DNS与BIND（影印版）

**4th Edition**
**Covers BIND 9**
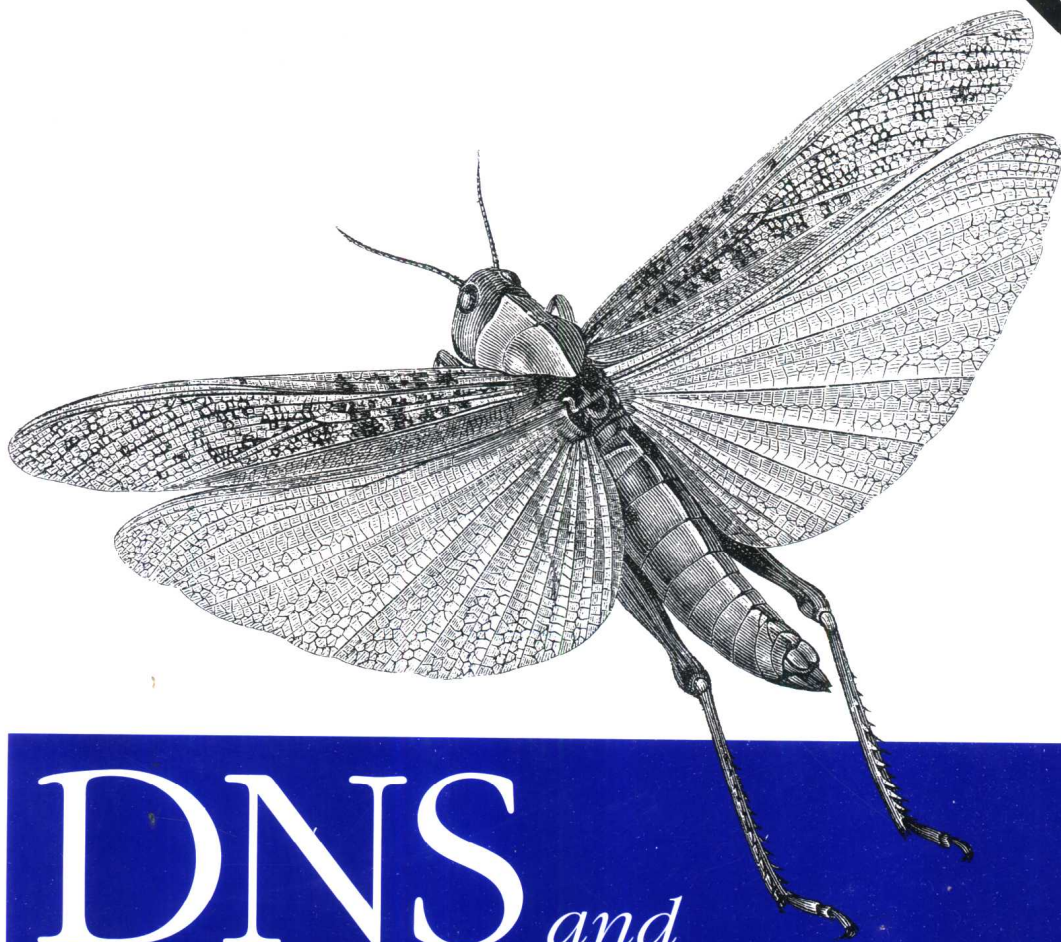
# DNS *and* BIND
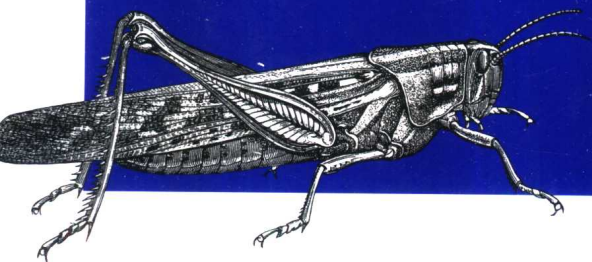
*Paul Albitz & Cricket Liu* 著

