BIND 9
ADMINISTRATOR REFERENCE MANUAL
BIND 9
Administrator Reference Manual

Version 9.1
January 2001

by the
Nominum BIND Development Team
Nominum, Inc.

for
Internet Software Consortium
Redwood City, CA 94063
Availability

The *BIND 9 Administrator Reference Manual* is based on BIND version 9.1. This manual was written and formatted by Nominum, Inc., and is distributed by Nominum on behalf of the Internet Software Consortium (ISC).

The information in this document is also included with the BIND 9 source distribution kit in the `doc/arm` directory in DocBook XML and HTML formats. Instructions for obtaining the latest release of the BIND 9 distribution kit can be found on the ISC web site at http://www.isc.org/.

Acknowledgments

BIND 9 development has been generously underwritten by the following organizations:

- Sun Microsystems, Inc.
- Hewlett Packard
- Compaq Computer Corporation
- IBM
- Process Software Corporation
- Silicon Graphics, Inc.
- Network Associates, Inc.
- U.S. Defense Information Systems Agency
- USENIX Association
- Stichting NLnet - NLnet Foundation

Trademark Information

UNIX® is a registered trademark of the Open Group.
AIX® is a registered trademark of IBM Corporation.
HP-UX® is a registered trademark of Hewlett-Packard Company.
Compaq® and Digital® are registered trademarks of the Compaq Computer Corporation.
Tru64™ UNIX® is a trademark of Compaq Computer Corporation.
IRIX® is a registered trademark of Silicon Graphics, Inc.
Red Hat® is a registered trademark of Red Hat, Inc.
Sun™ and Solaris™ are trademarks or registered trademarks of Sun Microsystems, Inc.
in the United States and other countries.

Nominum, Inc,
2385 Bay Road
Redwood City, CA 94063
http://www.nominum.com/

Internet Software Consortium
950 Charter Street
Redwood City, CA 94063
http://www.isc.org/

Copyright © 2001 Nominum, Inc. and Internet Software Consortium
Section 1: Introduction

1.1 Scope of Document ..................................................... 1
1.2 Organization of This Document ....................................... 1
1.3 Conventions Used in This Document .................................. 1
1.4 Discussion of Domain Name System (DNS) Basics and BIND ............ 2
  1.4.1 Nameservers .................................................. 2
  1.4.2 Types of Zones ............................................... 3
1.4.3 Servers .................................................................. 4
  1.4.3.1 Master Server ................................................ 4
  1.4.3.2 Slave Server .................................................. 4
  1.4.3.3 Caching Only Server ......................................... 4
  1.4.3.4 Forwarding Server .......................................... 4
  1.4.3.5 Stealth Server ............................................... 5

Section 2: BIND Resource Requirements .................................... 7
2.1 Hardware requirements .................................................. 7
2.2 CPU Requirements ..................................................... 7
2.3 Memory Requirements .................................................. 7
2.4 Nameserver Intensive Environment Issues ............................. 7
2.5 Supported Operating Systems ........................................... 7

Section 3: Nameserver Configuration ........................................ 9
3.1 Sample Configurations .................................................. 9
  3.1.1 A Caching-only Nameserver ..................................... 9
  3.1.2 An Authoritative-only Nameserver ................................ 9
3.2 Load Balancing .......................................................... 10
3.3 Notify ........................................................................ 10
3.4 Nameserver Operations ................................................. 11
  3.4.1 Tools for Use With the Nameserver Daemon ..................... 11
    3.4.1.1 Diagnostic Tools ........................................... 11
    3.4.1.2 Administrative Tools ....................................... 12
  3.4.2 Signals .......................................................... 14

Section 4: Advanced Concepts .............................................. 15
4.1 Dynamic Update ....................................................... 15
4.2 Incremental Zone Transfers (IXFR) .................................... 15
4.3 Split DNS ............................................................. 15
4.4 TSIG .................................................................. 19
  4.4.1 Generate Shared Keys for Each Pair of Hosts .................... 19
    4.4.1.1 Automatic Generation .................................... 19
    4.4.1.2 Manual Generation ....................................... 19
  4.4.2 Copying the Shared Secret to Both Machines .................... 20
  4.4.3 Informing the Servers of the Key's Existence ................... 20
  4.4.4 Instructing the Server to Use the Key .......................... 20
  4.4.5 TSIG Key Based Access Control ................................. 20
  4.4.6 Errors .......................................................... 21
8.1 Common Problems .................................................... 79
  8.1.1 It's not working; how can I figure out what’s wrong? ................. 79
8.2 Incrementing and Changing the Serial Number ............................. 79
8.3 Where Can I Get Help? ................................................ 79

Appendix A: Acknowledgements 83
  A.1 A Brief History of the DNS and BIND ................................. 83

Appendix B: Historical DNS Information 85
  B.1 Classes of Resource Records .......................................... 85
    B.1.1 HS = hesiod ..................................................... 85
    B.1.2 CH = chaos ...................................................... 85

Appendix C: General DNS Reference Information 87
  C.1 IPv6 addresses (A6) .................................................. 87

Appendix D: Bibliography (and Suggested Reading) 89
  D.1 Request for Comments (RFCs) ........................................ 89
    D.1.1 Standards ....................................................... 89
    D.1.2 Proposed Standards ............................................. 89
    D.1.3 Proposed Standards Still Under Development ..................... 89
    D.1.4 Other Important RFCs About DNS Implementation ................. 89
    D.1.5 Resource Record Types .......................................... 90
    D.1.6 DNS and the Internet .......................................... 90
    D.1.7 DNS Operations ................................................ 90
    D.1.8 Other DNS-related RFCs ........................................ 90
    D.1.9 Obsolete and Unimplemented Experimental RRs ...................... 91
  D.2 Internet Drafts .................................................... 91
  D.3 Other Documents About BIND ......................................... 91
Section 1. Introduction

The Internet Domain Name System (DNS) consists of the syntax to specify the names of entities in the Internet in a hierarchical manner, the rules used for delegating authority over names, and the system implementation that actually maps names to Internet addresses. DNS data is maintained in a group of distributed hierarchical databases.

1.1 Scope of Document

The Berkeley Internet Name Domain (BIND) implements an Internet nameserver for a number of operating systems. This document provides basic information about the installation and care of the Internet Software Consortium (ISC) BIND version 9 software package for system administrators.

1.2 Organization of This Document

In this document, Section 1 introduces the basic DNS and BIND concepts. Section 2 describes resource requirements for running BIND in various environments. Information in Section 3 is task-oriented in its presentation and is organized functionally, to aid in the process of installing the BIND 9 software. The task-oriented section is followed by Section 4, which contains more advanced concepts that the system administrator may need for implementing certain options. Section 5 describes the BIND 9 lightweight resolver. The contents of Section 6 are organized as in a reference manual to aid in the ongoing maintenance of the software. Section 7 addresses security considerations, and Section 8 contains troubleshooting help. The main body of the document is followed by several Appendices which contain useful reference information, such as a Bibliography and historic information related to BIND and the Domain Name System.

1.3 Conventions Used in This Document

In this document, we use the following general typographic conventions:

<table>
<thead>
<tr>
<th>To describe:</th>
<th>We use the style:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a pathname, filename, URL, hostname, mailing list name, or new term or concept</td>
<td><em>Italic</em></td>
</tr>
<tr>
<td>literal user input</td>
<td><em>Fixed Width Bold</em></td>
</tr>
<tr>
<td>variable user input</td>
<td><em>Fixed Width Italic</em></td>
</tr>
<tr>
<td>program output</td>
<td><em>Fixed Width Bold</em></td>
</tr>
</tbody>
</table>

The following conventions are used in descriptions of the BIND configuration file:

<table>
<thead>
<tr>
<th>To describe:</th>
<th>We use the style:</th>
</tr>
</thead>
<tbody>
<tr>
<td>keywords</td>
<td>Sans Serif Bold</td>
</tr>
<tr>
<td>variables</td>
<td>Sans Serif Italic</td>
</tr>
<tr>
<td>“meta-syntactic” information (within brackets when optional)</td>
<td><em>Fixed Width Italic</em></td>
</tr>
</tbody>
</table>
1.4 Discussion of Domain Name System (DNS) Basics and BIND

The purpose of this document is to explain the installation and basic upkeep of the BIND software package, and we begin by reviewing the fundamentals of the domain naming system as they relate to BIND. BIND consists of a nameserver (or “daemon”) called named and a resolver library. The BIND server runs in the background, servicing queries on a well known network port. The standard port for the User Datagram Protocol (UDP) and Transmission Control Protocol (TCP), usually port 53, is specified in /etc/services. The resolver is a set of routines residing in a system library that provides the interface that programs can use to access the domain name services.

1.4.1 Nameservers

A nameserver (NS) is a program that stores information about named resources and responds to queries from programs called resolvers which act as client processes. The basic function of an NS is to provide information about network objects by answering queries.

With the nameserver, the network can be broken into a hierarchy of domains. The name space is organized as a tree according to organizational or administrative boundaries. Each node of the tree, called a domain, is given a label. The name of the domain is the concatenation of all the labels of the domains from the root to the current domain. This is represented in written form as a string of labels listed from right to left and separated by dots. A label need only be unique within its domain. The whole name space is partitioned into areas called zones, each starting at a domain and extending down to the leaf domains or to domains where other zones start. Zones usually represent administrative boundaries. For example, a domain name for a host at the company Example, Inc. would be:

ourhost.example.com

where com is the top level domain to which ourhost.example.com belongs, example is a subdomain of com, and ourhost is the name of the host.

The specifications for the domain nameserver are defined in the RFC 1034, RFC 1035 and RFC 974. These documents can be found in /usr/src/etc/named/doc in 4.4BSD or are available via File Transfer Protocol (FTP) from ftp://www.isi.edu/in-notes/ or via the Web at http://www.ietf.org/rfc/. (See Appendix C for complete information on finding and retrieving RFCs.) It is also recommended that you read the related man pages: named and resolver.
1.4.2 Types of Zones

As we stated previously, a zone is a point of delegation in the DNS tree. A zone consists of those contiguous parts of the domain tree for which a domain server has complete information and over which it has authority. It contains all domain names from a certain point downward in the domain tree except those which are delegated to other zones. A delegation point has one or more NS records in the parent zone, which should be matched by equivalent NS records at the root of the delegated zone.

To properly operate a nameserver, it is important to understand the difference between a zone and a domain.

For instance, consider the example.com domain which includes names such as host.aaa.example.com and host.bbb.example.com even though the example.com zone includes only delegations for the aaa.example.com and bbb.example.com zones. A zone can map exactly to a single domain, but could also include only part of a domain, the rest of which could be delegated to other nameservers. Every name in the DNS tree is a domain, even if it is terminal, that is, has no subdomains. Every subdomain is a domain and every domain except the root is also a subdomain. The terminology is not intuitive and we suggest that you read RFCs 1033, 1034 and 1035 to gain a complete understanding of this difficult and subtle topic.

Though BIND is a Domain Nameserver, it deals primarily in terms of zones. The master and slave declarations in the named.conf file specify zones, not domains. When you ask some other site if it is willing to be a slave server for your domain, you are actually asking for slave service for some collection of zones.

Each zone will have one primary master (also called primary) server which loads the zone contents from some local file edited by humans or perhaps generated mechanically from some other local file which is edited by humans. There will be some number of slave (also called secondary) servers, which load the zone contents using the DNS protocol (that is, the secondary servers will contact the primary and fetch the zone data using TCP). This set of servers—the primary and all of its secondaries—should be listed in the NS records in the parent zone and will constitute a delegation. This set of servers must also be listed in the zone file itself, usually under the @ name which indicates the top level or root of the current zone. You can list servers in the zone’s top-level @ NS records that are not in the parent’s NS delegation, but you cannot list servers in the parent’s delegation that are not present in the zone’s @.

Any servers listed in the NS records must be configured as authoritative for the zone. A server is authoritative for a zone when it has been configured to answer questions for that zone with authority, which it does by setting the “authoritative answer” (AA) bit in reply packets. A server may be authoritative for more than one zone. The authoritative data for a zone is composed of all of the Resource Records (RRs)—the data associated with names in a tree-structured name space—attached to all of the nodes from the top node of the zone down to leaf nodes or nodes above cuts around the bottom edge of the zone.
Adding a zone as a type master or type slave will tell the server to answer questions for the zone authoritatively. If the server is able to load the zone into memory without any errors it will set the AA bit when it replies to queries for the zone. See RFCs 1034 and 1035 for more information about the AA bit.

1.4.3 Servers

A DNS server can be master for some zones and slave for others or can be only a master, or only a slave, or can serve no zones and just answer queries via its cache. Master servers are often also called primaries and slave servers are often also called secondaries. Both master/primary and slave/secondary servers are authoritative for a zone.

All servers keep data in their cache until the data expires, based on a Time To Live (TTL) field which is maintained for all resource records.

1.4.3.1 Master Server

The primary master server is the ultimate source of information about a domain. The primary master is an authoritative server configured to be the source of zone transfer for one or more secondary servers. The primary master server obtains data for the zone from a file on disk.

1.4.3.2 Slave Server

A slave server, also called a secondary server, is an authoritative server that uses zone transfers from the primary master server to retrieve the zone data. Optionally, the slave server obtains zone data from a cache on disk. Slave servers provide necessary redundancy. All secondary/slave servers are named in the NS RRs for the zone.

1.4.3.3 Caching Only Server

Some servers are caching only servers. This means that the server caches the information that it receives and uses it until the data expires. A caching only server is a server that is not authoritative for any zone. This server services queries and asks other servers, who have the authority, for the information it needs.

1.4.3.4 Forwarding Server

Instead of interacting with the nameservers for the root and other domains, a forwarding server always forwards queries it cannot satisfy from its authoritative data or cache to a fixed list of other servers. The forwarded queries are also known as recursive queries, the same type as a client would send to a server. There may be one or more servers forwarded to, and they are queried in turn until the list is exhausted or an answer is found. A forwarding server is typically used when you do not wish all the servers at a given site to interact with the rest of the Internet servers. A typical scenario would involve a number of internal DNS
servers and an Internet firewall. Servers unable to pass packets through the firewall would forward to the server that can do it, and that server would query the Internet DNS servers on the internal server’s behalf. An added benefit of using the forwarding feature is that the central machine develops a much more complete cache of information that all the workstations can take advantage of.

There is no prohibition against declaring a server to be a forwarder even though it has master and/or slave zones as well; the effect will still be that anything in the local server’s cache or zones will be answered, and anything else will be forwarded using the forwarders list.

### 1.4.3.5 Stealth Server

A *stealth server* is a server that answers authoritatively for a zone, but is not listed in that zone’s NS records. Stealth servers can be used as a way to centralize distribution of a zone, without having to edit the zone on a remote nameserver. Where the master file for a zone resides on a stealth server in this way, it is often referred to as a “hidden primary” configuration. Stealth servers can also be a way to keep a local copy of a zone for rapid access to the zone’s records, even if all “official” nameservers for the zone are inaccessible.
Section 2. BIND Resource Requirements

2.1 Hardware requirements

DNS hardware requirements have traditionally been quite modest. For many installations, servers that have been pensioned off from active duty have performed admirably as DNS servers.

The DNSSEC and IPv6 features of BIND 9 may prove to be quite CPU intensive however, so organizations that make heavy use of these features may wish to consider larger systems for these applications. BIND 9 is now fully multithreaded, allowing full utilization of multiprocessor systems for installations that need it.

2.2 CPU Requirements

CPU requirements for BIND 9 range from i486-class machines for serving of static zones without caching, to enterprise-class machines if you intend to process many dynamic updates and DNSSEC signed zones, serving many thousands of queries per second.

2.3 Memory Requirements

The memory of the server has to be large enough to fit the cache and zones loaded off disk. Future releases of BIND 9 will provide methods to limit the amount of memory used by the cache, at the expense of reducing cache hit rates and causing more DNS traffic. It is still good practice to have enough memory to load all zone and cache data into memory—unfortunately, the best way to determine this for a given installation is to watch the nameserver in operation. After a few weeks the server process should reach a relatively stable size where entries are expiring from the cache as fast as they are being inserted. Ideally, the resource limits should be set higher than this stable size.

2.4 Nameserver Intensive Environment Issues

For nameserver intensive environments, there are two alternative configurations that may be used. The first is where clients and any second-level internal nameservers query a main nameserver, which has enough memory to build a large cache. This approach minimizes the bandwidth used by external name lookups. The second alternative is to set up second-level internal nameservers to make queries independently. In this configuration, none of the individual machines needs to have as much memory or CPU power as in the first alternative, but this has the disadvantage of making many more external queries, as none of the nameservers share their cached data.

2.5 Supported Operating Systems

ISC BIND 9 compiles and runs on the following operating systems:

IBM AIX 4.3
Compaq Digital/Tru64 UNIX 4.0D
HP HP-UX 11
IRIX64 6.5
Red Hat Linux 6.0, 6.1
Sun Solaris 2.6, 7, 8 (beta)
FreeBSD 3.4-STABLE
NetBSD-current with “unproven” pthreads
Section 3. Nameserver Configuration

In this section we provide some suggested configurations along with guidelines for their use. We also address the topic of reasonable option setting.

