MacDNS 1.0.3 Administrator's Guide

About This Guide

This guide describes how to install, set up, and use MacDNS software. The guide also provides details about the Domain Name System.

This guide is provided to you in Adobe™ Acrobat format. You can view the entire guide on-screen; you can also print the document to have a hard-copy version available as a convenient reference.

Who should read this guide

This guide is intended for administrators of MacDNS servers. The guide assumes you are an administrator of a small- to medium-sized Internet site and that you are running the MacDNS software on a PowerPC™–based Internet Server from Apple Computer.

What you need to know

You don't need to have prior knowledge of the Domain Name System (DNS) to use the MacDNS program or to understand this guide. The guide does assume you have some familiarity with the Internet and internetworking concepts. If you want to learn about the Domain Name System, you can read the appendix to this guide, which provides details about how DNS works. You can also refer to the resources described in "For More Information" later in this section.

Balloon Help

The *MacDNS Administrator's Guide* provides you with all the details you'll need to set up and use the MacDNS software. If you're using the MacDNS software and you have a question about an item you see in the interface, you can use Balloon Help to provide you with on-screen information about that item. To turn on MacDNS Balloon Help, choose Show Balloons from the Help menu (the question mark in the upper-right corner of the menu bar at the top of your screen). To turn off Balloon Help, choose Hide Balloons from the Help menu.

For more information

If you want to know more about DNS than the information provided in the appendix of this guide, there are several publicly available books and documents that may be helpful:

DNS and BIND. 1992. Paul Albitz and Cricket Liu. Published by O'Reilly and Associates, Sebastopol, California. Though much of this retail book is devoted to explaining BIND, a program for the UNIX® operating system, this book has a good overview of the history and function of the Domain Name System.

"Domain Names—Concepts and Facilities." 1987. Paul Mockapetris. RFC 1034; available at `http://ds.internic.net/rfc/rfc1034.txt`. Provides technical details about the Domain Name System.

"Domain Names—Implementation and Specification." 1987. Paul Mockapetris. RFC 1035; available at `http://ds.internic.net/rfc/rfc1035.txt`. Provides technical details about the Domain Name System.

"DNS Encoding of Network Names and Other Types." 1989. Paul Mockapetris. 1989. RFC 1101; available at `http://ds.internic.net/rfc/rfc1101.txt`. Provides technical details about the Domain Name System.

The following URLs may also be helpful.

InterNIC directory and database services: `http://www.internic.net/`

Searchable database of domain names:
`gopher://rs.internic.net/7waissrc%3A/rs/whois.rc`

Information about fees for registering domain names:
`http://rs.internic.net/announcements/fee-policy.html`

1 About MacDNS Software

The Domain Name System (DNS) was developed in the 1980s to deal with the explosive growth of the Internet. Up until then, information about the names and addresses of the hosts (machines) on the Internet was kept in a single file. However, this single-file scheme became difficult to use for several reasons, including the problem of keeping copies of the file synchronized and the large amount of network traffic that occured when many requests were made for Internet address information.

Instead of storing Internet name and address information in a single file, the Domain Name System contains such information in a distributed database. Programs called *name servers* provide information about portions of the database. The function of name-server software is to map a name of a machine on the Internet to an IP address.

FEELING LOST? If the preceding paragraphs contain information that is not at all familiar to you, now is a good time to read the appendix, "How the Domain Name System Works." After you read the appendix, return here to learn about the MacDNS program.

What is MacDNS?

MacDNS is a Mac OS–based DNS name server. It is ideal for serving a small- to medium-sized site that is connected to the Internet. Once you've installed and set up the MacDNS program, MacDNS can handle any DNS queries about a particular host at your site, find information about that host, and send the information back to the requester.

The major features of MacDNS are:

- MacDNS has an easy-to-use interface. You can easily assign domain names and IP addresses for all of the hosts at your site.
- MacDNS can share load between several hosts. It does this by grouping a number of hosts under a single load-sharing group name. For each successive query, MacDNS returns the address of a different host in the load-sharing group. This has the effect of spreading the successive connections across all the hosts.
- MacDNS caches information for hosts on the Internet. This decreases network traffic on the link to the Internet (which is often slower than the local area network) and gives faster responses to these queries.
- Once you've configured the program with information about hosts, MacDNS handles the DNS queries for an entire site. Your Internet service provider (ISP) need not be consulted for any new hosts that are installed at a site.
- MacDNS acts as a primary DNS server. It exports its zone information, allowing another DNS server to provide secondary name service. MacDNS does not act as a secondary server—it does not import zone information from another DNS server.
- MacDNS automatically maintains address-to-name mappings for all hosts in a zone. It supports zone transfer requests from a secondary server for any reverse domain for which MacDNS is authoritative.