O'REILLY®

清华大学出版社

# DNS 与 BIND（影印版）

# DNS and BIND

*Paul Albitz and Cricket Liu*

## O'REILLY®

*Beijing • Cambridge • Farnham • Köln • Paris • Sebastopol • Taipei • Tokyo*

# O'Reilly & Associates 公司介绍

O'Reilly & Associates 公司是世界上在 UNIX、X、Internet 和其他开放系统图书领域具有领导地位的出版公司，同时是联机出版的先锋。

从最畅销的 *The Whole Internet User's Guide & Catalog*（被纽约公共图书馆评为 20 世纪最重要的 50 本书之一）到 GNN（最早的 Internet 门户和商业网站），再到 WebSite（第一个桌面 PC 的 Web 服务器软件），O'Reilly & Associates 一直处于 Internet 发展的最前沿。

许多书店的反馈表明，O'Reilly & Associates 是最稳定的计算机图书出版商 —— 每一本书都一版再版。与大多数计算机图书出版商相比，O'Reilly & Associates 公司具有深厚的计算机专业背景，这使得 O'Reilly & Associates 形成了一个非常不同于其他出版商的出版方针。O'Reilly & Associates 所有的编辑人员以前都是程序员，或者是顶尖级的技术专家。O'Reilly & Associates 还有许多固定的作者群体 —— 他们本身是相关领域的技术专家、咨询专家，而现在编写著作，O'Reilly & Associates 依靠他们及时地推出图书。因为 O'Reilly & Associates 紧密地与计算机业界联系着，所以 O'Reilly & Associates 知道市场上真正需要什么图书。

# 出版说明

　　计算机网络与通信技术的成熟和广泛应用，以及Internet与Web的迅速发展，为人类的工业生产、商业活动和日常生活都带来了巨大的影响。网络与通信技术在我国的很多领域也已经广泛应用，并且取得了巨大的效益。然而，该领域的技术创新的速度之快也是有目共睹的。为了帮助国内技术人员和网络管理人员在第一时间掌握国外最新的技术，清华大学出版社引进了美国O'Reilly & Associates公司的一批在计算机网络理论和应用方面代表前沿技术领域的著作，以飨读者。本套丛书采用影印版的形式，力求与国外图书"同步"出版，"原汁原味"地展现给读者各种权威技术理论和技术术语，适合于相关行业的高级技术人员、科研机构研究人员和高校教师阅读。

　　首批图书包括以下几种:

- 《Web 安全与电子商务》
- 《无线 Java 入门》
- 《Web 缓存》
- 《BEEP 权威指南》
- 《802.11 无线网络权威指南》
- 《大规模局域网设计》
- 《IP 路由》
- 《DNS 与 BIND》

# *Preface*

You may not know much about the Domain Name System—yet—but whenever you use the Internet, you use DNS. Every time you send electronic mail or surf the World Wide Web, you rely on the Domain Name System.

You see, while you, as a human being, prefer to remember the *names* of computers, computers like to address each other by number. On an internet, that number is 32 bits long, or between zero and four billion or so.* That's easy for a computer to remember because computers have lots of memory ideal for storing numbers, but it isn't nearly as easy for us humans. Pick 10 phone numbers out of the phone book at random and then try to remember them. Not easy? Now flip to the front of the phone book and attach random area codes to the phone numbers. That's about how difficult it would be to remember 10 arbitrary internet addresses.

This is part of the reason we need the Domain Name System. DNS handles mapping between host names, which we humans find convenient, and between internet addresses, which computers deal with. In fact, DNS is the standard mechanism on the Internet for advertising and accessing all kinds of information about hosts, not just addresses. And DNS is used by virtually all internetworking software, including electronic mail, remote terminal programs such as Telnet, file transfer programs such as FTP, and web browsers such as Netscape Navigator and Microsoft Internet Explorer.

Another important feature of DNS is that it makes host information available all over the Internet. Keeping information about hosts in a formatted file on a single computer only helps users on that computer. DNS provides a means of retrieving information remotely from anywhere on the network.

---

* And, with IP Version 6, it's a whopping 128 bits long, or between zero and a decimal number with 39 digits.

More than that, DNS lets you distribute the management of host information among many sites and organizations. You don't need to submit your data to some central site or periodically retrieve copies of the "master" database. You simply make sure your section, called a *zone*, is up to date on your *name servers*. Your name servers make your zone's data available to all the other name servers on the network.

Because the database is distributed, the system also needs the ability to locate the data you're looking for by searching a number of possible locations. The Domain Name System gives name servers the intelligence to navigate through the database and find data in any zone.

Of course, DNS does have a few problems. For example, the system allows more than one name server to store data about a zone, for redundancy's sake. But inconsistencies can crop up between copies of the zone data.