3.1 Sample Configurations

3.1.1 A Caching-only Nameserver

The following sample configuration is appropriate for a caching-only name server for use by clients internal to a corporation. All queries from outside clients are refused.
// Two corporate subnets we wish to allow queries from.
 acl "corpnets" { 192.168.4.0/24; 192.168.7.0/24; };

options {
    directory "/etc/namedb"; // Working directory
    pid-file "named.pid"; // Put pid file in working dir
    allow-query { "corpnets"; };
};

// Root server hints
zone "." { type hint; file "root.hint"; };

// Provide a reverse mapping for the loopback address 127.0.0.1
zone "0.0.127.in-addr.arpa" {
    type master;
    file "localhost.rev";
    notify no;
};

3.1.2 An Authoritative-only Nameserver

This sample configuration is for an authoritative-only server that is the master server for “example.com” and a slave for the subdomain “eng.example.com”.

options {
    directory "/etc/namedb"; // Working directory
    pid-file "named.pid"; // Put pid file in working dir
    allow-query { any; };
    allow-recursion no; // Do not provide recursive service
};

// Root server hints
zone "." { type hint; file "root.hint"; };

// Provide a reverse mapping for the loopback address 127.0.0.1
zone "0.0.127.in-addr.arpa" {
    type master;
    file "localhost.rev";
    notify no;
};
// We are the master server for example.com
zone "example.com" {
    type master;
    file "example.com.db";
    // IP addresses of slave servers allowed to transfer example.com
    allow-transfer {
        192.168.4.14;
        192.168.5.53;
    };
};
// We are a slave server for eng.example.com
zone "eng.example.com" {
    type slave;
    file "eng.example.com.bk";
    // IP address of eng.example.com master server
    masters { 192.168.4.12; };
};

3.2 Load Balancing

Primitive load balancing can be achieved in DNS using multiple A records for one name.

For example, if you have three WWW servers with network addresses of 10.0.0.1, 10.0.0.2 and 10.0.0.3, a set of records such as the following means that clients will connect to each machine one third of the time:

<table>
<thead>
<tr>
<th>Name</th>
<th>TTL</th>
<th>CLASS</th>
<th>TYPE</th>
<th>Resource Record (RR) Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>www</td>
<td>600</td>
<td>IN</td>
<td>A</td>
<td>10.0.0.1</td>
</tr>
<tr>
<td></td>
<td>600</td>
<td>IN</td>
<td>A</td>
<td>10.0.0.2</td>
</tr>
<tr>
<td></td>
<td>600</td>
<td>IN</td>
<td>A</td>
<td>10.0.0.3</td>
</tr>
</tbody>
</table>

When a resolver queries for these records, BIND will rotate them and respond to the query with the records in a different order. In the example above, clients will randomly receive records in the order 1, 2, 3; 2, 3, 1; and 3, 1, 2. Most clients will use the first record returned and discard the rest.

For more detail on ordering responses, check the rrset-order substatement in the options statement under Section 6.2.14.11, RRset Ordering on page 56. This substatement is not supported in BIND 9, and only the ordering scheme described above is available.

3.3 Notify

DNS Notify is a mechanism that allows master nameservers to notify their slave servers of changes to a zone’s data. In response to a NOTIFY from a master server, the slave will check to see that its version of the zone is the current version and, if not, initiate a transfer.
DNS Notify is fully documented in RFC 1996. See also the description of the zone option also-notify in under Section 6.2.14.6, Zone Transfers on page 50. More information about notify can be found under Section 6.2.14.1, Boolean Options on page 44.

3.4 Nameserver Operations

3.4.1 Tools for Use With the Nameserver Daemon

There are several indispensable diagnostic, administrative and monitoring tools available to the system administrator for controlling and debugging the nameserver daemon. We describe several in this section

3.4.1.1 Diagnostic Tools

dig

The domain information groper (dig) is a command line tool that can be used to gather information from the Domain Name System servers. Dig has two modes: simple interactive mode for a single query, and batch mode which executes a query for each in a list of several query lines. All query options are accessible from the command line.

Usage

dig [@server] domain [query-type] [query-class]
   [query-option] [dig-option] [comment]

The usual simple use of dig will take the form

dig @server domain query-type query-class

For more information and a list of available commands and options, see the dig man page.

host

The host utility provides a simple DNS lookup using a command-line interface for looking up Internet hostnames. By default, the utility converts between host names and Internet addresses, but its functionality can be extended with the use of options.

Usage

host [-aCdlrTwv] [-c class] [-N ndots] [-t type]
   [-W timeout] [-R retries] hostname [server]

For more information and a list of available commands and options, see the host man page.

nslookup

nslookup is a program used to query Internet domain nameservers. nslookup has two modes: interactive and non-interactive. Interactive
mode allows the user to query nameservers for information about various hosts and domains or to print a list of hosts in a domain. Non-interactive mode is used to print just the name and requested information for a host or domain.

Usage

nslookup [-option ...] [host-to-find | - [server]]

Interactive mode is entered when no arguments are given (the default nameserver will be used) or when the first argument is a hyphen ('-') and the second argument is the host name or Internet address of a nameserver.

Non-interactive mode is used when the name or Internet address of the host to be looked up is given as the first argument. The optional second argument specifies the host name or address of a nameserver.

Due to its arcane user interface and frequently inconsistent behavior, we do not recommend the use of nslookup. Use dig instead.

3.4.1.2 Administrative Tools

Administrative tools play an integral part in the management of a server.

rndc

The remote name daemon control (rndc) program allows the system administrator to control the operation of a nameserver. If you run rndc without any options it will display a usage message as follows:


command is one of the following for named:

- reload
  - Reload configuration file and zones.

- reload zone [ class [view] ]
  - Reload the given zone.

- refresh zone [ class [view] ]
  - Schedule zone maintenance for the given zone.

- stats
  - Write server statistics to the statistics file.

- querylog
  - Toggle query logging.

- stop
  - Stop the server, making sure any recent changes made through dynamic update or IXFR are first saved to the master files of the updated zones.
In BIND 9.1, \texttt{rndc} does not yet support all the commands of the BIND 8 \texttt{ndc} utility. Additional commands will be added in future releases.

A configuration file is required, since all communication with the server is authenticated with digital signatures that rely on a shared secret, and there is no way to provide that secret other than with a configuration file. The default location for the \texttt{rndc} configuration file is \texttt{/etc/rndc.conf}, but an alternate location can be specified with the \texttt{-c} option.

The format of the configuration file is similar to that of \texttt{named.conf}, but limited to only three statements, the \texttt{options}, \texttt{key} and \texttt{server} statements. These statements are what associate the secret keys to the servers with which they are meant to be shared. The order of statements is not significant.

The \texttt{options} statement has two clauses: \texttt{default-server} and \texttt{default-key}. \texttt{default-server} takes a host name or address argument and represents the server that will be contacted if no \texttt{-s} option is provided on the command line. \texttt{default-key} takes the name of key as its argument, as defined by a \texttt{key} statement. In the future a \texttt{default-port} clause will be added to specify the port to which \texttt{rndc} should connect.

The \texttt{key} statement names a key with its string argument. The string is required by the server to be a valid domain name, though it need not actually be hierarchical; thus, a string like “\texttt{rndc_key}” is a valid name. The \texttt{key} statement has two clauses: \texttt{algorithm} and \texttt{secret}. While the configuration parser will accept any string as the argument to \texttt{algorithm}, currently only the string “\texttt{hmac-md5}” has any meaning. The secret is a base-64 encoded string, typically generated with either \texttt{dnssec-keygen} or \texttt{mmencode}.

The \texttt{server} statement uses the key clause to associate a \texttt{key}-defined key with a server. The argument to the \texttt{server} statement is a host name or address (addresses must be double quoted). The argument to the key clause is the name of the key as defined by the \texttt{key} statement. A \texttt{port} clause will be added to a future release to specify the port to which \texttt{rndc} should connect on the given server.

A sample minimal configuration file is as follows:

```plaintext
key rndc_key {
    algorithm "hmac-md5";
}
```

halt

Stop the server immediately. Recent changes made through dynamic update or IXFR are not saved to the master files, but will be rolled forward from the journal files when the server is restarted.
secret "c3Ryb25nIGVub3VnaCBmb3IgYSBtYW4gYmV0IG1hZGUgZm9yIGEgd29tYW4K";
};

options {
    default-server localhost;
    default-key rndc_key;
};

This file, if installed as /etc/rndc.conf, would allow the command:

$ rndc reload

to connect to 127.0.0.1 port 953 and cause the nameserver to reload, if a
nameserver on the local machine were running with following controls
statements:

controls {
    inet 127.0.0.1 allow { localhost; } keys { rndc_key; }; 
};

and it had an identical key statement for rndc_key.

3.4.2 Signals

Certain UNIX signals cause the name server to take specific actions, as described in
the following table. These signals can be sent using the kill command.

- **SIGHUP**: Causes the server to read named.conf and reload the database.
- **SIGTERM**: Causes the server to clean up and exit.
- **SIGINT**: Causes the server to clean up and exit.
Section 4. Advanced Concepts

4.1 Dynamic Update

Dynamic update is the term used for the ability under certain specified conditions to add, modify or delete records or RRsets in the master zone files. Dynamic update is fully described in RFC 2136.

Dynamic update is enabled on a zone-by-zone basis, by including an allow-update or update-policy clause in the zone statement.

Updating of secure zones (zones using DNSSEC) is modelled after the simple-secure-update proposal, a work in progress in the DNS Extensions working group of the IETF. (See http://www.ietf.org/html.charters/dnsext-charter.html for information about the DNS Extensions working group.) SIG and NXT records affected by updates are automatically regenerated by the server using an online zone key. Update authorization is based on transaction signatures and an explicit server policy.

The zone files of dynamic zones must not be edited by hand. The zone file on disk at any given time may not contain the latest changes performed by dynamic update. The zone file is written to disk only periodically, and changes that have occurred since the zone file was last written to disk are stored only in the zone’s journal (.jnl) file. BIND 9 currently does not update the zone file when it exits as BIND 8 does, so editing the zone file manually is unsafe even when the server has been shut down.

4.2 Incremental Zone Transfers (IXFR)

The incremental zone transfer (IXFR) protocol is a way for slave servers to transfer only changed data, instead of having to transfer the entire zone. The IXFR protocol is documented in RFC 1995. See the list of proposed standards in Appendix C, Section D.1.2, “Proposed Standards”, page 89.

When acting as a master, BIND 9 supports IXFR for those zones where the necessary change history information is available. These include master zones maintained by dynamic update and slave zones whose data was obtained by IXFR, but not manually maintained master zones nor slave zones obtained by performing a full zone transfer (AXFR).

When acting as a slave, BIND 9 will attempt to use IXFR unless it is explicitly disabled. For more information about disabling IXFR, see the description of the request-ixfr clause of the server statement.

4.3 Split DNS

Setting up different views, or visibility, of DNS space to internal and external resolvers is usually referred to as a Split DNS setup. There are several reasons an organization would want to set up its DNS this way.

One common reason for setting up a DNS system this way is to hide “internal” DNS information from “external” clients on the Internet. There is some debate as to whether or
not this is actually useful. Internal DNS information leaks out in many ways (via email headers, for example) and most savvy “attackers” can find the information they need using other means.

Another common reason for setting up a Split DNS system is to allow internal networks that are behind filters or in RFC 1918 space (reserved IP space, as documented in RFC 1918) to resolve DNS on the Internet. Split DNS can also be used to allow mail from outside back in to the internal network.

Here is an example of a split DNS setup:

Let’s say a company named Example, Inc. (example.com) has several corporate sites that have an internal network with reserved Internet Protocol (IP) space and an external demilitarized zone (DMZ), or “outside” section of a network, that is available to the public. Example, Inc. wants its internal clients to be able to resolve external hostnames and to exchange mail with people on the outside. The company also wants its internal resolvers to have access to certain internal-only zones that are not available at all outside of the internal network.

In order to accomplish this, the company will set up two sets of nameservers. One set will be on the inside network (in the reserved IP space) and the other set will be on bastion hosts, which are “proxy” hosts that can talk to both sides of its network, in the DMZ.

The internal servers will be configured to forward all queries, except queries for site1.internal, site2.internal, site1.example.com, and site2.example.com, to the servers in the DMZ. These internal servers will have complete sets of information for site1.example.com, site2.example.com, site1.internal, and site2.internal.

To protect the site1.internal and site2.internal domains, the internal nameservers must be configured to disallow all queries to these domains from any external hosts, including the bastion hosts.

The external servers, which are on the bastion hosts, will be configured to serve the “public” version of the site1 and site2.example.com zones. This could include things such as the host records for public servers (www.example.com and ftp.example.com), and mail exchange (MX) records (a.mx.example.com and b.mx.example.com).

In addition, the public site1 and site2.example.com zones should have special MX records that contain wildcard (‘*’) records pointing to the bastion hosts. This is needed because external mail servers do not have any other way of looking up how to deliver mail to those internal hosts. With the wildcard records, the mail will be delivered to the bastion host, which can then forward it on to internal hosts.

Here’s an example of a wildcard MX record:

* IN MX 10 external1.example.com.

Now that they accept mail on behalf of anything in the internal network, the bastion hosts will need to know how to deliver mail to internal hosts. In order for this to work properly,
the resolvers on the bastion hosts will need to be configured to point to the internal
nameservers for DNS resolution.

Queries for internal hostnames will be answered by the internal servers, and queries for
external hostnames will be forwarded back out to the DNS servers on the bastion hosts.

In order for all this to work properly, internal clients will need to be configured to query only
the internal nameservers for DNS queries. This could also be enforced via selective filtering
on the network.

If everything has been set properly, Example, Inc.’s internal clients will now be able to:

- Look up any hostnames in the site1 and site2.example.com zones.
- Look up any hostnames in the site1.internal and site2.internal domains.
- Look up any hostnames on the Internet.
- Exchange mail with internal AND external people.

Hosts on the Internet will be able to:

- Look up any hostnames in the site1 and site2.example.com zones.
- Exchange mail with anyone in the site1 and site2.example.com zones.

Here is an example configuration for the setup we just described above. Note that this is only
configuration information; for information on how to configure your zone files, see Section

Internal DNS server config:

```
# acl internals { 172.16.72.0/24; 192.168.1.0/24; };
# acl externals { 192.168.1.0/24; };
# options {
#   ... 
#   ... 
#   forward only;
#   forwarders { bastion-ips-go-here; }; // forward to external servers
#   allow-transfer { none; }; // sample allow-transfer (no one)
#   allow-query { internals; externals; }; // restrict query access
#   allow-recursion { internals; }; // restrict recursion
#   ... 
#   ... 
#};
# zone "site1.example.com" { // sample slave zone
#   type master;
#   file "m/site1.example.com";
#   forwards { };
#   allow-query { internals; externals; }; // do normal iterative
#   allow-transfer { internals; };
#   allow-recursion { internals; };
#};
# zone "site2.example.com" {
#   type slave;
#   file "s/site2.example.com";
```
masters { 172.16.72.3; }
forwarders { }
allow-query { internals; externals; }
allow-transfer { internals; }

zone "site1.internal" {
type master;
file "m/site1.internal";
forwarders { }
allow-query { internals; }
allow-transfer { internals; }
}

zone "site2.internal" {
type slave;
file "s/site2.internal";
masters { 172.16.72.3; }
forwarders { }
allow-query { internals; }
allow-transfer { internals; }
}

External (bastion host) DNS server config:
acl internals { 172.16.72.0/24; 192.168.1.0/24; }
acl externals { bastion-ips-go-here; }
options {
    ...
    ...
    allow-transfer { none; }; // sample allow-transfer (no one)
    allow-query { internals; externals; }; // restrict query access
    allow-recursion { internals; externals; }; // restrict recursion
    ...
    ...
}

zone "site1.example.com" { // sample slave zone
type master;
file "m/site1.foo.com";
allow-query { any; }
allow-transfer { internals; externals; }
}

zone "site2.example.com" {
type slave;
file "s/site2.foo.com";
masters { another_bastion_host_maybe; }
allow-query { any; }
allow-transfer { internals; externals; }
}

In the resolv.conf (or equivalent) on the bastion host(s):
search ...
nameserver 172.16.72.2
nameserver 172.16.72.3
nameserver 172.16.72.4
4.4 TSIG

This is a short guide to setting up Transaction SIGnatures (TSIG) based transaction security
in BIND. It describes changes to the configuration file as well as what changes are required
for different features, including the process of creating transaction keys and using
transaction signatures with BIND.

BIND primarily supports TSIG for server to server communication. This includes zone
transfer, notify, and recursive query messages. Resolvers based on newer versions of
BIND 8 have limited support for TSIG.

TSIG might be most useful for dynamic update. A primary server for a dynamic zone should
use access control to control updates, but IP-based access control is insufficient. Key-based
access control is far superior. See RFC 2845 in “Proposed Standards” on page 89 of the
Appendix. The nsupdate program supports TSIG via the “-k” and “-y” command line
options.

