the task of tracking and managing IP address allocations, individual assignments, and associated DNS and DHCP server configurations grows in complexity.

The most common method for performing IPAM functions today entails the use of spreadsheets to track IP addresses, and text editors or Microsoft Windows to configure DHCP and DNS services. As such, IPAM concepts will be demonstrated throughout the book using sample spreadsheet data and configuration file examples as applied to a fictitious organization called IPAM Worldwide, Inc. The intent is to link the technology and configuration details to a real-world example.

CONVENTIONS

This book is typeset in 10-point Times Roman font. *Times Italic* font is used for terms introduced for the first time or to provide emphasis.

To differentiate prose from example configuration information within a DHCP or DNS server, for example, the Courier font in the following manner:

`Courier plain` font: Used to denote keywords or literal text within a configuration file or screen.

Courier italic font: Used to denote a parameter name that in practice is substituted for a value reflecting the denoted data element or type.

ORGANIZATION

The book is organized into four parts. The first three parts of the book focuses on each of the three core IPAM aspects, respectively: IP addressing and management, DHCP, and DNS. Part IV then integrates these three core components, describing management techniques and practice.

Part I: IP Addressing. Part I provides a detailed overview of IPv4, IPv6, and IP allocation and subnetting techniques.

Chapter 1: The Internet Protocol. Chapter 1 covers IP (IPv4) from a review of the IP header to classful, classless, and private IP addressing and discusses evolution of Internet

* In actuality, several constituent IPAM practices are discussed in respective technology chapters, though they are summarized in the context of overall practices in Part IV.

Protocol and the development of network address translation and private addressing as key technologies in preserving global IP address space.

Chapter 2: Internet Protocol Version 6 (IPv6). Chapter 2 describes the IPv6 header and IPv6 addressing, including address notation, structure, and current IANA allocations. This includes a detailed discussion of each address allocation by type (i.e., reserved, global unicast, unique local unicast, link local, and multicast). Special use addresses, including the solicited node address and the node information query address are also described. The chapter continues with a discussion of the modified EUI-64 algorithm and address autoconfiguration, then concludes with a discussion of reserved subnet anycast addresses and addresses required of IPv6 hosts.

Chapter 3: IP Address Allocation. Chapter 3 discusses techniques for IP block allocation for IPv4 and IPv6 address spaces. This includes coverage of best-fit hierarchical address allocation logic and examples, as well as sparse and random allocation approaches for IPv6. This chapter also discusses unique local address space as well as the role of Internet Registries. Block allocation is an important function of IP address management and it lays the groundwork for configuration of DHCP and DNS services.

Part II: DHCP. Part II provides an overview of DHCP for IPv4 and IPv6 and covers applications that rely on DHCP, DHCP server deployment strategies and DHCP and relevant network access security.

Chapter 4: Dynamic Host Configuration Protocol. Chapter 4 describes the DHCP protocol, including a discussion of protocol states, message formats, options, and examples. A table of standard option parameters with descriptions of each is provided.

Chapter 5: DHCP for IPv6 (DHCPv6). Chapter 5 covers the DHCPv6 protocol, including a comparison with DHCP(v4), message formats, options, and examples. A table of DHCPv6 option parameters is provided.

Chapter 6: DHCP Applications. Building on the previous two technology-based chapters, Chapter 6 highlights the end-user utility of DHCP in describing key applications that rely on DHCP, including VoIP device provisioning, broadband access provisioning, PXE client initialization, and lease limiting.

Chapter 7: DHCP Server Deployment Strategies. DHCP server deployment considerations are covered in Chapter 7, in terms of trading off server sizing, quantities, and locations. DHCP deployment options regarding distributed versus centralized approaches will be discussed, as will redundant DHCP configurations.

Chapter 8: DHCP and Network Access Security. Chapter 8 covers DHCP security considerations as well as discussion of network access security, of which DHCP is a component. A DHCP captive portal configuration example is described as is a summary of related network access control (NAC) approaches, including DHCP-based approaches, switch-based, Cisco NAC, and Microsoft NAP approaches.