But the *worst* problem with DNS is that despite its widespread use on the Internet, there's really very little documentation about managing and maintaining it. Most administrators on the Internet make do with the documentation their vendors see fit to provide and with whatever they can glean from following the Internet mailing lists and Usenet newsgroups on the subject.

This lack of documentation means that the understanding of an enormously important internet service—one of the linchpins of today's Internet—is either handed down from administrator to administrator like a closely guarded family recipe, or relearned repeatedly by isolated programmers and engineers. New administrators of zones suffer through the same mistakes made by countless others.

Our aim with this book is to help remedy this situation. We realize that not all of you have the time or the desire to become DNS experts. Most of you, after all, have plenty to do besides managing your zones and name servers: system administration, network engineering, or software development. It takes an awfully big institution to devote a whole person to DNS. We'll try to give you enough information to let you do what you need to do, whether that's running a small zone or managing a multinational monstrosity, tending a single name server or shepherding a hundred of them. Read as much as you need to know now, and come back later if you need to learn more.

DNS is a big topic—big enough to require two authors, anyway—and we've tried to present it as sensibly and understandably as possible. The first two chapters give you a good theoretical overview and enough practical information to get by, and later chapters fill in the nitty-gritty details. We provide a roadmap up front to suggest a path through the book appropriate for your job or interest.

When we talk about actual DNS software, we'll concentrate almost exclusively on BIND, the Berkeley Internet Name Domain software, which is the most popular implementation of the DNS specs (and the one we know best). We've tried to distill our experience in managing and maintaining zones with BIND into this book. (One of our zones, incidentally, was once one of the largest on the Internet, but that was a long time ago.) Where possible, we've included the real programs we use in administration, many of them rewritten into Perl for speed and efficiency.

We hope this book will help you get acquainted with DNS and BIND if you're just starting out, refine your understanding if you're already familiar with them, and provide valuable insight and experience even if you know 'em like the back of your hand.

## *Versions*

The fourth edition of this book deals with the new 9.1.0 and 8.2.3 versions of BIND as well as the older 4.9 versions. While 9.1.0 and 8.2.3 are the most recent versions as of this writing, they haven't made their way into many vendors' versions of Unix yet, partly because both versions have only recently been released and many vendors are wary of using such new software. We also occasionally mention other versions of BIND, especially 4.8.3, because many vendors continue to ship code based on this older software as part of their Unix products. Whenever a feature is available only in the 4.9, 8.2.3, or 9.1.0 version, or when there is a difference in the behavior of the versions, we try to point out which version does what.

We use *nslookup*, a name server utility program, very frequently in our examples. The version we use is the one shipped with the 8.2.3 BIND code. Older versions of *nslookup* provide much, but not quite all, of the functionality in the 8.2.3 *nslookup.*[*] We've used commands common to most *nslookup*s in most of our examples; when this was not possible, we tried to note it.

## *What's New in the Fourth Edition?*

Besides updating the book to cover the most recent versions of BIND, we've added a fair amount of new material to the fourth edition:

*   More extensive coverage of dynamic update and NOTIFY, including signed dynamic updates and BIND 9's new *update-policy* mechanism, in Chapter 10

*   Incremental zone transfer, also in Chapter 10

---

[*] This is also true of the version of *nslookup* shipped with BIND 9. See Chapter 12, *nslookup and dig*, for details.

- Forward zones, which support conditional forwarding, in Chapter 10

- IPv6 forward and reverse mapping using the new A6 and DNAME records, as well as bitstring labels, at the end of Chapter 10

- Transaction signatures, also known as TSIG, a new mechanism for authenticating transactions, in Chapter 11

- An expanded section on securing name servers, in Chapter 11

- An expanded section on dealing with Internet firewalls, in Chapter 11

- Coverage of the DNS Security Extensions, or DNSSEC, a new mechanism for digitally signing zone data, also in Chapter 11

- A section on accommodating Windows 2000 clients, servers, and Domain Controllers with BIND, in Chapter 16

# Organization

This book is organized to more or less follow the evolution of a zone and its administrator. Chapters 1 and 2 discuss Domain Name System theory. Chapters 3 through 6 help you decide whether or not to set up your own zones, then describe how to go about it should you choose to. The middle of the book, Chapters 7 through 11, describe how to maintain your zones, configure hosts to use your name servers, plan for the growth of your zones, create subdomains, and secure your name servers. Finally, Chapters 12 through 16 deal with troubleshooting tools, common problems, and the lost art of programming with the resolver library routines.