The rest of this guide explains how to install and use MacDNS software.

2 Installing and Setting Up MacDNS

This chapter describes how to set up your MacDNS software and also describes how to register your domain name.

System requirements

The MacDNS application is supported on the following hardware:

- a PowerPC-based Internet Server from Apple Computer

Your system should also include:

- at least one (1) megabyte of free random-access memory (RAM)
- MacTCP 2.0.6 or later, or Open Transport version 1.1 or later

Note: For best performance, Apple recommends that you use Open Transport (version 1.1 or later) instead of MacTCP with this version of MacDNS software. Open Transport 1.1 is part of System 7.5.3; if your server computer did not come with System 7.5.3 installed, you can install System 7.5 Update 2.0 (be sure to read the "Installing This Update" Read Me file, which accompanies the system update, for details about making Open Transport active). For information about obtaining the system update, see the following Web site:

`http://support.info.apple.com/update/update.html`

- System 7.5.1 or later (System 7.5.3 recommended)
- a network connection to the Internet (an Ethernet connection will give the highest speed, although a LocalTalk connection will work adequately)

Before you install

Prior to installing the MacDNS application, you should register your domain name and configure the MacTCP or TCP/IP control panel, as described in the following two sections.

Registering your domain name

Before you can use the MacDNS program for primary name service, you need to select a domain name and register your domain. Your domain name is the name that is used in tables and lists associating the domain with the domain server addresses.

Different domains have different registration processes. Your Internet service provider should be able to provide you with details about registering your domain name.

Note: To choose an appropriate name, you need to know where your organization fits within the overall Internet domain name space (see the appendix for more details about domains). Generally, shorter names are better than longer ones. Make sure the name you choose is easily remembered or user friendly.

Many sites are able to register directly with the Network Information Center (commonly referred to as *InterNIC*). You can find out more information about InterNIC registration services by using one of the following:

URL:	`http://rs.internic.net/rs-internic.html`
E-mail:	HOSTMASTER@INTERNIC.NET
Phone:	(703) 742-4777
Postal mail:	Network Solutions InterNIC Registration Services P.O. Box 1656 Herndon, VA 22070

Several of the references in the section “For More Information” in the preface also contain useful information about domain name registration (for example, you can search the Gopher database indicated in the preface to see whether a domain name is already taken).

Configuring your TCP/IP settings

Before you install MacDNS, your MacTCP or TCP/IP control panel should be configured correctly. If you've already installed and set up the Apple Internet Server Solution software, your TCP/IP settings should be configured, and you don't need to do anything more. Skip ahead to the next section of this guide.

If you haven't installed the Internet Server Solution software, you should do so now; configure your TCP/IP settings according to the instructions provided in your Internet Server Solution documentation.

Installing MacDNS and creating an alias for automatic startup

Unless you intentionally quit MacDNS for some reason, the program runs as long as your server computer is turned on. Because you need MacDNS to be up and running as much as possible, you should place an alias to the MacDNS application in your Startup Items folder within your System Folder. This ensures that MacDNS will start up after power failures, crashes, and so forth. When MacDNS starts up, it will open all the zone files that were open when it was last running.

To install MacDNS and create an alias for automatic startup:

1. **Drag the MacDNS icon to your hard disk and put the program in a convenient folder.**
2. **Click the MacDNS icon to select it (if it isn't selected already), and choose Make Alias from the File menu in the Finder.**
3. **Open the System Folder on your hard disk.**
4. **Move the alias of the MacDNS program to the Startup Items folder of your hard drive's System Folder.**

After installing MacDNS, you should:

- open the MacDNS application and create one or more zone files
- configure the parent server information
- enter information about the hosts in each zone

The following sections explain these procedures.

Starting the MacDNS program

To start the MacDNS program, you simply need to open it:

- **Double-click the MacDNS icon.**

  The first time you open the MacDNS program, a license agreement appears. Click the Accept button to accept the terms of the agreement.