4.4.1 Generate Shared Keys for Each Pair of Hosts

A shared secret is generated to be shared between host1 and host2. An arbitrary key
name is chosen: “host1-host2.”. The key name must be the same on both hosts.

4.4.1.1 Automatic Generation

The following command will generate a 128 bit (16 byte) HMAC-MD5
key as described above. Longer keys are better, but shorter keys are easier
to read. Note that the maximum key length is 512 bits; keys longer than
that will be digested with MD5 to produce a 128 bit key.

dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2.

The key is in the file Khost1-host2.+157+00000.private. Nothing directly
uses this file, but the base-64 encoded string following “Key:” can be
extracted from the file and used as a shared secret:

Key: La/E5Cj90+os1jq0a2jdA==

The string “La/E5Cj90+os1jq0a2jdA==” can be used as the shared
secret.

4.4.1.2 Manual Generation

The shared secret is simply a random sequence of bits, encoded in base-
64. Most ASCII strings are valid base-64 strings (assuming the length is a
multiple of 4 and only valid characters are used), so the shared secret can
be manually generated.

Also, a known string can be run through mmencode or a similar program to
generate base-64 encoded data.
4.4.2 Copying the Shared Secret to Both Machines

This is beyond the scope of DNS. A secure transport mechanism should be used. This could be secure FTP, ssh, telephone, etc.

4.4.3 Informing the Servers of the Key’s Existence

Imagine host1 and host2 are both servers. The following is added to each server’s named.conf file:

```plaintext
key host1-host2. {
    algorithm hmac-md5;
    secret "La/E5CjG90+os1jq0a2jdA==";
};
```

The algorithm, hmac-md5, is the only one supported by BIND. The secret is the one generated above. Since this is a secret, it is recommended that either named.conf be non-world readable, or the key directive be added to a non-world-readable file that is included by named.conf.

At this point, the key is recognized. This means that if the server receives a message signed by this key, it can verify the signature. If the signature succeeds, the response is signed by the same key.

4.4.4 Instructing the Server to Use the Key

Since keys are shared between two hosts only, the server must be told when keys are to be used. The following is added to the named.conf file for host1, if the IP address of host2 is 10.1.2.3:

```plaintext
server 10.1.2.3 {
    keys { host1-host2. ;};
};
```

Multiple keys may be present, but only the first is used. This directive does not contain any secrets, so it may be in a world-readable file.

If host1 sends a message that is a response to that address, the message will be signed with the specified key. host1 will expect any responses to signed messages to be signed with the same key.

A similar statement must be present in host2’s configuration file (with host1’s address) for host2 to sign non-response messages to host1.

4.4.5 TSIG Key Based Access Control

BIND allows IP addresses and ranges to be specified in ACL definitions and allow-{ query | transfer | update } directives. This has been extended to allow TSIG keys also. The above key would be denoted key host1-host2.

An example of an allow-update directive would be:
allow-update { key host1-host2. ;};

This allows dynamic updates to succeed only if the request was signed by a key named “host1-host2.”.

The more powerful update-policy statement is described in “Dynamic Update Policies” on page 67.

4.4.6 Errors

The processing of TSIG signed messages can result in several errors. If a signed message is sent to a non-TSIG aware server, a FORMERR will be returned, since the server will not understand the record. This is a result of misconfiguration, since the server must be explicitly configured to send a TSIG signed message to a specific server.

If a TSIG aware server receives a message signed by an unknown key, the response will be unsigned with the TSIG extended error code set to BADKEY. If a TSIG aware server receives a message with a signature that does not validate, the response will be unsigned with the TSIG extended error code set to BADSIG. If a TSIG aware server receives a message with a time outside of the allowed range, the response will be signed with the TSIG extended error code set to BADTIME, and the time values will be adjusted so that the response can be successfully verified. In any of these cases, the message’s rcode is set to NOTAUTH.

4.5 TKEY

TKEY is a mechanism for automatically generating a shared secret between two hosts. There are several “modes” of TKEY that specify how the key is generated or assigned. BIND implements only one of these modes, the Diffie-Hellman key exchange. Both hosts are required to have a Diffie-Hellman KEY record (although this record is not required to be present in a zone). The TKEY process must use signed messages, signed either by TSIG or SIG(0). The result of TKEY is a shared secret that can be used to sign messages with TSIG. TKEY can also be used to delete shared secrets that it had previously generated.

The TKEY process is initiated by a client or server by sending a signed TKEY query (including any appropriate KEYs) to a TKEY-aware server. The server response, if it indicates success, will contain a TKEY record and any appropriate keys. After this exchange, both participants have enough information to determine the shared secret; the exact process depends on the TKEY mode. When using the Diffie-Hellman TKEY mode, Diffie-Hellman keys are exchanged, and the shared secret is derived by both participants.

4.6 SIG(0)

BIND 9 partially supports DNSSEC SIG(0) transaction signatures as specified in RFC 2535. SIG(0) uses public/private keys to authenticate messages. Access control is performed in the same manner as TSIG keys; privileges can be granted or denied based on the key name.
When a SIG(0) signed message is received, it will only be verified if the key is known and trusted by the server; the server will not attempt to locate and/or validate the key.

BIND 9 does not ship with any tools that generate SIG(0) signed messages.

4.7 DNSSEC

Cryptographic authentication of DNS information is possible through the DNS Security (DNSSEC) extensions, defined in RFC 2535. This section describes the creation and use of DNSSEC signed zones.

In order to set up a DNSSEC secure zone, there are a series of steps which must be followed. BIND 9 ships with several tools that are used in this process, which are explained in more detail below. In all cases, the “-h” option prints a full list of parameters. Note that the DNSSEC tools require the keyset and signedkey files to be in the working directory; also note that the tools shipped with BIND 9.0.x are not fully compatible with the current ones.

There must also be communication with the administrators of the parent and/or child zone to transmit keys and signatures. A zone’s security status must be indicated by the parent zone for a DNSSEC capable resolver to trust its data.

For other servers to trust data in this zone, they must either be statically configured with this zone’s zone key or the zone key of another zone above this one in the DNS tree.

4.7.1 Generating Keys

The `dnssec-keygen` program is used to generate keys.

A secure zone must contain one or more zone keys. The zone keys will sign all other records in the zone, as well as the zone keys of any secure delegated zones. Zone keys must have the same name as the zone, a name type of `ZONE`, and must be usable for authentication. It is recommended that zone keys be mandatory to implement a cryptographic algorithm; currently the only key mandatory to implement an algorithm is DSA.

The following command will generate a 768 bit DSA key for the `child.example` zone:

```
dnssec-keygen -a DSA -b 768 -n ZONE child.example.
```

Two output files will be produced: `Kchild.example.+003+12345.key` and `Kchild.example.+003+12345.private` (where 12345 is an example of a key tag). The key file names contain the key name (`child.example.`), algorithm (3 is DSA, 1 is RSA, etc.), and the key tag (12345 in this case). The private key (in the `.private` file) is used to generate signatures, and the public key (in the `.key` file) is used for signature verification.

To generate another key with the same properties (but with a different key tag), repeat the above command.

The public keys should be inserted into the zone file with `$INCLUDE` statements, including the `.key` files.
4.7.2 Creating a Keyset

The `dnssec-makekeyset` program is used to create a key set from one or more keys.

Once the zone keys have been generated, a key set must be built for transmission to the administrator of the parent zone, so that the parent zone can sign the keys with its own zone key and correctly indicate the security status of this zone. When building a key set, the list of keys to be included and the TTL of the set must be specified, and the desired signature validity period of the parent’s signature may also be specified.

The list of keys to be inserted into the key set may also include non-zone keys present at the top of the zone. `dnssec-makekeyset` may also be used at other names in the zone.

The following command generates a key set containing the above key and another key similarly generated, with a TTL of 3600 and a signature validity period of 10 days starting from now.

```
dnssec-makekeyset -t 3600 -e +86400 Kchild.example.+003+12345 Kchild.example.+003+23456
```

One output file is produced: `child.example.keyset`. This file should be transmitted to the parent to be signed. It includes the keys, as well as signatures over the key set generated by the zone keys themselves, which are used to prove ownership of the private keys and encode the desired validity period.

4.7.3 Signing the Child’s Keyset

The `dnssec-signkey` program is used to sign one child’s keyset.

If the `child.example` zone has any delegations which are secure, for example, `grand.child.example`, the `child.example` administrator should receive keyset files for each secure subzone. These keys must be signed by this zone’s zone keys.

The following command signs the child’s key set with the zone keys:

```
dnssec-signkey grand.child.example.keyset Kchild.example.+003+12345 Kchild.example.+003+23456
```

One output file is produced: `signedkey-grand.child.example`. This file should be both transmitted back to the child and retained. It includes all keys (the child’s keys) from the keyset file and signatures generated by this zone’s zone keys.

4.7.4 Signing the Zone

The `dnssec-signzone` program is used to sign a zone.

Any `signedkey` files corresponding to secure subzones should be present, as well as a `signedkey` file for this zone generated by the parent (if there is one). The zone signer will generate `NXT` and `SIG` records for the zone, as well as incorporate the zone key signature from the parent and indicate the security status at all delegation points.
The following command signs the zone, assuming it is in a file called `zone.child.example`. By default, all zone keys which have an available private key are used to generate signatures.

```
dnssec-signzone -o child.example zone.child.example
```

One output file is produced: `zone.child.example.signed`. This file should be referenced by `named.conf` as the input file for the zone.

### 4.7.5 Configuring Servers

Unlike in BIND 8, data is not verified on load in BIND 9, so zone keys for authoritative zones do not need to be specified in the configuration file.

The public key for any security root must be present in the configuration file’s `trusted-keys` statement, as described later in this document.

### 4.8 IPv6 Support in BIND 9

BIND 9 fully supports all currently defined forms of IPv6 name to address and address to name lookups. It will also use IPv6 addresses to make queries when running on an IPv6 capable system.

For forward lookups, BIND 9 supports both A6 and AAAA records. The use of AAAA records is deprecated, but it is still useful for hosts to have both AAAA and A6 records to maintain backward compatibility with installations where AAAA records are still used. In fact, the stub resolvers currently shipped with most operating system support only AAAA lookups, because following A6 chains is much harder than doing A or AAAA lookups.

For IPv6 reverse lookups, BIND 9 supports the new “bitstring” format used in the `ip6.arpa` domain, as well as the older, deprecated “nibble” format used in the `ip6.int` domain.

BIND 9 includes a new lightweight resolver library and resolver daemon which new applications may choose to use to avoid the complexities of A6 chain following and bitstring labels. See “The BIND 9 Lightweight Resolver” on page 27 for more information.

#### 4.8.1 Address Lookups Using AAAA Records

The AAAA record is a parallel to the IPv4 A record. It specifies the entire address in a single record. For example,

```
$ORIGIN example.com.
host 3600 IN AAAA 3ffe:8050:201:1860:42::1
```

While their use is deprecated, they are useful to support older IPv6 applications. They should not be added where they are not absolutely necessary.

#### 4.8.2 Address Lookups Using A6 Records

The A6 record is more flexible than the AAAA record, and is therefore more complicated. The A6 record can be used to form a chain of A6 records, each specifying part of the IPv6 address. It can also be used to specify the entire record
as well. For example, this record supplies the same data as the AAAA record in the previous example:

```
$ORIGIN example.com.
host 3600 IN A6 0 3ffe:8050:201:1860:42::1
```

### 4.8.2.1 A6 Chains

A6 records are designed to allow network renumbering. This works when an A6 record only specifies the part of the address space the domain owner controls. For example, a host may be at a company named “company.” It has two ISPs which provide IPv6 address space for it. These two ISPs fully specify the IPv6 prefix they supply.

In the company’s address space:

```
$ORIGIN example.com.
host 3600 IN A6 64 0:0:0:0:42::1company.example1.net.
host 3600 IN A6 64 0:0:0:0:42::1company.example2.net.
```

ISP1 will use:

```
$ORIGIN example1.net.
company 3600 IN A6 0 3ffe:8050:201:1860::
```

ISP2 will use:

```
$ORIGIN example2.net.
company 3600 IN A6 0 1234:5678:90ab:fffa::
```

When `host.example.com` is looked up, the resolver (in the resolver daemon or caching name server) will find two partial A6 records, and will use the additional name to find the remainder of the data.

### 4.8.2.2 A6 Records for DNS Servers

When an A6 record specifies the address of a name server, it should use the full address rather than specifying a partial address. For example:

```
$ORIGIN example.com.
@ 14400 IN NS ns0
 14400 IN NS ns1
ns0 14400 IN A6 0 3ffe:8050:201:1860:42::1
ns1 14400 IN A 192.168.42.1
```

It is recommended that IPv4-in-IPv6 mapped addresses not be used. If a host has an IPv4 address, use an A record, not an A6, with `::ffff:192.168.42.1` as the address.

### 4.8.3 Address to Name Lookups Using Nibble Format

While the use of nibble format to look up names is deprecated, it is supported for backwards compatibility with existing IPv6 applications.
When looking up an address in nibble format, the address components are simply reversed, just as in IPv4, and `ip6.int.` is appended to the resulting name. For example, the following would provide reverse name lookup for a host with address 3ffe:8050:201:1860:42::1.

```
$ORIGIN 0.6.8.1.1.0.2.0.0.5.0.8.e.f.f.3.ip6.int.
1.0.0.0.0.0.0.0.0.0.0.2.4.0.0 IN 14400  PTR host.example.com.
```

### 4.8.4 Address to Name Lookups Using Bitstring Format

Bitstring labels can start and end on any bit boundary, rather than on a multiple of 4 bits as in the nibble format. They also use `ip6.arpa` rather than `ip6.int`.

To replicate the previous example using bitstrings:

```
$ORIGIN \[x3ffe805002011860/64].ip6.arpa.
\[x0042000000000001/64]14400 IN PTR host.example.com.
```

### 4.8.5 Using DNAME for Delegation of IPv6 Reverse Addresses

In IPv6, the same host may have many addresses from many network providers. Since the trailing portion of the address usually remains constant, `DNAME` can help reduce the number of zone files used for reverse mapping that need to be maintained.

For example, consider a host which has two providers (`example.net` and `example2.net`) and therefore two IPv6 addresses. Since the host chooses its own 64 bit host address portion, the provider address is the only part that changes:

```
$ORIGIN example.com.
host A6 64 ::1234:5678:1212:5675 cust1.example.net.
A6 64 ::1234:5678:1212:5675 subnet5.example2.net.
$ORIGIN example.net.
cust1 A6 48 0:0:0:dddd:: ipv6net.example.net.
ipv6net A6 0 aa:bb:cccc::
$ORIGIN example2.net.
subnet5 A6 48 0:0:0:1:: ipv6net2.example2.net.
ipv6net2A6 0 6666:5555:4::
```

This sets up forward lookups. To handle the reverse lookups, the provider `example.net` would have:

```
$ORIGIN \[x00aa00bbcccc/48].ip6.arpa.
\[xdddd/16] DNAME ipv6-rev.example.com.
```

and `example2.net` would have:

```
$ORIGIN \[x666655550004/48].ip6.arpa.
\[x0001/16] DNAME ipv6-rev.example.com.
```

`example.com` needs only one zone file to handle both of these reverse mappings:

```
$ORIGIN ipv6-rev.example.com.
\[xl234567812125675/64] PTR host.example.com.
```
Section 5. The BIND 9 Lightweight Resolver

5.1 The Lightweight Resolver Library

Traditionally applications have been linked with a stub resolver library that sends recursive DNS queries to a local caching name server.

IPv6 introduces new complexity into the resolution process, such as following A6 chains and DNAME records, and simultaneous lookup of IPv4 and IPv6 addresses. These are hard or impossible to implement in a traditional stub resolver.

Instead, BIND 9 provides resolution services to local clients using a combination of a lightweight resolver library and a resolver daemon process running on the local host. These communicate using a simple UDP-based protocol, the “lightweight resolver protocol” that is distinct from and simpler than the full DNS protocol.

5.2 Running a Resolver Daemon

To use the lightweight resolver interface, the system must run the resolver daemon lwresd.

By default, applications using the lightweight resolver library will make UDP requests to the IPv4 loopback address (127.0.0.1) on port 921. The address can be overridden by lwserver lines in /etc/resolv.conf. The daemon will try to find the answer to the questions “what are the addresses for host foo.example.com?” and “what are the names for IPv4 address 10.1.2.3?”

The daemon currently only looks in the DNS, but in the future it may use other sources such as /etc/hosts, NIS, etc.

The lwresd daemon is essentially a stripped-down, caching-only name server that answers requests using the lightweight resolver protocol rather than the DNS protocol. Because it needs to run on each host, it is designed to require no or minimal configuration. Unless configured otherwise, it uses the name servers listed on nameserver lines in /etc/resolv.conf as forwarders, but is also capable of doing the resolution autonomously if none are specified.

The lwresd daemon may also be configured with a named.conf style configuration file, in /etc/lwresd.conf by default. A name server may also be configured to act as a lightweight resolver daemon using the lwres statement in named.conf.
Section 6. BIND 9 Configuration Reference

BIND 9 configuration is broadly similar to BIND 8.x; however, there are a few new areas of configuration, such as views. BIND 8.x configuration files should work with few alterations in BIND 9, although more complex configurations should be reviewed to check if they can be more efficiently implemented using the new features found in BIND 9.