Here's a more detailed, chapter-by-chapter breakdown:

Chapter 1, *Background*, provides a little historical perspective and discusses the problems that motivated the development of DNS, and then presents an overview of DNS theory.

Chapter 2, *How Does DNS Work?*, goes over DNS theory in more detail, including the organization of the DNS namespace, domains, zones, and name servers. We also introduce important concepts like name resolution and caching.

Chapter 3, *Where Do I Start?*, covers how to get the BIND software if you don't already have it, what to do with it once you've got it, how to figure out what your domain name should be, and how to contact the organization that can delegate your zone to you.

Chapter 4, *Setting Up BIND*, details how to set up your first two BIND name servers, including creating your name server database, starting up your name servers, and checking their operation.

Chapter 5, *DNS and Electronic Mail*, deals with DNS's MX record, which allows administrators to specify alternate hosts to handle a given destination's mail. This chapter covers mail routing strategies for a wide variety of networks and hosts, including networks with Internet firewalls and hosts without direct Internet connectivity.

Chapter 6, *Configuring Hosts*, explains how to configure a BIND resolver. We also include notes on the idiosyncrasies of many major Unix vendors' resolver implementations, as well as the Windows 95, NT, and 2000 resolvers.

Chapter 7, *Maintaining BIND*, describes the periodic maintenance that administrators need to perform to keep their zones running smoothly, such as checking name server health and authority.

Chapter 8, *Growing Your Domain*, covers how to plan for the growth and evolution of your zones, including how to get big and how to plan for moves and outages.

Chapter 9, *Parenting*, explores the joys of becoming a parent zone. We explain when to become a parent (create subdomains), what to call your children, how to create them (!), and how to watch over them.

Chapter 10, *Advanced Features*, goes over some less-often-used name server configuration options that can help you tune your name server's operation and ease administration.

Chapter 11, *Security,* describes how to secure your name server and how to configure your name servers to deal with Internet firewalls, and also describes two new security enhancements to DNS: the DNS Security Extensions and Transaction Signatures.

Chapter 12, *nslookup and dig*, shows the ins and outs of the most popular tools for doing DNS debugging, including techniques for digging obscure information out of remote name servers.

Chapter 13, *Reading BIND Debugging Output*, is the Rosetta Stone of BIND's debugging information. This chapter will help you make sense of the cryptic debugging information that BIND emits, which in turn will help you understand your name server better.

Chapter 14, *Troubleshooting DNS and BIND*, covers many common DNS and BIND problems and their solutions, and describes a number of less common, harder-to-diagnose scenarios.

Chapter 15, *Programming with the Resolver and Name Server Library Routines*, demonstrates how to use BIND's resolver routines to query name servers and

retrieve data from within a C program or a Perl script. We include a useful (we hope!) program to check the health and authority of your name servers.

Chapter 16, *Miscellaneous*, ties up all the loose ends. We cover DNS wildcards, hosts and networks with intermittent Internet connectivity via dialup, network name encoding, experimental record types, and Windows 2000.

Appendix A, *DNS Message Format and Resource Records*, contains a byte-by-byte breakdown of the formats used in DNS queries and responses, as well as a comprehensive list of the currently defined resource record types.

Appendix B, *BIND Compatibility Matrix*, contains a matrix showing the most important features of the most popular BIND releases.

Appendix C, *Compiling and Installing BIND on Linux*, contains step-by-step instructions on how to compile the 8.2.3 version of BIND on Linux.

Appendix D, *Top-Level Domains*, lists the current top-level domains in the Internet's domain name space.

Appendix E, *BIND Name Server and Resolver Configuration*, summarizes the syntax and semantics of each of the parameters available for configuring name servers and resolvers.

## *Audience*

This book is intended primarily for system and network administrators who manage zones and one or more name servers, but it also includes material for network engineers, postmasters, and others. Not all of the book's chapters will be equally interesting to a diverse audience, though, and you don't want to wade through 16 chapters to find the information pertinent to your job. We hope the following roadmap will help you plot your way through the book.