  Once you open the MacDNS program, name service is started automatically. A MacDNS Preferences file is created automatically in the Preferences folder of your hard disk's System Folder. The first time you use the program, you need to configure the software for any actual name service to occur; once you do, you don't need to do anything else (such as restarting your computer) for name service to take place.

Creating a zone file

The part of the Internet domain name space for which your MacDNS server contains information is called its *zone* of authority. You need to provide your MacDNS software with details about your particular zone.

To create a zone file with the information about your zone:

1. **Choose New Zone File from the File menu.**

   A Zone Information dialog box appears, with an untitled host list window for the zone file underneath it.

   IMPORTANT When you first see the Zone Information dialog box, its text boxes contain "templates" of the information you need to enter. You can follow the style of the template when you provide the information for your own zone. In the instructions that follow, make sure the template information is selected for a particular text box, then type your own zone's information (the template text should be completely deleted or replaced).

2. **In the Zone Information dialog box, type the domain name of your zone in the Domain Name box.**

   The domain name should be the name you've registered, as explained previously in the section "Registering Your Domain."

3. **Type the DNS name of your server computer in the Primary Server box.**

   Note: Make sure you type a DNS name, which is different from the name you may have chosen for your computer for Macintosh file sharing.

4 **Type the name of a secondary server for the zone in the Secondary Server box.**

A secondary server keeps a copy of your zone's information; a secondary server is useful for spreading the name-service load across multiple machines and for ensuring that a zone has name service even if the primary server fails.

5 **Type your E-mail address in the Administrator box.**

Your address will be useful to other administrators who may need to contact you for help debugging problems that arise.

6 **Type an amount in the Refresh Interval box and choose a unit of time from the adjacent pop-up menu (or confirm the default value).**

The Refresh Interval indicates how often a secondary server will query your MacDNS name server to see if new information is available. If something has changed, the secondary server updates its information; the process of updating is referred to as a *zone transfer.*

The recommended Refresh Interval is 8 hours.

7 **Type an amount in the Retry Interval box and choose a unit of time from the adjacent pop-up menu (or confirm the default value).**

The Retry Interval represents the amount of time a secondary server will wait before reattempting to contact the MacDNS server if the first attempt has failed.

The recommended Retry Interval is 2 hours.

8 **Type an amount in the Expire Interval box and choose a unit of time from the adjacent pop-up menu (or confirm the default value).**

The Expire Interval is the amount of time a secondary server will cache zone information it has already received if the MacDNS server can't be reached to provide a zone transfer. The purpose of the Expire Interval is to set a time at which the zone data can no longer reasonably be regarded as up to date; after that point, the data is not considered useful, and it's better for the secondary server to provide no data than obsolete data. Once the Expire Interval limit is reached, the secondary server removes all data about your MacDNS server from its database.

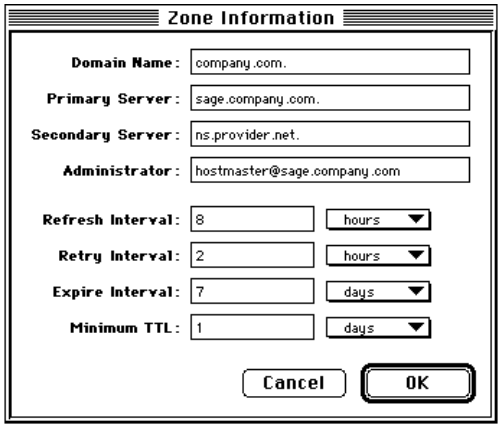
The recommended Expire Interval is 7 days.

9 Type an amount in the Minimum TTL box and choose a unit of time in the adjacent pop-up box (or confirm the default value).

TTL stands for *time to live*. The Minimum TTL is the minimum time to live for an entry in the MacDNS database.

The recommended Minimum TTL is 1 day.

The following figure shows an example of a completed Zone Information dialog box:



Note: The values for the Refresh, Expire, and Minimum Intervals as shown in the figure are the recommended settings for keeping your zone up to date without excessive network traffic.

10 Click OK.

After you click OK, the title of the host list window changes to the name you entered as the domain name in the Zone Information dialog box. The name is preceded by a diamond until you save the zone file.

