

The Essential Resource for Linux Administrators

Linux DNS Server Administration

Craig Hunt

Craig Hunt
Linux Library



SYBEX

EX1021

Associate Publisher: Neil Edde
Contracts and Licensing Manager: Kristine O'Callaghan
Acquisitions & Developmental Editor: Maureen Adams
Editor: Sarah Lemaire
Production Editor: Molly Glover
Technical Editor: Will Deutsch
Book Designer: Bill Gibson
Graphic Illustrator: Tony Jonick
Electronic Publishing Specialist: Adrian Woolhouse
Proofreaders: Dave Nash, Laurie O'Connell, Nancy Riddiough, Suzanne Stein, Nathan Whiteside
Indexer: Matthew Spence
Cover Designer: Ingalls & Associates
Cover Illustrator: Ingalls & Associates

Copyright © 2000 SYBEX Inc., 1151 Marina Village Parkway, Alameda, CA 94501. World rights reserved. No part of this publication may be stored in a retrieval system, transmitted, or reproduced in any way, including but not limited to photocopy, photograph, magnetic or other record, without the prior agreement and written permission of the publisher.

Library of Congress Card Number: 00-105386

ISBN: 0-7821-2736-3

SYBEX and the SYBEX logo are trademarks of SYBEX Inc. in the USA and other countries.

Screen reproductions produced with Gnu Image Manipulation Program. GIMP is a freely available public domain package included as part of Linux.

Netscape Communications, the Netscape Communications logo, Netscape, and Netscape Navigator are trademarks of Netscape Communications Corporation. Netscape Communications Corporation has not authorized, sponsored, endorsed, or approved this publication and is not responsible for its content. Netscape and the Netscape Communications Corporate Logos are trademarks and trade names of Netscape Communications Corporation. All other product names and/or logos are trademarks of their respective owners.

Internet screen shot(s) using Microsoft Internet Explorer version 5 reprinted by permission from Microsoft Corporation.

TRADEMARKS: SYBEX has attempted throughout this book to distinguish proprietary trademarks from descriptive terms by following the capitalization style used by the manufacturer.

The author and publisher have made their best efforts to prepare this book, and the content is based upon final release software whenever possible. Portions of the manuscript may be based upon pre-release versions supplied by software manufacturer(s). The author and the publisher make no representation or warranties of any kind with regard to the completeness or accuracy of the contents herein and accept no liability of any kind including but not limited to performance, merchantability, fitness for any particular purpose, or any losses or damages of any kind caused or alleged to be caused directly or indirectly from this book.

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

In Listing 6.4, every host name has a unique address and every address has a unique host name. This does not have to be the case, as illustrated in Listing 6.5.

Listing 6.5 Address Records for Multi-Homed Hosts

owl	A	172.16.5.15
owl	A	172.16.7.32
owl5	A	172.16.5.15
owl7	A	172.16.7.32

In Listing 6.5, owl is a multi-homed host. The name owl is assigned both of the host's addresses, so a query for owl returns both 172.16.5.15 and 172.16.7.32. The remote system's resolver can sort out which address it wants to use. (As you learned in Chapter 4, "Configuring the Resolver," the resolver `sortlist` option can be used to control which address is used.)

The address of each interface of the multi-homed host is also assigned a unique name—owl5 and owl7 in Listing 6.5. These unique names permit those interfaces to be addressed directly for testing or other purposes. Even simple name-to-address mapping is more flexible in DNS than it is in the host table.

Defining Nicknames

Host name aliases, or nicknames, provide shorter names, "historic" names, generic names, and alternate spellings. (All of these nickname functions are described in Chapter 1, "The DNS Architecture.") The CNAME record is used to define a host alias. The name field of the CNAME record contains the host alias and the data field contains the official (canonical) name of the host. That's why CNAME is short for canonical name record. The last five records in the sample zone file are CNAME records, as shown in Listing 6.6.

Listing 6.6 Sample CNAME Records

redbreast	CNAME	robin.foobirds.org.
bob	CNAME	robin.foobirds.org.
kestral	CNAME	kestrel.foobirds.org.
www	CNAME	wren.foobirds.org.
news	CNAME	parrot.foobirds.org.

Moving down the list of CNAME records provides the following information: redbreast is a host name alias for robin. bob is also a nickname for robin. In this case, bob is a historic name from a time before we standardized on bird names. It still occasionally pops up out of an old mailing list or newsgroup so we keep the alias around. The kestral alias is used as an alternate spelling of kestrel because we have a user who just

The *name* field contains the name of the domain or host to which the mail is addressed. The *server* field contains the name of the server to which the mail is delivered. *preference* is a number used to select the most preferred server when a domain or host has multiple MX records, with low numbers preferred over high numbers. See Chapter 6 for more information about using the MX record, which is defined in RFC 1035.