BIND 4 configuration files can be converted to the new format using the shell script `contrib/named-bootconf/named-bootconf.sh`.

6.1 Configuration File Elements

Following is a list of elements used throughout the BIND configuration file documentation:

- **acl_name**: The name of an `address_match_list` as defined by the `acl` statement.
- **address_match_list**: A list of one or more `ip_addr`, `ip_prefix`, `key_id`, or `acl_name` elements, as described in “Address Match Lists” on page 30.
- **domain_name**: A quoted string which will be used as a DNS name, for example “my.test.domain”.
- **dotted_decimal**: One or more integers valued 0 through 255 separated only by dots (‘.’), such as 123, 45.67 or 89.123.45.67.
- **ip4_addr**: An IPv4 address with exactly four elements in `dotted_decimal` notation.
- **ip6_addr**: An IPv6 address, such as `fe80::200:f8ff:fe01:9742`.
- **ip_addr**: An `ip4_addr` or `ip6_addr`.
- **ip_port**: An IP port `number`. `number` is limited to 0 through 65535, with values below 1024 typically restricted to root-owned processes. In some cases an asterisk (‘*’) character can be used as a placeholder to select a random high-numbered port.
- **ip_prefix**: An IP network specified as an `ip_addr`, followed by a slash (‘/’) and then the number of bits in the netmask. Trailing zeros in an `ip_addr` may be omitted. For example, `127/8` is the network `127.0.0.0` with netmask `255.0.0.0` and `1.2.3.0/28` is network `1.2.3.0` with netmask `255.255.255.240`.
- **key_id**: A `domain_name` representing the name of a shared key, to be used for transaction security.
- **key_list**: A list of one or more `key_ids`, separated by semicolons and ending with a semicolon.
6.1.1 Address Match Lists

6.1.1.1 Syntax

```plaintext
address_match_list = address_match_list_element ;
[ address_match_list_element ; . . . ]
address_match_list_element = [ ! ] ( ip_address / length ) |
key key_id ] acl_name | { address_match_list }
```

6.1.1.2 Definition and Usage

Address match lists are primarily used to determine access control for various server operations. They are also used to define priorities for querying other nameservers and to set the addresses on which named will listen for queries. The elements which constitute an address match list can be any of the following:

- an IP address (IPv4 or IPv6)
- an IP prefix (in the ‘/’-notation)
- a key ID, as defined by the key statement
• the name of an address match list previously defined with the `acl` statement

• a nested address match list enclosed in braces

Elements can be negated with a leading exclamation mark (‘!’) and the match list names “any,” “none,” “localhost” and “localnets” are predefined. More information on those names can be found in the description of the `acl` statement.

The addition of the key clause made the name of this syntactic element something of a misnomer, since security keys can be used to validate access without regard to a host or network address. Nonetheless, the term “address match list” is still used throughout the documentation.

When a given IP address or prefix is compared to an address match list, the list is traversed in order until an element matches. The interpretation of a match depends on whether the list is being used for access control, defining listen-on ports, or as a topology, and whether the element was negated.

When used as an access control list, a non-negated match allows access and a negated match denies access. If there is no match, access is denied. The clauses `allow-query`, `allow-transfer`, `allow-update` and `blackhole` all use address match lists this. Similarly, the listen-on option will cause the server to not accept queries on any of the machine's addresses which do not match the list.

When used with the topology clause, a non-negated match returns a distance based on its position on the list (the closer the match is to the start of the list, the shorter the distance is between it and the server). A negated match will be assigned the maximum distance from the server. If there is no match, the address will get a distance which is further than any non-negated list element, and closer than any negated element.

Because of the first-match aspect of the algorithm, an element that defines a subset of another element in the list should come before the broader element, regardless of whether either is negated. For example, in `1.2.3/24; ! 1.2.3.13;` the 1.2.3.13 element is completely useless because the algorithm will match any lookup for 1.2.3.13 to the 1.2.3/24 element. Using `! 1.2.3.13; 1.2.3/24` fixes that problem by having 1.2.3.13 blocked by the negation but all other 1.2.3.* hosts fall through.

### 6.1.2 Comment Syntax

The BIND 9 comment syntax allows for comments to appear anywhere that white space may appear in a BIND configuration file. To appeal to programmers of all kinds, they can be written in C, C++, or shell/perl constructs.
6.1.2.1 Syntax

/* This is a BIND comment as in C */
// This is a BIND comment as in C++
# This is a BIND comment as in common UNIX shells and perl

6.1.2.2 Definition and Usage

Comments may appear anywhere that whitespace may appear in a BIND configuration file.

C-style comments start with the two characters /* (slash, star) and end with */ (star, slash). Because they are completely delimited with these characters, they can be used to comment only a portion of a line or to span multiple lines.

C-style comments cannot be nested. For example, the following is not valid because the entire comment ends with the first */:

/* This is the start of a comment.
This is still part of the comment.
/* This is an incorrect attempt at nesting a comment. */
This is no longer in any comment. */

C++-style comments start with the two characters // (slash, slash) and continue to the end of the physical line. They cannot be continued across multiple physical lines; to have one logical comment span multiple lines, each line must use the // pair. For example:

// This is the start of a comment. The next line
// is a new comment, even though it is logically
// part of the previous comment.

Shell-style (or perl-style, if you prefer) comments start with the character # (number sign) and continue to the end of the physical line, as in C++ comments. For example:

# This is the start of a comment. The next line
# is a new comment, even though it is logically
# part of the previous comment.

WARNING: you cannot use the semicolon (‘;’) character to start a comment such as you would in a zone file. The semicolon indicates the end of a configuration statement.

6.2 Configuration File Grammar

A BIND 9 configuration consists of statements and comments. Statements end with a semicolon. Statements and comments are the only elements that can appear without
enclosing braces. Many statements contain a block of substatements, which are also terminated with a semicolon.

The following statements are supported:

- **acl** defines a named IP address matching list, for access control and other uses.
- **controls** declares control channels to be used by the **rndc** utility.
- **include** includes a file.
- **key** specifies key information for use in authentication and authorization using TSIG.
- **logging** specifies what the server logs, and where the log messages are sent.
- **options** controls global server configuration options and sets defaults for other statements.
- **server** sets certain configuration options on a per-server basis.
- **trusted-keys** defines trusted DNSSEC keys.
- **view** defines a view.
- **zone** defines a zone.

The **logging** and **options** statements may only occur once per configuration.

### 6.2.1 acl Statement Grammar

```plaintext
acl acl-name {
  address_match_list
};
```

### 6.2.2 acl Statement Definition and Usage

The acl statement assigns a symbolic name to an address match list. It gets its name from a primary use of address match lists: Access Control Lists (ACLs).

Note that an address match list’s name must be defined with acl before it can be used elsewhere; no forward references are allowed.

The following ACLs are built-in:

- **any** Matches all hosts.
- **none** Matches no hosts.
- **localhost** Matches the IP addresses of all interfaces on the system.
6.2.3 controls Statement Grammar

controls {
  inet ( ip_addr | * ) [ port ip_port ] allow address_match_list
    keys key_list ;
  [ inet ...; ]
} ;

6.2.4 controls Statement Definition and Usage

The controls statement declares control channels to be used by system administrators to affect the operation of the local nameserver. These control channels are used by the rndc utility to send commands to and retrieve non-DNS results from a nameserver.

An inet control channel is a TCP/IP socket accessible to the Internet, created at the specified ip_port on the specified ip_addr. If no port is specified, port 953 is used by default. "*" cannot be used for ip_port.

The ability to issue commands over the control channel is restricted by the allow and keys clauses. Connections to the control channel are permitted based on the address permissions in address_match_list. key_id members of the address_match_list are ignored, and instead are interpreted independently based the key_list. Each key_id in the key_list is allowed to be used to authenticate commands and responses given over the control channel by digitally signing each message between the server and a command client (see “rndc” on page 12). All commands to the control channel must be signed by one of its specified keys to be honored.

The UNIX control channel type of BIND 8 is not supported in BIND 9.0.0, and is not expected to be added in future releases. If it is present in the controls statement from a BIND 8 configuration file, a non-fatal warning will be logged.

6.2.5 include Statement Grammar

include filename;

6.2.6 include Statement Definition and Usage

The include statement inserts the specified file at the point that the include statement is encountered. The include statement facilitates the administration of configuration files by permitting the reading or writing of some things but not others. For example, the statement could include private keys that are readable only by a nameserver.
6.2.7 **key Statement Grammar**

```
key key_id {
  algorithm string;
  secret string;
};
```

6.2.8 **key Statement Definition and Usage**

The `key` statement defines a shared secret key for use with TSIG. See Section 4.4, “TSIG”, on page 19.

The `key_id`, also known as the key name, is a domain name uniquely identifying the key. It can be used in a “server” statement to cause requests sent to that server to be signed with this key, or in address match lists to verify that incoming requests have been signed with a key matching this name, algorithm, and secret.

The `algorithm_id` is a string that specifies a security/authentication algorithm. The only algorithm currently supported with TSIG authentication is `hmac-md5`. The `secret_string` is the secret to be used by the algorithm, and is treated as a base-64 encoded string.

6.2.9 **logging Statement Grammar**

```
logging {
  channel channel_name {
    ( file path name
       [ versions ( number | unlimited ) ]
       [ size size spec ]
       | syslog ( syslog_facility )
       | null );
    [ severity (critical | error | warning | notice | info | debug [ level ] | dynamic ); ]
    [ print-category yes or no; ]
    [ print-severity yes or no; ]
    [ print-time yes or no; ]
  );
  [ category category_name {
    channel_name ; [ category_name ; ... ]
  });
}...
```

6.2.10 **logging Statement Definition and Usage**

The `logging` statement configures a wide variety of logging options for the nameserver. Its `channel` phrase associates output methods, format options and severity levels with a name that can then be used with the `category` phrase to select how various classes of messages are logged.
Only one `logging` statement is used to define as many channels and categories as are wanted. If there is no `logging` statement, the logging configuration will be:

```plaintext
logging {
    category "default" { "default_syslog"; "default_debug"; };
};
```

In BIND 9, the logging configuration is only established when the entire configuration file has been parsed. In BIND 8, it was established as soon as the `logging` statement was parsed. When the server is starting up, all logging messages regarding syntax errors in the configuration file go to the default channels, or to standard error if the "-g" option was specified.

### 6.2.10.1 The `channel` Phrase

All log output goes to one or more `channels`; you can make as many of them as you want.

Every channel definition must include a clause that says whether messages selected for the channel go to a file, to a particular syslog facility, to the standard error stream, or are discarded. It can optionally also limit the message severity level that will be accepted by the channel (the default is `info`), and whether to include a `named`-generated time stamp, the category name and/or severity level (the default is not to include any).

The word `null` as the destination option for the channel will cause all messages sent to it to be discarded; in that case, other options for the channel are meaningless.

The `file` destination clause directs the channel to a disk file. It can include limitations both on how large the file is allowed to become, and how many versions of the file will be saved each time the file is opened.

The `size` option for files is simply a hard ceiling on log growth. If the file ever exceeds the size, then `named` will not write anything more to it until the file is reopened; exceeding the size does not automatically trigger a reopen. The default behavior is not to limit the size of the file.

If you use the `version` log file option, then `named` will retain that many backup versions of the file by renaming them when opening. For example, if you choose to keep 3 old versions of the file `lamers.log` then just before it is opened `lamers.log.1` is renamed to `lamers.log.2`, `lamers.log.0` is renamed to `lamers.log.1`, and `lamers.log` is renamed to `lamers.log.0`. No rolled versions are kept by default; any existing log file is simply appended. The `unlimited` keyword is synonymous with 99 in current BIND releases.

Example usage of the size and versions options:
channel "an_example_channel" {
    file "example.log" versions 3 size 20m;
    print-time yes;
    print-category yes;
};

The syslog destination clause directs the channel to the system log. Its argument is a syslog facility as described in the syslog man page. How syslog will handle messages sent to this facility is described in the syslog.conf man page. If you have a system which uses a very old version of syslog that only uses two arguments to the openlog() function, then this clause is silently ignored.

The severity clause works like syslog’s “priorities,” except that they can also be used if you are writing straight to a file rather than using syslog. Messages which are not at least of the severity level given will not be selected for the channel; messages of higher severity levels will be accepted.

If you are using syslog, then the syslog.conf priorities will also determine what eventually passes through. For example, defining a channel facility and severity as daemon and debug but only logging daemon.warning via syslog.conf will cause messages of severity info and notice to be dropped. If the situation were reversed, with named writing messages of only warning or higher, then syslogd would print all messages it received from the channel.

The stderr destination clause directs the channel to the server’s standard error stream. This is intended for use when the server is running as a foreground process, for example when debugging a configuration.

The server can supply extensive debugging information when it is in debugging mode. If the server’s global debug level is greater than zero, then debugging mode will be active. The global debug level is set either by starting the named server with the “-d” flag followed by a positive integer, or by running rndc trace

(Note: the latter method is not yet implemented).

The global debug level can be set to zero, and debugging mode turned off, by running ndc notrace. All debugging messages in the server have a debug level, and higher debug levels give more detailed output. Channels that specify a specific debug severity, for example:

channel "specific_debug_level" {
    file "foo";
    severity debug 3;
};

will get debugging output of level 3 or less any time the server is in debugging mode, regardless of the global debugging level. Channels with
**dynamic** severity use the server's global level to determine what messages to print.

If **print-time** has been turned on, then the date and time will be logged. **print-time** may be specified for a **syslog** channel, but is usually pointless since **syslog** also prints the date and time. If **print-category** is requested, then the category of the message will be logged as well. Finally, if **print-severity** is on, then the severity level of the message will be logged. The **print-** options may be used in any combination, and will always be printed in the following order: time, category, severity. Here is an example where all three **print-** options are on:

```
28-Feb-2000 15:05:32.863 general: notice: running
```

There are four predefined channels that are used for **named**’s default logging as follows. How they are used is described in “The category Phrase” on page 39.

```
channel "default_syslog" {  
  syslog daemon; // end to syslog's daemon  
    // facility  
  severity info; // only send priority info  
    // and higher
};
channel "default_debug" {  
  file "named.run"; // write to named.run in  
    // the working directory  
    // Note: stderr is used instead  
    // of "named.run"  
    // if the server is started  
    // with the '-f' option.  
  severity dynamic // log at the server's  
    // current debug level
};
channel "default_stderr" {  
  stderr;  
  severity info; // only send priority info  
    // and higher
};
channel "null" {  
  null;  
    // toss anything sent to  
    // this channel
};
```

The **default_debug** channel normally writes to a file **named.run** in the server’s working directory. For security reasons, when the “-u” command line option is used, the **named.run** file is created only after **named** has changed to the new UID, and any debug output generated while **named** is starting up and still running as root is discarded. If you need to capture this output, you must run the server with the “-g” option and redirect standard error to a file.
Once a channel is defined, it cannot be redefined. Thus you cannot alter the built-in channels directly, but you can modify the default logging by pointing categories at channels you have defined.

### 6.2.10.2 The category Phrase

There are many categories, so you can send the logs you want to see wherever you want, without seeing logs you don’t want. If you don’t specify a list of channels for a category, then log messages in that category will be sent to the `default` category instead. If you don’t specify a default category, the following “default default” is used:

```plaintext
category "default" { "default_syslog"; "default_debug"; }
```

As an example, let’s say you want to log security events to a file, but you also want keep the default logging behavior. You'd specify the following:

```plaintext
channel "my_security_channel" {
    file "my_security_file";
    severity info;
};
category "security" {
    "my_security_channel";
    "default_syslog";
    "default_debug";
};
```

To discard all messages in a category, specify the `null` channel:

```plaintext
category "xfer-out" { "null"; }
category "notify" { "null"; }
```

Following are the available categories and brief descriptions of the types of log information they contain. More categories may be added in future BIND releases.

- **default**
  The default category defines the logging options for those categories where no specific configuration has been defined.

- **general**
  The catch-all. Many things still aren’t classified into categories, and they all end up here.

- **database**
  Messages relating to the databases used internally by the name server to store zone and cache data.

- **security**
  Approval and denial of requests.

- **config**
  Configuration file parsing and processing.

- **resolver**
  DNS resolution, such as the recursive lookups performed on behalf of clients by a caching name server.

- **xfer-in**
  Zone transfers the server is receiving.

- **xfer-out**
  Zone transfers the server is sending.

- **notify**
  The NOTIFY protocol.
6.2.11 lwres Statement Grammar

This is the grammar of the lwres statement in the named.conf file:

```
lwres {
    [ listen-on {address_match_list }; ]
    [ view view_name; ]
    [ search {domain_name ; [ ip_addr ; . . . ]}; ]
    [ ndots number; ]
};
```

6.2.12 lwres Statement Definition and Usage

The lwres statement configures the name server to also act as a lightweight resolver server. (See “The BIND 9 Lightweight Resolver” on page 27.) There may be multiple lwres statements configuring lightweight resolver servers with different properties.