*System administrators setting up their first zones* should read Chapters 1 and 2 for DNS theory, Chapter 3 for information on getting started and selecting a good domain name, and Chapters 4 and 5 to learn how to set up a zone for the first time. Chapter 6 explains how to configure hosts to use the new name servers. Later, you should read Chapter 7, which explains how to "flesh out" your implementation by setting up additional name servers and adding additional zone data. Chapters 12, 13, and 14 describe troubleshooting tools and techniques.

*Experienced administrators* will benefit from reading Chapter 6 to learn how to configure DNS resolvers on different hosts, and Chapter 7 for information on maintaining your zones. Chapter 8 contains instructions on planning for a zone's growth and evolution, which should be especially valuable to administrators of large zones. Chapter 9 explains parenting—creating subdomains—which is de rigueur

reading for those considering the big move. Chapter 10 covers many new and advanced features of the BIND 8.2.3 and 9.1.0 name servers. Chapter 11 goes over securing name servers, which may be of particular interest to experienced administrators. Chapters 12 through 14 describe tools and techniques for troubleshooting, which even advanced administrators may find worth reading.

*System administrators on networks without full Internet connectivity* should read Chapter 5 to learn how to configure mail on such networks, and Chapter 11 to learn how to set up an independent DNS infrastructure.

*Programmers* can read Chapters 1 and 2 for DNS theory, then Chapter 15 for detailed coverage of how to program with the BIND resolver library routines.

*Network administrators not directly responsible for any zones* should still read Chapters 1 and 2 for DNS theory, Chapter 12 to learn how to use *nslookup* and *dig*, and Chapter 14 for troubleshooting tactics.

*Postmasters* should read Chapters 1 and 2 for DNS theory, then Chapter 5 to find out how DNS and electronic mail coexist. Chapter 12, which describes *nslookup* and *dig*, will help postmasters extract mail routing information from the domain name space.

*Interested users* can read Chapters 1 and 2 for DNS theory, and then whatever else you like!

Note that we assume you're familiar with basic Unix system administration, TCP/IP networking, and programming using simple shell scripts and Perl. We don't assume you have any other specialized knowledge, though. When we introduce a new term or concept, we'll do our best to define or explain it. Whenever possible, we'll use analogies from Unix (and from the real world) to help you understand.

# Obtaining the Example Programs

The example programs in this book are available electronically via FTP from the following URLs:

*ftp://ftp.uu.net/published/oreilly/nutshell/dnsbind/*
*ftp://ftp.oreilly.com/published/oreilly/nutshell/dnsbind/dns.tar.Z*

In either case, extract the files from the archive by typing:

```
% zcat dns.tar.Z | tar xf -
```

System V systems require the following *tar* command instead:

```
% zcat dns.tar.Z | tar xof -
```

If *zcat* is not available on your system, use separate *uncompress* and *tar* commands.

If you can't get the examples directly over the Internet but can send and receive email, you can use *ftpmail* to get them. For help using *ftpmail*, send an email to *ftpmail@online.oreilly.com* with no subject and the single word "help" in the body of the message.

## Contacting O'Reilly

You can address comments and questions about this book to the publisher:

> O'Reilly & Associates, Inc.
> 101 Morris Street
> Sebastopol, CA 95472
> (800) 998-9938 (in the United States or Canada)
> (707) 829-0515 (international/local)
> (707) 829-0104 (fax)

O'Reilly has a web page for this book, which lists errata and any additional information. You can access this page at:

> *http://www.oreilly.com/catalog/dns4*

To comment or ask technical questions about this book, send email to:

> *bookquestions@oreilly.com*

For more information about books, conferences, software, Resource Centers, and the O'Reilly Network, see the O'Reilly web site at:

> *http://www.oreilly.com*

## Conventions Used in This Book

We use the following font and format conventions for Unix commands, utilities, and system calls:

- Excerpts from scripts or configuration files are shown in a constant-width font:

  ```
  if test -x /usr/sbin/named -a -f /etc/named.conf
  then
      /usr/sbin/named
  fi
  ```

- Sample interactive sessions, showing command-line input and corresponding output, are shown in a constant-width font, with user-supplied input in bold:

  ```
  % cat /var/run/named.pid
  78
  ```

- If the command must be typed by the superuser (root), we use the sharp or pound sign (#):

  ```
  # /usr/sbin/named
  ```

- Replaceable items in code are printed in constant-width italics.