Text Record (TXT) The Text record is used to define free-form information about the named object. Its format is simple

```
name ttl class TXT string
```

On Linux systems, the TXT record is generally used to provide information about a host to the technical support group. The following example illustrates this use:

```
buzzard IN TXT "Accounting Department server in room B152"
```

Because of its free-form nature, the TXT record has been used over time for special purposes, such as providing input to locally developed scripts that collect domain information. An earlier version of BIND that runs on some Unix systems even uses these records to define security information. Linux, of course, uses the latest version of BIND so it does not need to use TXT records for security. RFC 1035 defines the TXT record.

Responsible Person Record (RP) The Responsible Person record identifies the point of contact for a host or domain. The format of the RP record is

```
name ttl class RP mail_address text_pointer
```

The *mail_address* is the e-mail address of the responsible person. The @ usually included in an e-mail address is replaced with a dot. Thus, *craig@foobirds.org* becomes *craig.foobirds.org*. The *text_pointer* is the domain name of a TXT record that contains additional information about the responsible person. Here's an example of how an RP record is used with a TXT record:

```
ibis.foobirds.org. IN RP craig.foobirds.org. ibisRP
ibisRP.foobirds.org. IN TXT "Craig Hunt (301)555-1234 X237"
```

The RP record states that the person responsible for *ibis.foobirds.org* can be reached via e-mail at *craig@foobirds.org* and that additional information about the person can be obtained in the TXT records for *ibisRP.foobirds.org*. The TXT record provides the contact person's name and phone number.

Use RP records to make it easier for system administrators to contact each other when things go wrong. Unfortunately, most domains don't use RP records. Maybe the system administrators don't want people to know how to get in touch with them. But if you don't use RP records, remote administrators will contact the domain administrator when the

Linux

DNS Server Administration

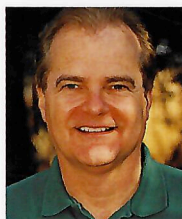
Answers to all your DNS questions—written specifically for Linux administrators

Linux DNS Server Administration is the most complete, most advanced guide to DNS for Linux you'll find anywhere. Written by a leading Linux expert, this book teaches you, step-by-step, all the standard and advanced techniques you need to know to configure and maintain a DNS server on a Linux box. Hundreds of clear, consistent examples illustrate these techniques in detail—so you stay on track and accomplish all your goals. Coverage includes:

- Understanding DNS architecture
- Understanding the protocols and messages used by DNS clients and servers
- Downloading, compiling, and installing BIND
- Configuring the resolver using the resolv.conf file and environment variables
- Setting the order of resolver queries
- Configuring the named.conf file for caching, slave, and master name servers
- Creating a domain database file and a reverse domain database file
- Creating delegated and non-delegated subdomains for your domain and reverse domain
- Securing a Linux DNS server with wrapper and ipchains
- Understanding and deploying DNSSEC protocols
- Testing DNS with host, dig, and nslookup
- Using the named.run, named_dump.db, and named.stats files to monitor your server
- Customizing BIND logging

About the Library

The **Craig Hunt Linux Library** is an eight-book set that provides in-depth, advanced coverage of the key topics for Linux administrators. Topics include Samba, System Administration, Sendmail, Apache, NFS and Automounter, and Linux Security. Each book in the library is either written by or meticulously reviewed by Craig Hunt to ensure the highest quality and most complete coverage for networking professionals working specifically in Linux environments.



Visit Sybex's Web site
(www.sybex.com)
for more information.

COMPUTER BOOK SHELF CATEGORY

Networking

US \$39.99 CAN \$59.95 UK £29.99

ISBN 0-7821-2736-3

- Perform Advanced Configuration Tasks
- Clear, In-Depth Coverage of Every Aspect of the Domain Name System
- Master the Features of BIND 8—and Look Ahead to the Forthcoming BIND 9
- Look for Other Titles in the *Craig Hunt Linux Library* from Sybex

About the Author

Craig Hunt is a noted TCP/IP and Linux expert who lectures regularly on the topics at the NetWorld+Interop, ComNet, and other networking trade shows. His other books include the best-selling *Linux Network Servers 24seven* from Sybex and the classic *TCP/IP Network Administration* from O'Reilly & Associates.



0 25211 22736 7



9 780782 127362

EX1021