IMPORTANT To ensure that you have a permanent record of the host information for your zone, be sure to save the zone file (choose Save from the File menu).

Configuring your parent server

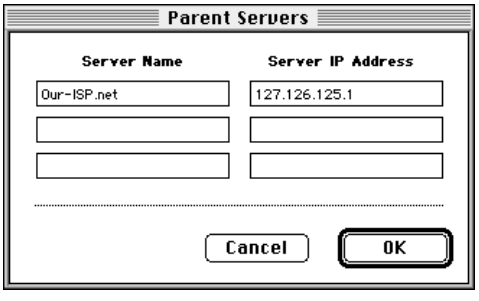
The MacDNS server relies on other DNS servers (called *parent servers*) for answers to queries that it doesn't have in its own database. In general, the MacDNS server should use the DNS server for your Internet service provider as its parent. You may also enter other servers to be alternate parents, which will be used if the first parent server isn't available.

MacDNS uses the DNS information that is configured in the MacTCP or TCP control panel to obtain a default list of parent servers. If that information has not been configured or is incorrect, you will have to configure the parent server(s) yourself.

To verify that your parent server information is correct, or to add alternate parent servers:

1 **Choose Set Parent Servers from the Hosts menu.**

A dialog box similar to the following one appears.



2 **Make sure that the default parent server information is correct; if it isn't, select the server name or the server IP address and type the correct information.**

3 **If you want to add alternate parent servers, type the appropriate information in the Server Name and the Server IP Address boxes, respectively.**

4 **Click OK.**

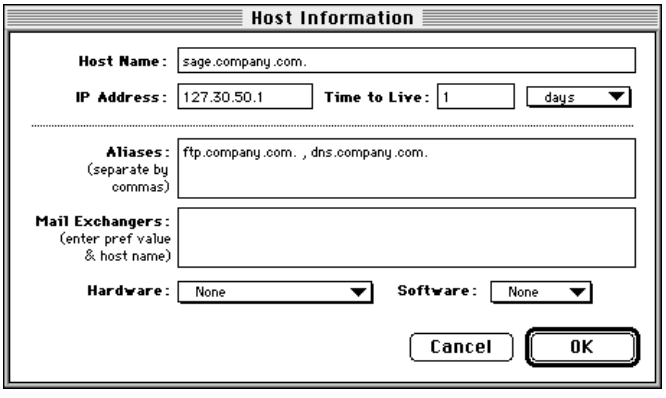
Note: When you click OK, the new parent server information takes effect immediately; you don't need to restart the MacDNS application.

Adding hosts

To add information about a host computer:

1 **Choose Add Permanent Host from the Hosts menu.**

The Host Information dialog box appears. The following figure shows an example of a Host Information dialog box; note that most of the information has been entered according to the subsequent task steps in this section.



2 **Type the name of the host in the Host Name box.**

When the Host Information dialog box first appears, a "template" name appears in the Host Name text box.

The host name is the canonical or "real" name of the host. You assign this name permanently to the host. The host name must include the domain name; since the domain name is automatically included as part of the template, all you need to do is select "a-permanent-host" and type the first part of your host's name.

3 **Type the IP address assigned to the host in the IP Address box.**

4 **Type an amount in the "Time to Live" box box and choose a unit of time in the adjacent pop-up menu; or, confirm the default setting.**

The Time to Live indicates the amount of time that a remote DNS server can cache information about this host. The default is the minimum time-to-live value for the zone, which is usually a good choice.

5 **(Optional) Type the name of aliases for this host in the Aliases text box.**

The names you type must be separated by commas. Each name must be a fully qualified domain name.

Note: You cannot use an alias name that does not include the domain name of the host. For example, you can use "www.company.com" for an alias of "sage.company.com," but you can't use "www.provider.com," because "provider.com" is outside of the "company.com" zone. To work around this restriction, you can create a new zone file for the "provider.com" domain and add "www.provider.com" as a permanent host. You can then assign the IP address of the "real" host machine (sage.company.com) to this host.

6 **(Optional) Type mail exchanger information in the Mail Exchangers text box; each entry you type must consist of a numeric preference value, followed by a space, then the name of the host that will either process or forward mail for the host that you are adding.**

The mail exchangers are alternate hosts to which mail may be sent for ultimate delivery to this host (see the appendix for more details about mail exchangers).