Part III: DNS. Part III describes the DNS protocol, DNS applications, deployment strategies and associated configurations, and security, including the security of DNS servers and configurations and DNSSEC.

Chapter 9: The Domain Name System (DNS) Protocol. The opening chapter of Part III, provides a DNS overview, including a discussion of DNS concepts, message details, and protocol extensions. Covered DNS concepts include the basic resolution

process, the domain tree for forward and reverse domains, root hints, local-host domains, and resolver configuration. Message details include the encoding of DNS messages, including the DNS header, label formatting, and an overview of International domain names. DNS Update message formatting is also discussed as is EDNS0.

Chapter 10: DNS Applications and Resource Records. Chapter 10 builds on the material in Chapter 9 to describe key applications, which rely on DNS, including name resolution, services location, ENUM, antispam techniques via black/white listing, SPF, Sender ID, and DKIM. Discussion of applications support is presented in the context of associated resource records.

Chapter 11: DNS Server Deployment Strategies. DNS server deployment strategies and trade-offs are covered in Chapter 11. DNS server deployment scenarios include external DNS, Internet caching, hidden masters/slaves, multimaster, views, forwarding, internal roots, and anycast.

Chapter 12: Securing DNS (Part I). Chapter 12 is the first of two chapters on DNS security. This chapter covers a variety of topics related to DNS security, other than DNSSEC (DNS security extensions), which is covered in its own chapter. Known DNS vulnerabilities are presented first, followed by mitigation approaches for each.

Chapter 13: Securing DNS (Part II): DNSSEC—Chapter 13 covers DNSSEC in detail. The process of creating keys, signing zones, securely resolving names, and rolling keys is discussed, along with an example configuration.

Part IV: IPAM Integration. Part IV brings together the prior three parts, discussing techniques for cohesively managing IP address space, including impacts to DHCP and DNS.

Chapter 14: IP Address Management Practices. In Chapter 14, everyday IP address management functions are described, including IP address allocation and assignment, renumbering, moves, splits, joins, DHCP and DNS server configuration, inventory assurance, fault management, performance monitoring, and disaster recovery. This chapter is framed around the FCAPS network management model, emphasizing the necessity of a disciplined “network management” approach to IPAM.

Chapter 15: IPv6 Deployment and IPv4 Coexistence. The implementation of IPv6 within an IPv4 network will drive a lengthy coexistence of IPv4 and IPv6 protocols. Chapter 15 provides details on coexistence strategies, grouped into sections on dual stack, tunneling approaches, and translation techniques. Coverage includes 6to4, ISATAP, 6over4, Teredo, DSTM, and tunnel broker tunneling approaches and NAPT-PT, SOCKS, TRT, ALG, and bump-in-the-stack or API translation approaches. The chapter concludes with some basic migration scenarios.

ACKNOWLEDGMENTS



First, and foremost, I'd like to thank the following technical reviewers who provided extremely useful feedback, suggestions, and encouragement in the process: Greg Rabil (IPAM and DHCP engineer extraordinaire) and Paul Vixie (Internet guru and President of the Internet Systems Consortium).

I'd like to thank Janet Hurwitz, Alex Drescher, Brian Hart, and Michael Dooley who also provided input and feedback on this book.

I'd also like to thank the following individuals with whom I've had the pleasure to work and from whom I've learned tremendously about communications technologies and IPAM in particular: John Ramkawsky, Steve Thompson, Andy D'Ambrosio, Sean Fisher, Chris Scamuffa, David Cross, Scott Medrano, Marco Mecarelli, Frank Jennings, Jim Offut, Rob Woodruff, Stacie Doyle, Ralph Senseny, and those I've worked with at BT Diamond IP, INS, and Lucent. From my past life at Bell Laboratories, I thank John Marciszewski, Anthony Longhitano, Sampath Ramaswami, Maryclaire Brescia, Krishna Murti, Gaston Arredondo, Robert Schoenweisner, Tom Walker, Ray Pennotti, and especially my mentor, Thomas Chu.

Most of all, I'd also like to thank my family, my wife LeeAnn and my daughters Maeve and Tess, for putting up with my countless hours in writer's isolation and for supporting me throughout this process!

T. R.