- Domain names, filenames, functions, commands, Unix manpages, and programming elements taken from the code snippets are printed in italics when they appear within a paragraph.

# Quotations

The Lewis Carroll quotations that begin each chapter are from the Millennium Fulcrum Edition 2.9 of the Project Gutenberg electronic text of *Alice's Adventures in Wonderland* and Edition 1.7 of *Through the Looking-Glass.* Quotations in Chapters 1, 2, 5, 6, 8, and 14 come from *Alice's Adventures in Wonderland,* and those in Chapters 3, 4, 7, 9, 10, 11, 12, 13, 15, and 16 come from *Through the Looking-Glass.*

# Acknowledgments

review sessions, and for proving that she could make a quilt in her spare time more quickly than her spouse could write his half of a book.

We would also like to thank the folks at O'Reilly & Associates for their hard work and patience. Credit is especially due our editors, Mike Loukides (first through third editions) and Debra Cameron (fourth edition), as well as countless others who worked on the various editions: Nancy Kotary, Ellie Fountain Maden, Robert Romano, Steven Abrams, Kismet McDonough-Chan, Seth Maislin, Ellie Cutler, Mike Sierra, Lenny Muellner, Chris Reilley, Emily Quill, Anne-Marie Vaduva, and Brenda Miller. Thanks besides to Jerry Peek for all sorts of miscellaneous help and to Tim O'Reilly for inspiring us to put it all in print.

And thanks, Edie, for the cricket on the cover!

# About the Authors

**Paul Albitz** is a software engineer at Hewlett-Packard. Paul earned a Bachelor of Science degree from the University of Wisconsin, LaCrosse, and a Master of Science degree from Purdue University.

Paul worked on BIND for the HP-UX 7.0 and 8.0 releases. During this time he developed the tools used to run the *hp.com* domain. Since then Paul has worked on networking HP's DesignJet plotter and on the fax subsystem of HP's OfficeJet multifunction peripheral. Before joining HP, Paul was a system administrator in the CS Department of Purdue University. As system administrator, he ran versions of BIND before BIND's initial release with 4.3 BSD. Paul and his wife, Katherine, live in San Diego, CA.

**Cricket Liu** matriculated at the University of California's Berkeley campus, that great bastion of free speech, unencumbered Unix, and cheap pizza. He joined Hewlett-Packard after graduation and worked for HP for nine years.

Cricket began managing the *hp.com* zone after the Loma Prieta earthquake forcibly transferred the zone's management from HP Labs to HP's Corporate Offices (by cracking a sprinkler main and flooding Labs' computer room). Cricket was *hostmaster@hp.com* for over three years, and then joined HP's Professional Services Organization to found HP's Internet consulting program.

Cricket left HP in 1997 to form Acme Byte & Wire, a DNS consulting and training company, with his friend (and now co-author) Matt Larson. Network Solutions acquired Acme in June 2000, and later the same day merged with VeriSign. Cricket is now Director of DNS Product Management for VeriSign Global Registry Services.

Cricket, his wife, Paige, and their son, Walt, live in Colorado with two Siberian Huskies, Annie and Dakota. On warm weekend afternoons, you'll probably find them on the flying trapeze or wakeboarding behind Betty Blue.

# Colophon

Our look is the result of reader comments, our own experimentation, and feedback from distribution channels. Distinctive covers complement our distinctive approach to technical topics, breathing personality and life into potentially dry subjects.

The insects featured on the cover of *DNS and BIND* are grasshoppers. Grasshoppers are found all over the globe. Of over 5000 species, 100 different grasshopper species

are found in North America. Grasshoppers are greenish-brown, and range in length from a half inch to four inches, with wingspans of up to six inches. Their bodies are divided into three sections: the head, thorax, and abdomen, with three pairs of legs and two pairs of wings.

Male grasshoppers use their hind legs and forewings to produce a "chirping" sound. Their hind legs have a ridge of small pegs that are rubbed across a hardened vein in the forewing, causing an audible vibration much like a bow being drawn across a string.

Grasshoppers are major crop pests, particularly when they collect in swarms. A single grasshopper can consume 30mg of food a day. In collections of 50 or more grasshoppers per square yard—a density often reached during grasshopper outbreaks—grasshoppers consume as much as a cow would per acre. In addition to consuming foliage, grasshoppers damage plants by attacking them at vulnerable points and causing the stems to break off.