The preference value indicates the mail exchanger's priority; the lower the number, the greater the preference. The value itself isn't important, as long as the number for the mail exchanger that you want to be used first is lower than than the values for any other mail exchangers you've entered.

Multiple entries must be separated by a comma.

The following example indicates the correct format for an entry that includes two mail exchangers:

```
10 E-mail.webewidgets.com, 20 Ur-mail.webewidgets.com
```

7 **(Optional) Select the computer type for the host you're adding in the Hardware pop-up menu.**

If you leave "None" selected, no computer type will be returned for host information queries from other DNS servers.

8 **(Optional) Select the operating system for the host you're adding in the Software pop-up menu.**

If you leave "None" selected, no operating system type will be returned for host information queries from other DNS servers.

9 **Click OK.**

Adding hosts that require a mail exchanger only

The MacDNS program allows you to designate hosts that need mail exchange service only and no other Internet services. If a host needs special handling of its mail delivery only, you don't need to assign an IP address, but you can assign a mail exchanger. Such hosts are referred to as *MX-only hosts.*

An MX-only host is most commonly used when your domain name itself is not an actual host computer. You can use the domain name as the MX-only host name, then use the name of your local E-mail host (and possibly your Internet service provider's E-mail host, if you have made arrrangements to do so) as the mail exchanger.

To assign a mail exchanger for an MX-only host:

1 **From the Hosts menu, choose Add MX-Only Host.**

The MX-Only Host Information dialog box appears.

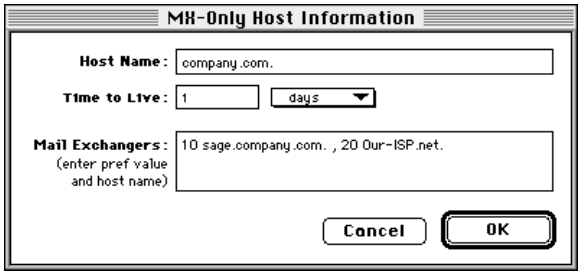
2 **Type the name of the host in the Host Name text box.**

3 **Type an entry in the "Time to Live" box and select a value from the adjacent pop-up menu; or confirm the default value.**

The default time-to-live value is the minimum TTL for the zone, which is usually a good choice.

4 **Type the numeric preferences and the names of hosts to act as mail exchangers in the "Mail Exchangers" text box.**

Multiple entries should be separated by a comma. The lower the number you assign as a preference value, the greater the preference is for a host to act as a mail exchanger.



5 **Click OK.**

Creating a load-sharing group

The MacDNS program allows you to set up load sharing among several hosts in its zone. When you set up MacDNS to perform load sharing, MacDNS will return the address of one host out of a group when it is queried for the name of that group.

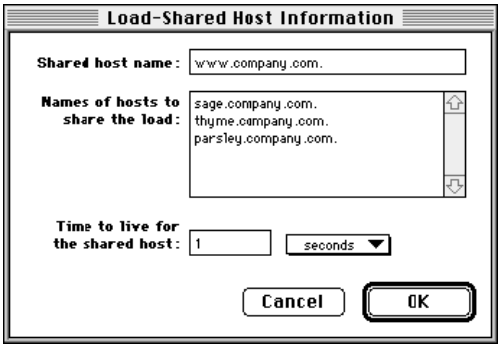
For example, a site administrator could install Web servers on three hosts, each with identical data. The administrator could then assign a name to the collection of three hosts. MacDNS would then respond to queries for that name with one of the three hosts, in round-robin fashion. This kind of load-sharing arrangement is referred to as a *RAIC* system, or *redundant array of independent computers.*

For load-sharing groups, the TTL is generally kept to a small number of seconds. This prevents information about any one host from dwelling in a remote cache for a long time and prevents that host from being swamped by requests due to the cached information.

To create a load-sharing group:

1. **In the host list window, Shift-click to select a group of hosts that you want to have as a load-sharing group.**
2. **Choose Share Load from the Hosts menu.**
   The Load-Shared Host Information dialog box appears.
3. **Type the name of the load-sharing group in the “Shared host name” text box.**
4. **Confirm that the host names in the “Names of hosts to share the load” text box are the ones you want.**
   The names appear automatically; they are the names you selected in the host list window.