The listen-on statement specifies a list of addresses (and ports) on which this instance of a lightweight resolver daemon should accept requests. If this statement is omitted, requests will be accepted on 127.0.0.1, port 53.

The view statement binds this instance of a lightweight resolver daemon to a view in the DNS namespace, so that the response will be constructed in the same manner as a normal DNS query matching this view. If this statement is omitted, the default view is used, and if there is no default view, an error is triggered.

The search statement is equivalent to the search statement in /etc/resolv.conf. It provides a list of domains which are appended to relative names in queries.

The ndots dstatement is equivalent to the ndots statement in /etc/resolv.conf. It indicates the minimum number of dots in a relative domain name that should result in an exact match lookup before the search path elements are appended.

6.2.13 options Statement Grammar

This is the grammar of the option statement in the named.conf file:

```
options {
    [ version version_string; ]
    [ directory path_name; ]
    [ named-xfer path_name; ]
    [ tkey-domain domainname; ]
    [ tkey-dhkey key_name key_tag; ]
    [ dump-file path_name; ]
    [ memstatistics-file path_name; ]
```
[ pid-file path_name; ]
[ statistics-file path_name; ]
[ zone-statistics yes_or_no; ]
[ auth-nxdomain yes_or_no; ]
[ deallocate-on-exit yes_or_no; ]
[ dialup yes_or_no; ]
[ fake-iquery yes_or_no; ]
[ fetch-glue yes_or_no; ]
[ has-old-clients yes_or_no; ]
[ host-statistics yes_or_no; ]
[ multiple-cnames yes_or_no; ]
[ notify yes_or_no | explicit; ]
[ recursion yes_or_no; ]
[ rfc2308-type1 yes_or_no; ]
[ use-id-pool yes_or_no; ]
[ maintain-ixfr-base yes_or_no; ]
[ forward ( only | first ); ]
[ forwarders { [ in addr ; [ in addr ; ... ] ] }; ]
[ check-names ( master | slave | response ) ( warn | fail | ignore ); ]
[ allow-query { address_match_list }; ]
[ allow-transfer { address_match_list }; ]
[ allow-recursion { address_match_list }; ]
[ blackhole { address_match_list }; ]
[ listen-on { port ip_port } { address_match_list }; ]
[ listen-on-v6 { port ip_port } { address_match_list }; ]
[ query-source { address ( ip addr | * ) | port ( ip_port | * ) } ]; ]
[ max-transfer-time-in number; ]
[ max-transfer-time-out number; ]
[ max-transfer-idle-in number; ]
[ max-transfer-idle-out number; ]
[ tcp-clients number; ]
[ recursive-clients number; ]
[ serial-queries number; ]
[ transfer-format ( one-answer | many-answers ); ]
[ transfers-in number; ]
[ transfers-out number; ]
[ transfers-per-ns number; ]
[ transfer-source ( ip4_addr | * ) | port ip_port ] ;]
[ transfer-source-v6 ( ip6_addr | * ) | port ip_port ] ;]
[ notify-source ( ip4_addr | * ) | port ip_port ] ;]
[ notify-source-v6 ( ip6_addr | * ) | port ip_port ] ;]
[ also-notify { ip_addr | port ip_port; [ ip_addr | port ip_port; ... ] } ];]
[ max-ixfr-log-size number; ]
[ coresize size_spec ; ]
[ datasize size_spec ; ]
[ files size_spec ; ]
[ stacksize size_spec ; ]
[ cleaning-interval number; ]
[ heartbeat-interval number; ]
[ interface-interval number; ]
[ statistics-interval number; ]
[ topology { address_match_list }; ]
[ sortlist { address_match_list }; ]
[ rrset-order { order_spec ; [ order_spec ; ... ] } ];]
[ lame-ttl number; ]
[ max-ncache-ttl number; ]
[ max-cache-ttl number; ]
[ sig-validity-interval number ; ]
The `options` statement sets up global options to be used by BIND. This statement may appear only once in a configuration file. If more than one occurrence is found, the first occurrence determines the actual options used, and a warning will be generated. If there is no `options` statement, an options block with each option set to its default will be used.

**version**

The version the server should report via a query of name `version.bind` in class `chaos`. The default is the real version number of this server.

**directory**

The working directory of the server. Any non-absolute pathnames in the configuration file will be taken as relative to this directory. The default location for most server output files (e.g. `named.run`) is this directory. If a directory is not specified, the working directory defaults to `.` (the directory from which the server was started). The directory specified should be an absolute path.

**named-xfer**

*This option is obsolete.* It was used in BIND 8 to specify the pathname to the `named-xfer` program. In BIND 9, no separate `named-xfer` program is needed; its functionality is built into the name server.

**tkey-domain**

The domain appended to the names of all shared keys generated with `TKEY`. When a client requests a `TKEY` exchange, it may or may not specify the desired name for the key. If present, the name of the shared key will be "`client specified part` + "tkey-domain". Otherwise, the name of the shared key will be "`random hex digits` + "tkey-domain". In most cases, the `domainname` should be the server’s domain name.
tkey-dhkey

The Diffie-Hellman key used by the server to generate shared keys with clients using the Diffie-Hellman mode of TKEY. The server must be able to load the public and private keys from files in the working directory. In most cases, the keyname should be the server’s host name.

dump-file

The pathname of the file the server dumps the database to when instructed to do so with `rndc dumpdb`. If not specified, the default is `named_dump.db`. Note: Not yet implemented in BIND 9.

memstatistics-file

The pathname of the file the server writes memory usage statistics to on exit. If not specified, the default is `named.memstats`. Not yet implemented in BIND 9.

pid-file

The pathname of the file the server writes its process ID in. If not specified, the default is operating system dependent, but is usually `/var/run/named.pid` or `/etc/named.pid`. The pid-file is used by programs that want to send signals to the running nameserver.

statistics-file

The pathname of the file to which the server appends statistics when instructed to do so using `rndc stats`. If not specified, the default is `named.stats` in the server’s current directory. The format of the file is described in “The Statistics File” on page 58.

port

The UDP/TCP port number the server uses for receiving and sending DNS protocol traffic. The default is 53. This option is mainly intended for server testing; a server using a port other than 53 will not be able to communicate with the global DNS. The `port` option should be placed at the beginning of the options block, before any other options that take port numbers or IP addresses, to ensure that the port value takes effect for all addresses used by the server.
6.2.14.1 Boolean Options

auth-nxdomain
If yes, then the AA bit is always set on NXDOMAIN responses, even if the server is not actually authoritative. The default is no; this is a change from BIND 8. If you are using very old DNS software, you may need to set it to yes.

deallocate-on-exit
This option was used in BIND 8 to enable checking for memory leaks on exit. BIND 9 ignores the option and always performs the checks.

dialup
If yes, then the server treats all zones as if they are doing zone transfers across a dial on demand dialup link, which can be brought up by traffic originating from this server. This has different effects according to zone type and concentrates the zone maintenance so that it all happens in a short interval, once every heartbeat-interval and hopefully during the one call. It also suppresses some of the normal zone maintenance traffic. The default is no.

The dialup option may also be specified in the view and zone statements, in which case it overrides the global dialup option.

If the zone is a master zone, then the server will send out a NOTIFY request to all the slaves. This will trigger the zone serial number check in the slave (providing it supports NOTIFY) allowing the slave to verify the zone while the connection is active.

If the zone is a slave or stub, then the server will suppress the regular “zone up to date” (refresh) queries and only perform them when the heartbeat-interval expires in addition to sending NOTIFY requests.

Finer control can be achieved by using notify, which only sends NOTIFY messages; notify-passive, which sends NOTIFY messages and suppresses the normal refresh queries; refresh, which suppresses normal refresh processing and sends refresh queries when the heartbeat-interval expires; and passive, which just disables normal refresh processing.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fake-iquery</td>
<td>In BIND 8, this option was used to enable simulating the obsolete DNS query type IQUERY. BIND 9 never does IQUERY simulation.</td>
</tr>
<tr>
<td>fetch-glue</td>
<td>This option is obsolete. In BIND 8, <code>fetch-glue yes</code> caused the server to attempt to fetch glue resource records it didn't have when constructing the additional data section of a response. (Information present outside of the authoritative nodes in the zone is called glue information). This is now considered a bad idea and BIND 9 never does it.</td>
</tr>
<tr>
<td>has-old-clients</td>
<td>This option was incorrectly implemented in BIND 8, and is ignored by BIND 9. To achieve the intended effect of <code>has-old-clients yes</code>, specify the two separate options <code>auth-nxdomain yes</code> and <code>rfc2308-typel no</code> instead.</td>
</tr>
<tr>
<td>host-statistics</td>
<td>In BIND 8, this enables keeping of statistics for every host with which the nameserver interacts.</td>
</tr>
<tr>
<td></td>
<td>Not yet implemented in BIND 9.</td>
</tr>
<tr>
<td>maintain-ixfr-base</td>
<td>This option is obsolete. It was used in BIND 8 to determine whether a transaction log was kept for Incremental Zone Transfer. BIND 9 maintains a transaction log whenever possible. If you need to disable outgoing incremental zone transfers, use <code>provide-ixfr no</code>.</td>
</tr>
<tr>
<td>multiple-cnames</td>
<td>This option was used in BIND 8 to allow a domain name to allow multiple CNAME records in violation of the DNS standards. BIND 9.1 always strictly enforces the CNAME rules both in master files and dynamic updates.</td>
</tr>
</tbody>
</table>
**notify**

If **yes** (the default), DNS NOTIFY messages are sent when a zone the server is authoritative for changes. See Section 3.3, “Notify”, on page 10, for more information. The messages are sent to the servers listed in the zone’s NS records (except the master server identified in the SOA MNAME field), and to any servers listed in the **also-notify** option.

If **explicit**, notifies are sent only to servers explicitly listed using **also-notify**. If **no**, no notifies are sent.

The **notify** option may also be specified in the **zone** statement, in which case it overrides the **options notify** statement. It would only be necessary to turn off this option if it caused slaves to crash.

**recursion**

If **yes**, and a DNS query requests recursion, then the server will attempt to do all the work required to answer the query. If recursion is off and the server does not already know the answer, it will return a referral response. The default is **yes**. Note that setting **recursion no** does not prevent clients from getting data from the server’s cache; it only prevents new data from being cached as an effect of client queries. Caching may still occur as an effect of the server’s internal operation, such as NOTIFY address lookups. See also **fetch-glue** above.

**rfc2308-type1**

Setting this to **yes** will cause the server to send NS records along with the SOA record for negative answers. The default is **no**. Not yet implemented in BIND 9.

**use-id-pool**

This option is obsolete. BIND 9 always allocates query IDs from a pool.

**zone-statistics**

If **yes**, the server will, by default, collect statistical data on all zones in the server. These statistics may be accessed using **rndc stats**, which will dump them to the file listed in the **statistics-file**. See also “The Statistics File” on page 58.

**use-ixfr**

This option is obsolete. If you need to disable IXFR to a particular server or servers, see the information on the **provide-ixfr** option in the “server Statement Definition and Usage” on page 59. See also “Incremental Zone Transfers (IXFR)” on page 15.
treat-cr-as-space

This option was used in BIND 8 to make the server treat carriage return ("\r") characters the same way as a space or tab character or to facilitate loading of zone files on a UNIX system that were generated on an NT or DOS machine. In BIND 9, both UNIX "\n" and NT/DOS "\r\n" newlines are always accepted, and the option is ignored.

min-refresh-time

max-refresh-time

min-retry-time

max-retry-time

These options control the server’s behavior on refreshing a zone (querying for SOA changes or retrying failed transfers. Usually the SOA values for the zone are used, but these values are set by the master, giving the slave server administrators little control over their contents. They allow the administrator to set a minimum and maximum refresh and retry time either per-zone, per-view, or per-server. These options are valid for master, slave and stub zones, and clamp the SOA refresh and retry times to the specified values.

additional-from-auth

These options control the server’s behavior when answering queries which have additional data or when following CNAME and DNAME chains to provide additional data. When both of these options are set to yes (the default) and a query is being answered from authoritative data (a zone configured into the server), the additional data section of the reply will be filled in using data from other authoritative zones and from the cache. In some situations this is undesirable, such as when there is concern over the correctness of the cache, or in servers where slave zones may be added and modified by untrusted third parties. Also, avoiding the search for this additional data will speed up server operations at the possible expense of additional queries to resolve what would otherwise be provided in the additional section.

For example, if a query asks for an MX record for host foo.example.com, and the record found is “MX 10 mail.example.net”, normally the address records (A, A6, and AAAA) for mail.example.net will be provided as well, if known. These options disable that behavior.
6.2.14.2 Forwarding

The forwarding facility can be used to create a large site-wide cache on a few servers, reducing traffic over links to external nameservers. It can also be used to allow queries by servers that do not have direct access to the Internet, but wish to look up exterior names anyway. Forwarding occurs only on those queries for which the server is not authoritative and does not have the answer in its cache.

forward This option is only meaningful if the forwarders list is not empty. A value of first, the default, causes the server to query the forwarders first, and if that doesn't answer the question the server will then look for the answer itself. If only is specified, the server will only query the forwarders.

forwarders Specifies the IP addresses to be used for forwarding. The default is the empty list (no forwarding).

Forwarding can also be configured on a per-domain basis, allowing for the global forwarding options to be overridden in a variety of ways. You can set particular domains to use different forwarders, or have a different forward only/first behavior, or not forward at all. See “zone Statement Grammar” on page 61 for more information.

6.2.14.3 Access Control

Access to the server can be restricted based on the IP address of the requesting system. See “Address Match Lists” on page 30 for details on how to specify IP address lists.

allow-query Specifies which hosts are allowed to ask ordinary questions. allow-query may also be specified in the zone statement, in which case it overrides the options allow-query statement. If not specified, the default is to allow queries from all hosts.

allow-recursion Specifies which hosts are allowed to make recursive queries through this server. If not specified, the default is to allow recursive queries from all hosts. Note that disallowing recursive queries for a host does not prevent the host from retrieving data that is already in the server’s cache.
allow-transfer

Specifies which hosts are allowed to receive zone transfers from the server. allow-transfer may also be specified in the zone statement, in which case it overrides the options allow-transfer statement. If not specified, the default is to allow transfers from all hosts.

blackhole

Specifies a list of addresses that the server will not accept queries from or use to resolve a query. Queries from these addresses will not be responded to. The default is none. Not yet implemented in BIND 9.

6.2.14.4 Interfaces

The interfaces and ports that the server will answer queries from may be specified using the listen-on option. listen-on takes an optional port, and an address_match_list. The server will listen on all interfaces allowed by the address match list. If a port is not specified, port 53 will be used.

Multiple listen-on statements are allowed. For example,

listen-on { 5.6.7.8; };
listen-on port 1234 { !1.2.3.4; 1.2/16; };

will enable the nameserver on port 53 for the IP address 5.6.7.8, and on port 1234 of an address on the machine in net 1.2 that is not 1.2.3.4.

If no listen-on is specified, the server will listen on port 53 on all interfaces.

The listen-on-v6 option is used to specify the ports on which the server will listen for incoming queries sent using IPv6.

The server does not bind a separate socket to each IPv6 interface address as it does for IPv4. Instead, it always listens on the IPv6 wildcard address. Therefore, the only values allowed for the address_match_list argument to the listen-on-v6 statement are "{ any; }" and "{ none; }".

Multiple listen-on-v6 options can be used to listen on multiple ports:

listen-on-v6 port 53 { any; };
listen-on-v6 port 1234 { any; };

To make the server not listen on any IPv6 address, use

listen-on-v6 { none; };

If no listen-on-v6 statement is specified, the server will not listen on any IPv6 address.
6.2.14.5 Query Address

If the server doesn't know the answer to a question, it will query other nameservers. **query-source** specifies the address and port used for such queries. For queries sent over IPv6, there is a separate **query-source-v6** option. If **address** is * or is omitted, a wildcard IP address (INADDR_ANY) will be used. If **port** is * or is omitted, a random unprivileged port will be used. The defaults are

```plaintext
query-source address * port *
query-source-v6 address * port *
```

Note: **query-source** currently applies only to UDP queries; TCP queries always use a wildcard IP address and a random unprivileged port.

6.2.14.6 Zone Transfers

BIND has mechanisms in place to facilitate zone transfers and set limits on the amount of load that transfers place on the system. The following options apply to zone transfers.

- **also-notify**
  
  Defines a global list of IP addresses that are also sent NOTIFY messages whenever a fresh copy of the zone is loaded, in addition to the servers listed in the zone's NS records. This helps to ensure that copies of the zones will quickly converge on stealth servers. If an **also-notify** list is given in a **zone** statement, it will override the options **also-notify** statement. When a **zone notify** statement is set to **no**, the IP addresses in the global **also-notify** list will not be sent NOTIFY messages for that zone. The default is the empty list (no global notification list).

- **max-transfer-time-in**
  
  Inbound zone transfers running longer than this many minutes will be terminated. The default is 120 minutes (2 hours).

- **max-transfer-idle-in**
  
  Inbound zone transfers making no progress in this many minutes will be terminated. The default is 60 minutes (1 hour).