5 **Type a value in the “Time to live for the shared host” box and choose a unit of time from the adjacent pop-up menu; or, confirm the default setting.**



6 **Click OK.**

Address-to-name mapping

On the Internet, a special domain named in-addr.arpa is used to support address-to-name mapping. The in-addr.arpa domains are represented using the network number in reverse. For example, the in-addr.arpa domain for network 123.45.67.0 is represented as 67.45.123.in-addr.arpa. As the administrator of a particular domain, you are usually also responsible for the corresponding in-addr.arpa domain that reflects the portion of the Internet address space that you’ve been assigned: your reverse domain.

MacDNS automatically maintains reverse domains for you; there’s no need to create a separate zone file for your in-addr.arpa domain, or to worry about keeping the address-to-name mappings synchronized.

The MacDNS server will automatically respond to all pointer queries, which are requests to the name server to return the correct domain name for a machine with a specified Internet address. MacDNS also supports zone transfer requests from a secondary server for any reverse domain for which MacDNS is authoritative.

MacDNS will answer authoritatively for queries involving an in-addr.arpa domain corresponding to a network number in which one or more permanent hosts are being served. For example, if MacDNS is serving one or more hosts on network 204.96.16.0, it will respond authoritatively for the 16.96.204.in-addr.arpa domain.

Reverse domains and serving multiple domain names with the same IP address

If you are serving multiple zones, and have two or more permanent host entries mapped to the same IP addresss, you cannot specify which name will be returned when an in-addr.arpa lookup is requested. MacDNS searches for the first matching name for the IP address, starting in the zone that was opened first.

For example, if the hosts www.provider.com and www.vanity.com both have the IP address 127.26.25.24, a reverse lookup for 24.25.26.127.in-addr.arpa will yield www.provider.com if the provider.com zone file was opened before the vanity.com zone.

To ensure that MacDNS returns a particular name for a reverse lookup when more than one name is mapped to an IP address, you can create or open the zone file containing the canonical host entry for the duplicate IP address first.

3 Managing Your MacDNS Server

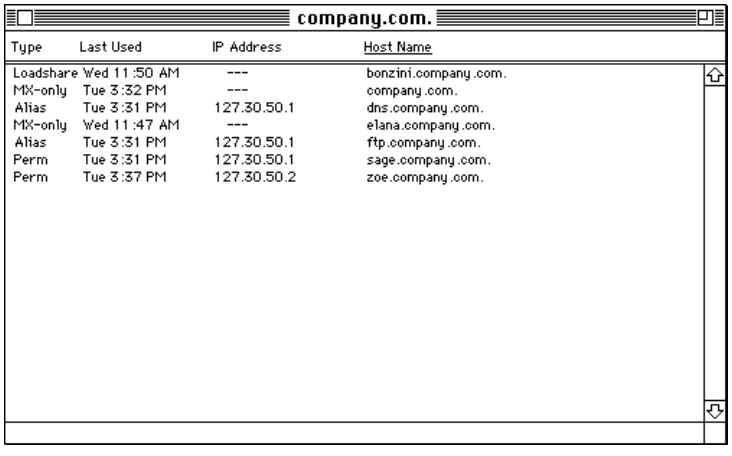
Now that you've set up your MacDNS server, you may want to modify information about your zone(s) or about your MacDNS hosts. You may also want to view the status of domain name services provided by your MacDNS server. This chapter explains these procedures.

About the host list window

The host list window, which displays the title you assigned to the zone in the Zone Information dialog box, lists and contains information about all of the hosts that make up the zone. When you create or modify information in a zone file, the title of the host list window is preceded by a diamond (◆) until you choose Save from the File menu and save the information.

When MacDNS receives queries about hosts, it searches the information from its internal database for the zone and sends a reply. There is one window for each zone; thus, if you set up MacDNS name service for "webewidgets.com" and "non-profit.org," you would have a separate window for each zone.

The following figure shows an example of a host list window:



The columns in the host list window indicate the type of information that is displayed:

Type	Indicates the type of host: Perm is the canonical (“real”) name of a host that you’ve registered in the MacDNS software. Alias is an alias to a “permanent” host. Loadshare designates several hosts that are sharing a load. MX-only is a host that requires mail-exchange service only.
Last Used	Refers to the time the host was created, changed, or last queried.
IP Address	Indicates the IP address assigned to the host. Certain hosts do not have a real IP address, so this column contains “---”.
Host Name	Refers to the name of the host.