- **max-transfer-time-out**
  
  Outbound zone transfers running longer than this many minutes will be terminated. The default is 120 minutes (2 hours).
max-transfer-idle-out

Outbound zone transfers making no progress in this many minutes will be terminated. The default is 60 minutes (1 hour).

serial-queries

Slave servers will periodically query master servers to find out if zone serial numbers have changed. Each such query uses a minute amount of the slave server’s network bandwidth, but more importantly each query uses a small amount of memory in the slave server while waiting for the master server to respond. In BIND 8, the serial-queries option sets the maximum number of concurrent serial-number queries allowed to be outstanding at any given time. BIND 9 does not limit the number of outstanding serial queries and ignores the serial-queries option; instead, it limits the rate at which the queries are sent. The maximum rate is currently fixed at 20 queries per second but may become configurable in a future release.

transfer-format

The server supports two zone transfer methods. one-answer uses one DNS message per resource record transferred. many-answers packs as many resource records as possible into a message. many-answers is more efficient, but is only known to be understood by BIND 9, BIND 8.x and patched versions of BIND 4.9.5. The default is many-answers. transfer-format may be overridden on a per-server basis by using the server statement.

transfers-in

The maximum number of inbound zone transfers that can be running concurrently. The default value is 10. Increasing transfers-in may speed up the convergence of slave zones, but it also may increase the load on the local system.

transfers-out

The maximum number of outbound zone transfers that can be running concurrently. Zone transfer requests in excess of the limit will be refused. The default value is 10.
6.2.14.7 Resource Limits

The server’s usage of many system resources can be limited. Some operating systems don’t support some of the limits. On such systems, a warning will be issued if the unsupported limit is used. Some operating systems don’t support limiting resources.

Scaled values are allowed when specifying resource limits. For example, 1G can be used instead of 1073741824 to specify a limit of one gigabyte. unlimited requests unlimited use, or the maximum available amount. default uses the limit that was in force when the server was started. See the description of size_spec in “Configuration File Elements” on page 29 for more details.

transfers-per-ns

The maximum number of inbound zone transfers that can be concurrently transferring from a given remote nameserver. The default value is 2. Increasing transfers-per-ns may speed up the convergence of slave zones, but it also may increase the load on the remote nameserver. transfers-per-ns may be overridden on a per-server basis by using the transfers phrase of the server statement.

transfer-source

transfer-source determines which local address will be bound to IPv4 TCP connections used to fetch zones transferred inbound by the server. It also determines the source IPv4 address, and optionally the UDP port, used for the refresh queries and forwarded dynamic updates. If not set, it defaults to a system controlled value which will usually be the address of the interface “closest to” the remote end. This address must appear in the remote end’s allow-transfer option for the zone being transferred, if one is specified. This statement sets the transfer-source for all zones, but can be overridden on a per-view or per-zone basis by including a transfer-source statement within the view or zone block on the configuration file.

transfer-source-v6

The same as transfer-source, except zone transfers are performed using IPv6.
Resource limits are not yet implemented in BIND 9.

6.2.14.8 Periodic Task Intervals

cleaning-interval The server will remove expired resource records from the cache every cleaning-interval minutes. The default is 60 minutes. If set to 0, no periodic cleaning will occur.
heartbeat-interval  The server will perform zone maintenance
tasks for all zones marked dialup yes
whenever this interval expires. The default is
60 minutes. Reasonable values are up to 1
day (1440 minutes). If set to 0, no zone
maintenance for these zones will occur. Not
yet implemented in BIND 9.

interface-interval  The server will scan the network interface
list every interface-interval minutes.
The default is 60 minutes. If set to 0,
interface scanning will only occur when the
configuration file is loaded. After the scan,
listeners will be started on any new
interfaces (provided they are allowed by the
listen-on configuration). Listeners on
interfaces that have gone away will be
cleaned up.

statistics-interval  Nameserver statistics will be logged every
statistics-interval minutes. The default
is 60. If set to 0, no statistics will be logged.
Not yet implemented in BIND 9.

6.2.14.9  Topology

All other things being equal, when the server chooses a nameserver to
query from a list of nameservers, it prefers the one that is topologically
closest to itself. The topology statement takes an address_match_list
and interprets it in a special way. Each top-level list element is assigned a
distance. Non-negated elements get a distance based on their position in
the list, where the closer the match is to the start of the list, the shorter the
distance is between it and the server. A negated match will be assigned
the maximum distance from the server. If there is no match, the address
will get a distance which is further than any non-negated list element, and
closer than any negated element. For example,

```
topology {
    10/8;
    !1.2.3/24;
    { 1.2/16; 3/8; };
};
```

will prefer servers on network 10 the most, followed by hosts on network
1.2.0.0 (netmask 255.255.0.0) and network 3, with the exception of hosts
on network 1.2.3 (netmask 255.255.255.0), which is preferred least of all.

The default topology is
```
topology { localhost; localnets; }
```

The topology option is not yet implemented in BIND 9.
6.2.14.10 The sortlist Statement

Resource Records (RRs) are the data associated with the names in a domain name space. The data is maintained in the form of sets of RRs. The order of RRs in a set is, by default, not significant. Therefore, to control the sorting of records in a set of resource records, or RRset, you must use the sortlist statement.

RRs are explained more fully in Section 6.3.1, “Types of Resource Records and When to Use Them”, on page 68. Specifications for RRs are documented in RFC 1035.

When returning multiple RRs the nameserver will normally return them in Round Robin order, that is, after each request the first RR is put at the end of the list. The client resolver code should rearrange the RRs as appropriate, that is, using any addresses on the local net in preference to other addresses. However, not all resolvers can do this or are correctly configured. When a client is using a local server the sorting can be performed in the server, based on the client’s address. This only requires configuring the nameservers, not all the clients.

The sortlist statement (see below) takes an address_match_list and interprets it even more specifically than the topology statement does (see “Topology” on page 54). Each top level statement in the sortlist must itself be an explicit address_match_list with one or two elements. The first element (which may be an IP address, an IP prefix, an ACL name or an established address_match_list) of each top level list is checked against the source address of the query until a match is found.

Once the source address of the query has been matched, if the top level statement contains only one element, the actual primitive element that matched the source address is used to select the address in the response to move to the beginning of the response. If the statement is a list of two elements, then the second element is treated the same as the address_match_list in a topology statement. Each top level element is assigned a distance and the address in the response with the minimum distance is moved to the beginning of the response.

In the following example, any queries received from any of the addresses of the host itself will get responses preferring addresses on any of the locally connected networks. Next most preferred are addresses on the 192.168.1/24 network, and after that either the 192.168.2/24 or 192.168.3/24 network with no preference shown between these two networks. Queries received from a host on the 192.168.1/24 network will prefer other addresses on that network to the 192.168.2/24 and 192.168.3/24 networks. Queries received from a host on the 192.168.4/24 or the 192.168.5/24 network will only prefer other addresses on their directly connected networks.

```
sortlist {
    { localhost;       // IF the local host
    ...
```
{ localnets; // THEN first fit on the
  192.168.1/24; // following nets
  { 192.168.2/24; 192.168.3/24; }; };
{ 192.168.1/24; // IF on class C 192.168.1
  { 192.168.1/24; // THEN use .1, or .2 or .3
    { 192.168.2/24; 192.168.3/24; }; };
{ 192.168.2/24; // IF on class C 192.168.2
  { 192.168.2/24; // THEN use .2, or .1 or .3
    { 192.168.1/24; 192.168.3/24; }; };
{ 192.168.3/24; // IF on class C 192.168.3
  { 192.168.3/24; // THEN use .3, or .1 or .2
    { 192.168.1/24; 192.168.2/24; }; };
{ { 192.168.4/24; 192.168.5/24; }
  // if .4 or .5, prefer that net
};

The following example will give reasonable behavior for the local host
and hosts on directly connected networks. It is similar to the behavior of
the address sort in BIND 4.9.x. Responses sent to queries from the local
host will favor any of the directly connected networks. Responses sent to
queries from any other hosts on a directly connected network will prefer
addresses on that same network. Responses to other queries will not be
sorted.

sortlist {
  { localhost; localnets; };
  { localnets; };
};

The sortlist option is not yet implemented in BIND 9.

6.2.14.11 RRset Ordering

When multiple records are returned in an answer it may be useful to
configure the order of the records placed into the response. For example,
the records for a zone might be configured always to be returned in the
order they are defined in the zone file. Or perhaps a random shuffle of the
records as they are returned is wanted. The rrset-order statement
permits configuration of the ordering made of the records in a multiple
record response. The default, if no ordering is defined, is a cyclic ordering
(round robin).

An order_spec is defined as follows:
[ class class_name ] [ type type_name ] [ name "domain_name"]
  order ordering

If no class is specified, the default is ANY. If no type is specified, the
default is ANY. If no name is specified, the default is "*".

The legal values for ordering are:
For example:

```c
rrset-order {
    class IN type A name "host.example.com" order random;
    order cyclic;
};
```

will cause any responses for type A records in class IN that have “host.example.com” as a suffix, to always be returned in random order. All other records are returned in cyclic order.

If multiple `rrset-order` statements appear, they are not combined—the last one applies.

If no `rrset-order` statement is specified, then a default one of:

```c
rrset-order { class ANY type ANY name "*"; order cyclic ;
};
```

is used.

The `rrset-order` statement is not yet implemented in BIND 9.

### 6.2.14.12 Tuning

- **lame-ttl**
  
  Sets the number of seconds to cache a lame server indication. 0 disables caching. (This is NOT recommended.) Default is 600 (10 minutes). Maximum value is 1800 (30 minutes). Not yet implemented in BIND 9.

- **max-ncache-ttl**
  
  To reduce network traffic and increase performance the server stores negative answers. `max-ncache-ttl` is used to set a maximum retention time for these answers in the server in seconds. The default `max-ncache-ttl` is 10800 seconds (3 hours). `max-ncache-ttl` cannot exceed 7 days and will be silently truncated to 7 days if set to a greater value.

- **max-cache-ttl**
  
  `max-cache-ttl` sets the maximum time for which the server will cache ordinary (positive) answers. The default is one week (7 days).
The statistics file generated by BIND 9 is similar, but not identical, to that generated by BIND 8.

The statistics dump begins with the line `+++ Statistics Dump +++ (973798949)`, where the number in parentheses is a standard UNIX-style timestamp, measured as seconds since January 1, 1970. Following that line are a series of lines containing a counter type, the value of the counter, optionally a zone name, and optionally a view name. The lines without view and zone listed are global statistics for the entire server. Lines with a zone and view name for the given view and zone (the view name is omitted for the default view). The statistics dump ends with the line `--- Statistics Dump --- (973798949)`, where the number is identical to the number in the beginning line.

The following statistics counters are maintained:

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>min-roots</td>
<td>The minimum number of root servers that is required for a request for the root servers to be accepted. Default is 2. Not yet implemented in BIND 9.</td>
</tr>
<tr>
<td>sig-validity-interval</td>
<td>Specifies the number of days into the future when DNSSEC signatures automatically generated as a result of dynamic updates (see Section 4.1, “Dynamic Update”, on page 15) will expire. The default is 30 days. The signature inception time is unconditionally set to one hour before the current time to allow for a limited amount of clock skew.</td>
</tr>
</tbody>
</table>

6.2.14.13 The Statistics File

The number of successful queries made to the server or zone. A successful query is defined as query which returns a NOERROR response other than a referral response.

The number of queries which resulted in referral responses.

The number of queries which resulted in NOERROR responses with no data.

The number of queries which resulted in NXDOMAIN responses.

The number of queries which caused the server to perform recursion in order to find the final answer.

The number of queries which resulted in a failure response other than those above.
6.2.15 server Statement Grammar

```plaintext
server ip_addr {
  [ bogus yes_or_no ; ]
  [ provide-ixfr yes_or_no ; ]
  [ request-ixfr yes_or_no ; ]
  [ transfers number ; ]
  [ transfer-format ( one-answer | many-answers ) ; ]
  [ keys { string ; [ string ; [ ... ] ] } ; ]
};
```

6.2.16 server Statement Definition and Usage

The `server` statement defines the characteristics to be associated with a remote nameserver.

If you discover that a remote server is giving out bad data, marking it as bogus will prevent further queries to it. The default value of `bogus` is no. The `bogus` clause is not yet implemented in BIND 9.

The `provide-ixfr` clause determines whether the local server, acting as master, will respond with an incremental zone transfer when the given remote server, a slave, requests it. If set to `yes`, incremental transfer will be provided whenever possible. If set to `no`, all transfers to the remote server will be nonincremental. If not set, the value of the `provide-ixfr` option in the global options block is used as a default.

IXFR requests to servers that do not support IXFR will automatically fall back to AXFR. Therefore, there is no need to manually list which servers support IXFR and which ones do not; the global default of `yes` should always work. The purpose of the `provide-ixfr` and `request-ixfr` clauses is to make it possible to disable the use of IXFR even when both master and slave claim to support it, for example if one of the servers is buggy and crashes or corrupts data when IXFR is used.

The server supports two zone transfer methods. The first, `one-answer`, uses one DNS message per resource record transferred. `many-answers` packs as many resource records as possible into a message. `many-answers` is more efficient, but is only known to be understood by BIND 9, BIND 8.x, and patched versions of BIND 4.9.5. You can specify which method to use for a server with the `transfer-format` option. If `transfer-format` is not specified, the `transfer-format` specified by the `options` statement will be used.

`transfers` is used to limit the number of concurrent inbound zone transfers from the specified server. If no `transfers` clause is specified, the limit is set according to the `transfers-per-ns` option.
The `keys` clause is used to identify a `key_id` defined by the `key` statement, to be used for transaction security when talking to the remote server. The `key` statement must come before the `server` statement that references it. When a request is sent to the remote server, a request signature will be generated using the key specified here and appended to the message. A request originating from the remote server is not required to be signed by this key.

Although the grammar of the `keys` clause allows for multiple keys, only a single key per server is currently supported.

### 6.2.17 `trusted-keys` Statement Grammar

```
trusted-keys {
    string number number number string ;
    [ string number number number string ; [ ... ]]
};
```

### 6.2.18 `trusted-keys` Statement Definition and Usage

The `trusted-keys` statement defines DNSSEC security roots. DNSSEC is described in Section 4.7, “DNSSEC”, on page 22. A security root is defined when the public key for a non-authoritative zone is known, but cannot be securely obtained through DNS, either because it is the DNS root zone or its parent zone is unsigned. Once a key has been configured as a trusted key, it is treated as if it had been validated and proven secure. The resolver attempts DNSSEC validation on all DNS data in subdomains of a security root.

The `trusted-keys` statement can contain multiple key entries, each consisting of the key’s domain name, flags, protocol, algorithm, and the base-64 representation of the key data.

### 6.2.19 `view` Statement Grammar

```
view view name {
    match-clients { address_match_list } ;
    [ view_option; ...]
    [ zone_statement; ...]
};
```

### 6.2.20 `view` Statement Definition and Usage

The `view` statement is a powerful new feature of BIND 9 that lets a name server answer a DNS query differently depending on who is asking. It is particularly useful for implementing split DNS setups without having to run multiple servers.

Each `view` statement defines a view of the DNS namespace that will be seen by those clients whose IP addresses match the `address_match_list` of the view’s `match-clients` clause. The order of the `view` statements is significant—a client query will be resolved in the context of the first `view` whose `match-clients` list matches the client’s IP address.
Zones defined within a `view` statement will be only be accessible to clients that match the `view`. By defining a zone of the same name in multiple views, different zone data can be given to different clients, for example, “internal” and “external” clients in a split DNS setup.

Many of the options given in the `options` statement can also be used within a `view` statement, and then apply only when resolving queries with that view. When no a view-specific value is given, the value in the `options` statement is used as a default. Also, zone options can have default values specified in the `view` statement; these view-specific defaults take precedence over those in the `options` statement.

Views are class specific. If no class is given, class IN is assumed. Note that all non-IN views must contain a hint zone, since only the IN class has compiled-in default hints.

If there are no `view` statements in the config file, a default view that matches any client is automatically created in class IN, and any `zone` statements specified on the top level of the configuration file are considered to be part of this default view. If any explicit `view` statements are present, all `zone` statements must occur inside `view` statements.