If you want to change the order of the way the information is presented:

- **Choose the way you want to view the host information (by Type, Last Use, IP Address, or Name) from the View menu; or, click the appropriate column heading in the host list window.**

  The host list information is rearranged according to the ordering method you indicated.

  Note: You can’t close a host list window without discontinuing name service for its zone. To reduce the clutter on your screen that may occur if you have multiple zones (and thus multiple host list windows), you can choose either the Move To Back or the Hide Window option from the Window menu. You can reopen a host list window by choosing its name from the Window menu; you can also make a window the front-most window by choosing its name from the Window menu or by clicking in the window itself.

Modifying the zone file

To change global information about the domain that you’ve entered into your zone file:

1. **Make sure that the host list window for the zone you wish to modify is the front-most window.**

   Click in the appropriate window or select the name of the zone from the Window menu.

2. **Choose Set Zone Information from the Hosts menu.**

   The Zone Information dialog box appears.

3 **In the appropriate text box, select the old information and delete it, and type any new information; if necessary, choose a new interval from one or more of the pop-up menus.**

4 **Click OK.**

The new information takes effect immediately.

IMPORTANT Changing your domain name or the minimum time to live will affect all the hosts in your zone.

Modifying host information

If you want to change information about hosts:

1 **Double-click the entry for the host in the host list window; or, select the host entry and choose Modify Host from the Hosts menu.**

Depending on the type of host that you're modifying, the Host Information dialog box, the Load-Shared Host Information dialog box, or the MX-Only Host Information dialog box appears.

2 **Modify the information you want in the dialog box that appeared in step 1.**

3 **Click OK.**

Deleting hosts

To delete one or more hosts from your MacDNS name server:

1 **Select the entry of a host from the host list window; Shift-click to select multiple entries.**

2 **Press the Delete key; or, choose Clear from the Edit menu.**

The following dialog box appears:

3 **Click OK.**

Adding hosts to a load-sharing group

To add new hosts to an existing load-sharing group:

1. **In the host list window, select the new host(s) and Shift-click to select the load-sharing host name.**
2. **Choose Share Load from the Hosts menu.**
3. **In the dialog box that appears, click OK.**

   Note: You can also copy and paste new hosts in the Load-Shared Host Information dialog box. Select the new host(s) that you are adding to the load-sharing group and choose Copy from the File menu. Double-click an entry for a Loadshare host in the host list window, click in the "Name of hosts to share the load" box, and choose Paste from the File menu. Click OK to accept the change.

Deleting hosts from a load-sharing group

To delete a host from an existing load-sharing group:

1. **Select the load-sharing host name in the host list window.**
2. **In the Load-Shared Host Information dialog box, select the host(s) you wish to delete.**
3. **Choose Cut or Clear from the Edit menu; or press the Delete key.**
4. **Click OK.**

Temporarily removing a host from a load-sharing group

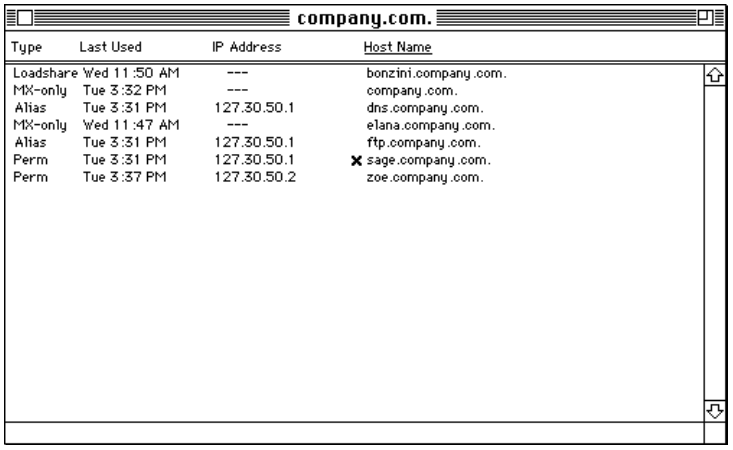
From time to time, one of the hosts in a load-sharing group may fail. When this happens, name service requests that attempt to use that load-sharing group will fail sporadically (because one member of the shared group is not operating.) MacDNS offers a way to remove a host from a group temporarily so that queries for the shared service aren't routed to the disabled computer.