Here is an example of a typical split DNS setup implemented using `view` statements.

```plaintext
view "internal" {
    // This should match our internal networks.
    match-clients { 10.0.0.0/8; };
    // Provide recursive service to internal clients only.
    recursion yes;
    // Provide a complete view of the example.com zone
    // including addresses of internal hosts.
    zone "example.com" {
        type master;
        file "example-internal.db";
    };
}
view "external" {
    match-clients { any; };
    // Refuse recursive service to external clients.
    recursion no;
    // Provide a restricted view of the example.com zone
    // containing only publicly accessible hosts.
    zone "example.com" {
        type master;
        file "example-external.db";
    };
}
```

### 6.2.21 zone Statement Grammar

```plaintext
zone zone name {class} {
    type ( master/slave/hint/stub/forward ) ;
    [ allow-query { address_match_list } ] ;
    [ allow-transfer { address_match_list } ] ;
    [ allow-update { address_match_list } ] ;
}
```
[ update-policy { update_policy_rule [...] } ; ]
[ allow-update-forwarding { address_match_list } ; ]
[ also-notify { [ ip_addr ; [ip_addr ; [...] ] ] ; ]
[ check-names (warn|fail|ignore) ; ]
[ dialup true_or_false ; ]
[ file string ; ]
[ forward (only|first) ; ]
[ forwarders { [ ip_addr ; [ ip_addr ; [...] ] ] ; ]
[ ixfr-base string ; ]
[ ixfr-tmp-file string ; ]
[ maintain-ixfr-base true_or_false ; ]
[ masters [port number] { ip_addr ; [ip_addr ; [...] ] } ; ]
[ max-ixfr-log-size number ; ]
[ max-transfer-idle-in number ; ]
[ max-transfer-idle-out number ; ]
[ max-transfer-time-in number ; ]
[ max-transfer-time-out number ; ]
[ notify true_or_false ; ]
[ pubkey number number number string ; ]
[ transfer-source (ip4_addr | *) ; ]
[ transfer-source-v6 (ip6_addr | *) ; ]
[ notify-source (ip4_addr | *) [port ip_port] ; ]
[ notify-source-v6 (ip6_addr | *) [port ip_port] ; ]
[ zone-statistics yes_or_no ; ]
[ sig-validity-interval number ; ]
[ database string ; ]
]};
6.2.22 zone Statement Definition and Usage

6.2.22.1 Zone Types

**master**
The server has a master copy of the data for the zone and will be able to provide authoritative answers for it.

**slave**
A slave zone is a replica of a master zone. The masters list specifies one or more IP addresses that the slave contacts to update its copy of the zone. By default, transfers are made from port 53 on the servers; this can be changed for all servers by specifying a port number before the list of IP addresses, or on a per-server basis after the IP address. If a port is specified, the slave then checks to see if the zone is current and zone transfers will be done to the port given. If a file is specified, then the replica will be written to this file whenever the zone is changed, and reloaded from this file on a server restart. Use of a file is recommended, since it often speeds server start-up and eliminates a needless waste of bandwidth. Note that for large numbers (in the tens or hundreds of thousands) of zones per server, it is best to use a two level naming scheme for zone file names. For example, a slave server for the zone *example.com* might place the zone contents into a file called *ex/example.com* where *ex/* is just the first two letters of the zone name. (Most operating systems behave very slowly if you put 100K files into a single directory.)

**stub**
A stub zone is similar to a slave zone, except that it replicates only the NS records of a master zone instead of the entire zone. Stub zones are not a standard part of the DNS; they are a peculiarity of BIND 4 and BIND 8 that relies heavily on the particular way the zone data is structured in those servers. BIND 9 attempts to emulate the BIND 4/8 stub zone feature for backwards compatibility, but we do not recommend its use in new configurations.

In BIND 4/8, zone transfers of a parent zone included the NS records from stub children of that zone. This meant that, in some cases, users could get away with configuring child stubs only in the master server for the parent zone. BIND 9 never mixes together zone data from different zones in this way. Therefore, if a BIND 9 master serving a parent zone has child stub zones configured, all the slave servers for the parent zone also need to have the same child stub zones configured.
6.2.22.2 Class

The zone’s name may optionally be followed by a class. If a class is not specified, class IN (for Internet), is assumed. This is correct for the vast majority of cases.

The hesiod class is named for an information service from MIT’s Project Athena. It is used to share information about various systems databases, such as users, groups, printers and so on. The keyword HS is a synonym for hesiod.

Another MIT development is CHAOSnet, a LAN protocol created in the mid-1970s. Zone data for it can be specified with the chaos class.
6.2.22.3 Zone Options

**allow-query**
See the description of `allow-query` under “Access Control” on page 48.

**allow-transfer**
See the description of `allow-transfer` under “Access Control” on page 48.

**allow-update**
Specifies which hosts are allowed to submit Dynamic DNS updates for master zones. The default is to deny updates from all hosts.

**update-policy**

**allow-update-forwarding**
Specifies which hosts are allowed to submit Dynamic DNS updates to slave zones to be forwarded to the master. The default is `{ none; }`, which means that no update forwarding will be performed. To enable update forwarding, specify `allow-update-forwarding { any; };`.

Specifying values other than `{ none; }` or `{ any; }` is usually counterproductive, since the responsibility for update access control should rest with the master server, not the slaves.

Note that enabling the update forwarding feature on a slave server may expose master servers relying on insecure IP address based access control to attacks; see “Dynamic Update Security” on page 78 for more details.

**also-notify**
Only meaningful if `notify` is active for this zone. The set of machines that will receive a DNS NOTIFY message for this zone is made up of all the listed nameservers (other than the primary master) for the zone plus any IP addresses specified with `also-notify`.

A port may be specified with each `also-notify` address to send the notify messages to a port other than the default of 53. `also-notify` is not meaningful for stub zones. The default is the empty list.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>check-names</td>
<td>This option was used in BIND 8 to restrict the character set of domain names in master files and/or DNS responses received from the network. BIND 9 does not restrict the character set of domain names and does not implement the <code>check-names</code> option.</td>
</tr>
<tr>
<td>database</td>
<td>Specify the type of database to be used for storing the zone data. The string following the <code>database</code> keyword is interpreted as a list of whitespace-delimited words. The first word identifies the database type, and any subsequent words are passed as arguments to the database to be interpreted in a way specific to the database type. The default is <code>&quot;rbt&quot;</code>, BIND 9's native in-memory red-black-tree database. Other values are possible if additional database drivers have been linked into the server. Some sample drivers are included with the distribution but none are linked in by default.</td>
</tr>
<tr>
<td>dialup</td>
<td>See the description of <code>dialup</code> under “Boolean Options” on page 44.</td>
</tr>
<tr>
<td>forward</td>
<td>Only meaningful if the zone has a forwarders list. The <code>only</code> value causes the lookup to fail after trying the forwarders and getting no answer, while <code>first</code> would allow a normal lookup to be tried.</td>
</tr>
<tr>
<td>forwarders</td>
<td>Used to override the list of global forwarders. If it is not specified in a zone of type <code>forward</code>, no forwarding is done for the zone; the global options are not used.</td>
</tr>
<tr>
<td>ixfr-base</td>
<td>Was used in BIND 8 to specify the name of the transaction log (journal) file for dynamic update and IXFR. BIND 9 ignores the option and constructs the name of the journal file by appending “.jnl” to the name of the zone file.</td>
</tr>
<tr>
<td>max-transfer-time-in</td>
<td>See the description of <code>max-transfer-time-in</code> under “Zone Transfers” on page 50.</td>
</tr>
<tr>
<td>max-transfer-idle-in</td>
<td>See the description of <code>max-transfer-idle-in</code> under “Zone Transfers” on page 50.</td>
</tr>
</tbody>
</table>
6.2.22.4 Dynamic Update Policies

BIND 9 supports two alternative methods of granting clients the right to perform dynamic updates to a zone, configured by the `allow-update` and `update-policy` option, respectively.

The `allow-update` clause works the same way as in previous versions of BIND. It grants given clients the permission to update any record of any name in the zone.
The `update-policy` clause is new in BIND 9 and allows more fine-grained control over what updates are allowed. A set of rules is specified, where each rule either grants or denies permissions for one or more names to be updated by one or more identities. If the dynamic update request message is signed (that is, it includes either a TSIG or SIG(0) record), the identity of the signer can be determined.

Rules are specified in the `update-policy` zone option, and are only meaningful for master zones. When the `update-policy` statement is present, it is a configuration error for the `allow-update` statement to be present. The `update-policy` statement only examines the signer of a message; the source address is not relevant.

This is how a rule definition looks:
```
(grant | deny) identity nametype name [ types ]
```

Each rule grants or denies privileges. Once a message has successfully matched a rule, the operation is immediately granted or denied and no further rules are examined. A rule is matched when the signer matches the identity field, the name matches the name field, and the type is specified in the type field.

The identity field specifies a name or a wildcard name. The nametype field has 4 values: `name`, `subdomain`, `wildcard`, and `self`.

- **name** Matches when the updated name is the same as the name in the name field.
- **subdomain** Matches when the updated name is a subdomain of the name in the name field.
- **wildcard** Matches when the updated name is a valid expansion of the wildcard name in the name field.
- **self** Matches when the updated name is the same as the message signer. The name field is ignored.

If no types are specified, the rule matches all types except SIG, NS, SOA, and NXT. Types may be specified by name, including “ANY” (ANY matches all types except NXT, which can never be updated).

### 6.3 Zone File

#### 6.3.1 Types of Resource Records and When to Use Them

This section, largely borrowed from RFC 1034, describes the concept of a Resource Record (RR) and explains when each is used. Since the publication of RFC 1034, several new RRs have been identified and implemented in the DNS. These are also included.
6.3.1.1 Resource Records

A domain name identifies a node. Each node has a set of resource information, which may be empty. The set of resource information associated with a particular name is composed of separate RRs. The order of RRs in a set is not significant and need not be preserved by nameservers, resolvers, or other parts of the DNS. However, sorting of multiple RRs is permitted for optimization purposes, for example, to specify that a particular nearby server be tried first. See “The sortlist Statement” on page 55 and “RRset Ordering” on page 56 for details.

The components of a Resource Record are

- **owner name**: the domain name where the RR is found.
- **type**: an encoded 16 bit value that specifies the type of the resource in this resource record. Types refer to abstract resources.
- **TTL**: the time to live of the RR. This field is a 32 bit integer in units of seconds, and is primarily used by resolvers when they cache RRs. The TTL describes how long a RR can be cached before it should be discarded.
- **class**: an encoded 16 bit value that identifies a protocol family or instance of a protocol.
- **RDATA**: the type and sometimes class-dependent data that describes the resource.

The following are types of valid RRs (some of these listed, although not obsolete, are experimental (x) or historical (h) and no longer in general use):

- **A**: a host address.
- **A6**: an IPv6 address.
- **AAAA**: Obsolete format of IPv6 address
- **AFSDB**: (x) location of AFS database servers. Experimental.
- **CNAME**: identifies the canonical name of an alias.
- **DNAME**: for delegation of reverse addresses. Replaces the domain name specified with another name to be looked up. Described in RFC 2672.
- **HINFO**: identifies the CPU and OS used by a host.
- **ISDN**: (x) representation of ISDN addresses. Experimental.
- **KEY**: stores a public key associated with a DNS name.
- **LOC**: (x) for storing GPS info. See RFC 1876. Experimental.
- **MX**: identifies a mail exchange for the domain. See RFC 974 for details.
The following classes of resource records are currently valid in the DNS:

**NS** the authoritative nameserver for the domain.

**NXT** used in DNSSEC to securely indicate that RRs with an owner name in a certain name interval do not exist in a zone and indicate what RR types are present for an existing name. See RFC 2535 for details.

**PTR** a pointer to another part of the domain name space.

**RP** (x) information on persons responsible for the domain. Experimental.

**RT** (x) route-through binding for hosts that do not have their own direct wide area network addresses. Experimental.

**SIG** (“signature”) contains data authenticated in the secure DNS. See RFC 2535 for details.

**SOA** identifies the start of a zone of authority.

**SRV** information about well known network services (replaces WKS).

**WKS** (h) information about which well known network services, such as SMTP, that a domain supports. Historical, replaced by newer RR SRV.

**X25** (x) representation of X.25 network addresses. Experimental.

The following classes of resource records are currently valid in the DNS:

**IN** the Internet system.

For information about other, older classes of RRs, see Section B.1, “Classes of Resource Records”, on page 85 of the Appendix.

**RDATA** is the type-dependent or class-dependent data that describes the resource:

**A** for the IN class, a 32 bit IP address.

**A6** maps a domain name to an IPv6 address, with a provision for indirection for leading “prefix” bits.

**CNAME** a domain name.

**DNAME** provides alternate naming to an entire subtree of the domain name space, rather than to a single node. It causes some suffix of a queried name to be substituted with a name from the DNAME record’s RDATA.

**MX** a 16 bit preference value (lower is better) followed by a host name willing to act as a mail exchange for the owner domain.

**NS** a fully qualified domain name.

**PTR** a fully qualified domain name.
The owner name is often implicit, rather than forming an integral part of the RR. For example, many nameservers internally form tree or hash structures for the name space, and chain RRs off nodes. The remaining RR parts are the fixed header (type, class, TTL) which is consistent for all RRs, and a variable part (RDATA) that fits the needs of the resource being described.

The meaning of the TTL field is a time limit on how long an RR can be kept in a cache. This limit does not apply to authoritative data in zones; it is also timed out, but by the refreshing policies for the zone. The TTL is assigned by the administrator for the zone where the data originates. While short TTLs can be used to minimize caching, and a zero TTL prohibits caching, the realities of Internet performance suggest that these times should be on the order of days for the typical host. If a change can be anticipated, the TTL can be reduced prior to the change to minimize inconsistency during the change, and then increased back to its former value following the change.

The data in the RDATA section of RRs is carried as a combination of binary strings and domain names. The domain names are frequently used as “pointers” to other data in the DNS.

### 6.3.1.2 Textual expression of RRs

RRs are represented in binary form in the packets of the DNS protocol, and are usually represented in highly encoded form when stored in a nameserver or resolver. In the examples provided in RFC 1034, a style similar to that used in master files was employed in order to show the contents of RRs. In this format, most RRs are shown on a single line, although continuation lines are possible using parentheses.

The start of the line gives the owner of the RR. If a line begins with a blank, then the owner is assumed to be the same as that of the previous RR. Blank lines are often included for readability.

Following the owner, we list the TTL, type, and class of the RR. Class and type use the mnemonics defined above, and TTL is an integer before the type field. In order to avoid ambiguity in parsing, type and class mnemonics are disjoint, TTLs are integers, and the type mnemonic is always last. The IN class and TTL values are often omitted from examples in the interests of clarity.

The resource data or RDATA section of the RR are given using knowledge of the typical representation for the data.

For example, we might show the RRs carried in a message as:

```
SOA  several fields.

ISI.EDU.  MX 10 VENERA.ISI.EDU.
```
The MX RRs have an RDATA section which consists of a 16 bit number followed by a domain name. The address RRs use a standard IP address format to contain a 32 bit internet address.

This example shows six RRs, with two RRs at each of three domain names.

Similarly we might see:

```
XX.LCS.MIT.EDU. IN A 10.0.0.44
CH A MIT.EDU. 2420
```

This example shows two addresses for XX.LCS.MIT.EDU, each of a different class.

### 6.3.2 Discussion of MX Records

As described above, domain servers store information as a series of resource records, each of which contains a particular piece of information about a given domain name (which is usually, but not always, a host). The simplest way to think of a RR is as a typed pair of datum, a domain name matched with relevant data, and stored with some additional type information to help systems determine when the RR is relevant.

MX records are used to control delivery of email. The data specified in the record is a priority and a domain name. The priority controls the order in which email delivery is attempted, with the lowest number first. If two priorities are the same, a server is chosen randomly. If no servers at a given priority are responding, the mail transport agent will fall back to the next largest priority. Priority numbers do not have any absolute meaning - they are relevant only respective to other MX records for that domain name. The domain name given is the machine to which the mail will be delivered. It *must* have an associated A record—a CNAME is not sufficient.

For a given domain, if there is both a CNAME record and an MX record, the MX record is in error, and will be ignored. Instead, the mail will be delivered to the server specified in the MX record pointed to by the CNAME.

For example:

```
example.com. IN MX 10 mail.example.com.
IN MX 10 mail2.example.com.
IN MX 20 mail.backup.org.
```
Mail delivery will be attempted to `mail.example.com` and `mail2.example.com` (in any order), and if neither of those succeed, delivery to `mail.backup.org` will be attempted.

### 6.3.3 Setting TTLs

The time to live (TTL) of the RR field is a 32 bit integer represented in units of seconds, and is primarily used by resolvers when they cache RRs. The TTL describes how long a RR can be cached before it should be discarded. The following three types of TTL are currently used in a zone file.

- **SOA** The last field in the SOA is the negative caching TTL. This controls how long other servers will cache no-such-domain (NXDOMAIN) responses from you.
  - The maximum time for negative caching is 3 hours (3h).
- **$TTL** The $TTL directive at the top of the zone file (before the SOA) gives a default TTL for every RR without a specific TTL set.
- **RR TTLs** Each RR can have a TTL as the second field in the RR, which will control how long other servers can cache it.

All of these TTLs default to units of seconds, though units can be explicitly specified, for example, `1h30m`.

### 6.3.4 Inverse Mapping in IPv4

Reverse name resolution (that is, translation from IP address to name) is achieved by means of the `in-addr.arpa` domain and PTR records. Entries in the `in-addr.arpa` domain are made in least-to-most significant order, read left to right. This is the opposite order to the way IP addresses are usually written. Thus, a machine with an IP address of 10.1.2.3 would have a corresponding `in-addr.arpa` name of 3.2.1.10.in-addr.arpa. This name should have a PTR resource record whose data field is the name of the machine or, optionally, multiple PTR records if the machine has more than one name. For example, in the `example.com` domain:

```
$ORIGIN 2.1.10.in-addr.arpa
3 IN PTR foo.example.com.
```

(Note: The `$ORIGIN` lines in the examples are for providing context to the examples only—they do not necessarily appear in the actual usage. They are only used here to indicate that the example is relative to the listed origin.)
6.3.5 Other Zone File Directives

The Master File Format was initially defined in RFC 1035 and has subsequently been extended. While the Master File Format itself is class independent all records in a Master File must be of the same class.

Master File Directives include $ORIGIN, $INCLUDE, and $TTL.

6.3.5.1 The $ORIGIN Directive

Syntax: $ORIGIN domain-name [ comment ]

$ORIGIN sets the domain name that will be appended to any unqualified records. When a zone is first read in there is an implicit $ORIGIN <zone-name>. The current $ORIGIN is appended to the domain specified in the $ORIGIN argument if it is not absolute.

$ORIGIN example.com
WWW CNAME MAIN-SERVER

is equivalent to
WWW.EXAMPLE.COM CNAME MAIN-SERVER.EXAMPLE.COM.

6.3.5.2 The $INCLUDE Directive

Syntax: $INCLUDE filename [ origin ] [ comment ]

Read and process the file filename as if it were included into the file at this point. If origin is specified the file is processed with $ORIGIN set to that value, otherwise the current $ORIGIN is used.

NOTE: The behavior when origin is specified differs from that described in RFC 1035. The origin and current domain revert to the values they were prior to the $INCLUDE once the file has been read.

6.3.5.3 The $TTL Directive

Syntax: $TTL default-ttl [ comment ]

Set the default Time To Live (TTL) for subsequent records with undefined TTLs. Valid TTLs are of the range 0-2147483647 seconds.

$TTL is defined in RFC 2308.

6.3.6 BIND Master File Extension: the $GENERATE Directive

$GENERATE

Syntax: $GENERATE range hs type rhs [ comment ]
$GENERATE is used to create a series of resource records that only differ from each other by an iterator. $GENERATE can be used to easily generate the sets of records required to support sub /24 reverse delegations described in RFC 2317: Classless IN-ADDR.ARPA delegation.

$ORIGIN 0.0.192.IN-ADDR.ARPA.
$GENERATE 1-2 0 NS SERVER$.EXAMPLE.
$GENERATE 1-127 $ CNAME $.0

is equivalent to

- 0.0.0.192.IN-ADDR.ARPA NS SERVER1.EXAMPLE.
- 0.0.0.192.IN-ADDR.ARPA NS SERVER2.EXAMPLE.
- 1.0.0.192.IN-ADDR.ARPA CNAME 1.0.0.0.192.IN-ADDR.ARPA
- 2.0.0.192.IN-ADDR.ARPA CNAME 2.0.0.0.192.IN-ADDR.ARPA
- ...
- 127.0.0.192.IN-ADDR.ARPA CNAME 127.0.0.0.192.IN-ADDR.ARPA

range

This can be one of two forms: start-stop or start-stop/step. If the first form is used then step is set to 1. All of start, stop and step must be positive.

lhs

lhs describes the owner name of the resource records to be created. Any single $ symbols within the lhs side are replaced by the iterator value. To get a $ in the output you need to escape the $ using a backslash ("\"), for example, \$. The $ may optionally be followed by modifiers which change the offset from the iterator, field width, and base. Modifiers are introduced by a left brace character ("{"), immediately following the $ as ${offset[,width[,base]]}. For example, ${-20,3,d}, which subtracts 20 from the current value, prints the result as a decimal in a zero padded field of width 3. Available output forms are decimal (d), octal (o) and hexadecimal (x or X for uppercase). The default modifier is ${0,0,d}. If the lhs is not absolute, the current $ORIGIN is appended to the name.

For compatibility with earlier versions $$ is still recognized as indicating a literal $ in the output.

type

At present the only supported types are PTR, CNAME and NS.

rhs

rhs is a domain name. It is processed similarly to lhs.

The $GENERATE directive is a BIND extension and not part of the standard zone file format.
Section 7. BIND 9 Security Considerations

7.1 Access Control Lists

Access Control Lists (ACLs), are address match lists that you can set up and nickname for future use in allow-query, allow-recursion, blackhole, allow-transfer, etc.

Using ACLs allows you to have finer control over who can access your nameserver, without cluttering up your config files with huge lists of IP addresses.

It is a good idea to use ACLs, and to control access to your server. Limiting access to your server by outside parties can help prevent spoofing and DoS attacks against your server.

Here is an example of how to properly apply ACLs:

// Set up an ACL named “bogusnets” that will block RFC1918 space,
// which is commonly used in spoofing attacks.
acl bogusnets { 0.0.0.0/8; 1.0.0.0/8; 2.0.0.0/8; 192.0.2.0/24; 224.0.0.0/3;
10.0.0.0/8; 172.16.0.0/12; 192.168.0.0/16; }

// Set up an ACL called our-nets. Replace this with the real IP numbers.
acl our-nets { x.x.x.x/24; x.x.x.x/21; }
options {
...
...
allow-query { our-nets; }
allow-recursion { our-nets; }
...
blackhole { bogusnets; }
....
};

zone "example.com" {
    type master;
    file "m/example.com";
    allow-query { any; }
};

This allows recursive queries of the server from the outside unless recursion has been previously disabled.

For more information on how to use ACLs to protect your server, see the AUSCERT advisory at ftp://ftp.auscert.org.au/pub/auscert/advisory/AL-1999.004.dns_dos

7.2 chroot and setuid (for UNIX servers)

On UNIX servers, it is possible to run BIND in a chrooted environment (chroot()) by specifying the “-t” option. This can help improve system security by placing BIND in a “sandbox,” which will limit the damage done if a server is compromised.
Another useful feature in the UNIX version of BIND is the ability to run the daemon as a nonprivileged user (-u user). We suggest running as a nonprivileged user when using the chroot feature.

Here is an example command line to load BIND in a chroot() sandbox, /var/named, and to run named setuid to user 202:
/usr/local/bin/named -u 202 -t /var/named

7.2.1 The chroot Environment

In order for a chroot() environment to work properly in a particular directory (for example, /var/named), you will need to set up an environment that includes everything BIND needs to run. From BIND’s point of view, /var/named is the root of the filesystem. You will need /dev/null, and any library directories and files that BIND needs to run on your system. Please consult your operating system’s instructions if you need help figuring out which library files you need to copy over to the chroot() sandbox.

If you are running an operating system that supports static binaries, you can also compile BIND statically and avoid the need to copy system libraries over to your chroot() sandbox.

7.2.2 Using the setuid Function

Prior to running the named daemon, use the touch utility (to change file access and modification times) or the chown utility (to set the user id and/or group id) on files to which you want BIND to write.

7.3 Dynamic Update Security

Access to the dynamic update facility should be strictly limited. In earlier versions of BIND the only way to do this was based on the IP address of the host requesting the update, by listing an IP address or network prefix in the allow-update zone option. This method is insecure since the source address of the update UDP packet is easily forged. Also note that if the IP addresses allowed by the allow-update option include the address of a slave server which performs forwarding of dynamic updates, the master can be trivially attacked by sending the update to the slave, which will forward it to the master with its own source IP address causing the master to approve it without question.

For these reasons, we strongly recommend that updates be cryptographically authenticated by means of transaction signatures (TSIG). That is, the allow-update option should list only TSIG key names, not IP addresses or network prefixes. Alternatively, the new update-policy option can be used.

Some sites choose to keep all dynamically updated DNS data in a subdomain and delegate that subdomain to a separate zone. This way, the top-level zone containing critical data such as the IP addresses of public web and mail servers need not allow dynamic update at all.
Section 8. Troubleshooting

8.1 Common Problems

8.1.1 It’s not working; how can I figure out what’s wrong?

The best solution to solving installation and configuration issues is to take preventative measures by setting up logging files beforehand (see the sample configurations in Section 3.1 “Sample Configurations”, page 9). The log files provide a source of hints and information that can be used to figure out what went wrong and how to fix the problem.

8.2 Incrementing and Changing the Serial Number

Zone serial numbers are just numbers—they aren’t date related. A lot of people set them to a number that represents a date, usually of the form YYYYMMDDRR. A number of people have been testing these numbers for Y2K compliance and have set the number to the year 2000 to see if it will work. They then try to restore the old serial number. This will cause problems because serial numbers are used to indicate that a zone has been updated. If the serial number on the slave server is lower than the serial number on the master, the slave server will attempt to update its copy of the zone.

Setting the serial number to a lower number on the master server than the slave server means that the slave will not perform updates to its copy of the zone.

The solution to this is to add 2147483647 (2^31-1) to the number, reload the zone and make sure all slaves have updated to the new zone serial number, then reset the number to what you want it to be, and reload the zone again.

8.3 Where Can I Get Help?

The last major versions of BIND have been written by Nominum, Inc. according to an agreement with the Internet Software Consortium (ISC).

Nominum offers a wide range of support and service agreements for BIND. Several levels of premium support are available which include support for BIND and DHCP, significant discounts on products and training, and a recognized priority on bug fixes and non-funded feature requests. In addition, Nominum offers an urgent support package that provides fast response for urgent issues.

To discuss arrangements for support, contact sales@nominum.com or visit the Nominum web page at http://www.nominum.com/services/index.html to learn more.
Appendices
Appendix A. Acknowledgements

A.1 A Brief History of the DNS and BIND

Although the “official” beginning of the Domain Name System occurred in 1984 with the publication of RFC 920, the core of the new system was described in 1983 in RFCs 882 and 883. From 1984 to 1987, the ARPAnet (the precursor to today’s Internet) became a testbed of experimentation for developing the new naming/addressing scheme in an rapidly expanding, operational network environment. New RFCs were written and published in 1987 that modified the original documents to incorporate improvements based on the working model. RFC 1034, “Domain Names–Concepts and Facilities,” and RFC 1035, “Domain Names–Implementation and Specification” were published and became the standards upon which all DNS implementations are built.

The first working domain name server, called “Jeeves,” was written in 1983-84 by Paul Mockapetris for operation on DEC Tops-20 machines located at the University of Southern California’s Information Sciences Institute (USC-ISI) and SRI International’s Network Information Center (SRI-NIC). A DNS server for Unix machines, the Berkeley Internet Name Domain (BIND) package, was written soon after by a group of graduate students at the University of California at Berkeley under a grant from the US Defense Advanced Research Projects Administration (DARPA). Versions of BIND through 4.8.3 were maintained by the Computer Systems Research Group (CSRG) at UC Berkeley. Douglas Terry, Mark Painter, David Riggle and Songnian Zhou made up the initial BIND project team. After that, additional work on the software package was done by Ralph Campbell. Kevin Dunlap, a Digital Equipment Corporation employee on loan to the CSRG, worked on BIND for 2 years, from 1985 to 1987. Many other people also contributed to BIND development during that time: Doug Kingston, Craig Partridge, Smoot Carl-Mitchell, Mike Muuss, Jim Bloom and Mike Schwartz. BIND maintenance was subsequently handled by Mike Karels and O. Kure.

BIND versions 4.9 and 4.9.1 were released by Digital Equipment Corporation (now Compaq Computer Corporation). Paul Vixie, then a DEC employee, became BIND’s primary caretaker. Paul was assisted by Phil Almquist, Robert Elz, Alan Barrett, Paul Albitz, Bryan Beecher, Andrew Partan, Andy Cherenson, Tom Limoncelli, Berthold Paffrath, Fuat Baran, Anant Kumar, Art Harkin, Win Treese, Don Lewis, Christophe Wolfhugel, and others.

BIND Version 4.9.2 was sponsored by Vixie Enterprises. Paul Vixie became BIND’s principal architect/programmer.

BIND versions from 4.9.3 onward have been developed and maintained by the Internet Software Consortium with support being provided by ISC’s sponsors. As co-architects/programmers, Bob Halley and Paul Vixie released the first production-ready version of BIND version 8 in May 1997.

BIND development work is made possible today by the sponsorship of several corporations, and by the tireless work efforts of numerous individuals.
Appendix B. Historical DNS Information

B.1 Classes of Resource Records

B.1.1 HS = hesiod

The hesiod class is an information service developed by MIT’s Project Athena. It is used to share information about various systems databases, such as users, groups, printers and so on. The keyword hs is a synonym for hesiod.

B.1.2 CH = chaos

The chaos class is used to specify zone data for the MIT-developed CHAOSnet, a LAN protocol created in the mid-1970s.
Appendix C. General DNS Reference Information

C.1 IPv6 addresses (A6)

IPv6 addresses are 128-bit identifiers for interfaces and sets of interfaces which were introduced in the DNS to facilitate scalable Internet routing. There are three types of addresses: Unicast, an identifier for a single interface; Anycast, an identifier for a set of interfaces; and Multicast, an identifier for a set of interfaces. Here we describe the global Unicast address scheme. For more information, see RFC 2374.

The aggregatable global Unicast address format is as follows:

```
<table>
<thead>
<tr>
<th>3</th>
<th>13</th>
<th>8</th>
<th>24</th>
<th>16</th>
<th>64 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>FP</td>
<td>TLA</td>
<td>RES</td>
<td>NLA</td>
<td>SLA</td>
<td>Interface ID</td>
</tr>
</tbody>
</table>

<------ Public Topology ------>

<---Site Topology-->

<------ Interface Identifier ------>
```

Where

- **FP** = Format Prefix (001)
- **TLA ID** = Top-Level Aggregation Identifier
- **RES** = Reserved for future use
- **NLA ID** = Next-Level Aggregation Identifier
- **SLA ID** = Site-Level Aggregation Identifier
- **INTERFACE ID** = Interface Identifier

The **Public Topology** is provided by the upstream provider or ISP, and (roughly) corresponds to the IPv4 network section of the address range. The **Site Topology** is where you can subnet this space, much the same as subnetting an IPv4 /16 network into /24 subnets. The **Interface Identifier** is the address of an individual interface on a given network. (With IPv6, addresses belong to interfaces rather than machines.)

The subnetting capability of IPv6 is much more flexible than that of IPv4: subnetting can now be carried out on bit boundaries, in much the same way as Classless InterDomain Routing (CIDR).

The internal structure of the Public Topology for an A6 global unicast address consists of:

```
<table>
<thead>
<tr>
<th>3</th>
<th>13</th>
<th>8</th>
<th>24</th>
</tr>
</thead>
<tbody>
<tr>
<td>FP</td>
<td>TLA ID</td>
<td>RES</td>
<td>NLA ID</td>
</tr>
</tbody>
</table>
```
A 3 bit FP (Format Prefix) of 001 indicates this is a global Unicast address. FP lengths for other types of addresses may vary.

13 TLA (Top Level Aggregator) bits give the prefix of your top-level IP backbone carrier.

8 Reserved bits

24 bits for Next Level Aggregators. This allows organizations with a TLA to hand out portions of their IP space to client organizations, so that the client can then split up the network further by filling in more NLA bits, and hand out IPv6 prefixes to their clients, and so forth.

There is no particular structure for the Site topology section. Organizations can allocate these bits in any way they desire.

The Interface Identifier must be unique on that network. On ethernet networks, one way to ensure this is to set the address to the first three bytes of the hardware address, “FFFE”, then the last three bytes of the hardware address. The lowest significant bit of the first byte should then be complemented. Addresses are written as 32-bit blocks separated with a colon, and leading zeros of a block may be omitted, for example:

3ffe:8050:201:9:a00:20ff:fe81:2b32

IPv6 address specifications are likely to contain long strings of zeros, so the architects have included a shorthand for specifying them. The double colon (‘::’) indicates the longest possible string of zeros that can fit, and can be used only once in an address.
Appendix D. Bibliography (and Suggested Reading)

D.1 Request for Comments (RFCs)

Specification documents for the Internet protocol suite, including the DNS, are published as part of the Request for Comments (RFCs) series of technical notes. The standards themselves are defined by the Internet Engineering Task Force (IETF) and the Internet Engineering Steering Group (IESG). RFCs can be obtained online via FTP at ftp://www.isi.edu/in-notes/RFCxxx.txt (where xxx is the number of the RFC). RFCs are also available via the Web at http://www.ietf.org/rfc/.

D.1.1 Standards


D.1.2 Proposed Standards


D.1.3 Proposed Standards Still Under Development

Note: the following list of RFCs are undergoing major revision by the IETF.


D.1.4 Other Important RFCs About DNS Implementation

D.1.5 Resource Record Types


D.1.6 DNS and the Internet


D.1.7 DNS Operations


D.1.8 Other DNS-related RFCs

*Note: the following list of RFCs, although DNS-related, are not concerned with implementing software.*


D.1.9 Obsolete and Unimplemented Experimental RRs


D.2 Internet Drafts

Internet Drafts (IDs) are rough-draft working documents of the Internet Engineering Task Force. They are, in essence, RFCs in the preliminary stages of development. Implementors are cautioned not to regard IDs as archival, and they should not be quoted or cited in any formal documents unless accompanied by the disclaimer that they are “works in progress.” IDs have a lifespan of six months after which they are deleted unless updated by their authors.

D.3 Other Documents About BIND