To remove a host from a load-sharing group temporarily:

1. **In the host list window, select the host to be removed from the group.**
2. **Choose Disable Sharing from the Hosts menu.**

The host remains part of the load-sharing group, but MacDNS will not return an address for that host any time the load-sharing host is requested. Note that this affects all the groups to which the host belongs. MacDNS will respond with the proper information if the request is for the host itself, and not one of the load-sharing hosts.

When a host is disabled, the entry for a host changes to include an **X** before the host name to show that it's no longer sharing part of the load.



To re-enable sharing by a host:

1. **Select the host in the host list window.**
2. **Choose Enable Sharing from the Hosts menu.**

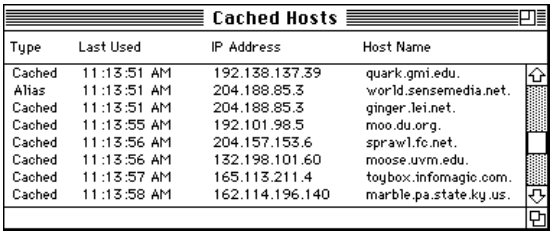
Viewing the cache

Like other DNS servers, MacDNS keeps a cache. Whenever MacDNS receives a query for information that is not in its database, it sends the query on to a parent server. Once MacDNS receives information from the parent server, it adds that information to its cache and responds to the original requester. Subsequent queries for the same information are then answered more quickly.

To view the cache:

- **From the Window menu, choose Cached Hosts.**

A window similar to the following appears:



The cached query responses are kept in a window that is similar to the host list window, with the following exceptions:

- Although double-clicking will open an entry to view its current values, no values can be changed (the OK button is dimmed to prevent this).
- There are several listings for Type:
  —*Cached* entries
  —the *Negative* entry, which indicates that there is no such host (and that the parent server has said so authoritatively)
  —the *NoResp* entry, which indicates that MacDNS could not get a response from any parent server for the record

The latter two types have a time to live of two minutes, which minimizes the number of requests over the Internet for nonexistent hosts.

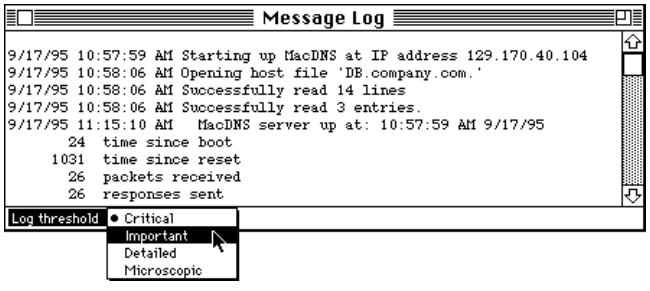
Viewing the Message Log

The MacDNS server keeps a history of significant events that occur during its operation. The information is displayed in the Message Log window. To view the Message Log:

- **Choose Message Log from the Window menu.**

The Message Log window appears.

Each entry in the Message Log indicates a date and time and a text message. At the bottom of the window is a pop-up menu that controls the level of detail that appears in the Message Log window, as shown in the following figure:



The levels of detail are:

Critical	Messages about significant changes or errors.
Important	Messages about erroneous queries that have been received; low-memory conditions within MacDNS; other warnings, including all Critical messages.
Detailed	A summary of query packets as they arrive as well as messages from the Critical and Important levels.
Microscopic	All messages, with detailed notices of events that occur during normal operation.

You can use the Message Log to view various statistics that have been gathered by MacDNS software during its operation, as explained in the next section. In addition, you can use the Message Log to view the contents of trapped packets, as explained in the section “Trapping Packets” later in this chapter.

The MacDNS program creates a log file that keeps the same information as displayed in the Message Log window. The file is created in the same folder as the MacDNS program.

Viewing server statistics

To view various statistics gathered by the MacDNS program:

- **Choose Show Query Counts or choose Show Requesters from the Stats menu.**

  If you choose Show Query Counts, a detailed summary of all queries received by MacDNS is displayed in the Message Log window.

  If you choose Show Requesters, the IP addresses of all machines that have requested information from MacDNS are displayed in the Message Log window.

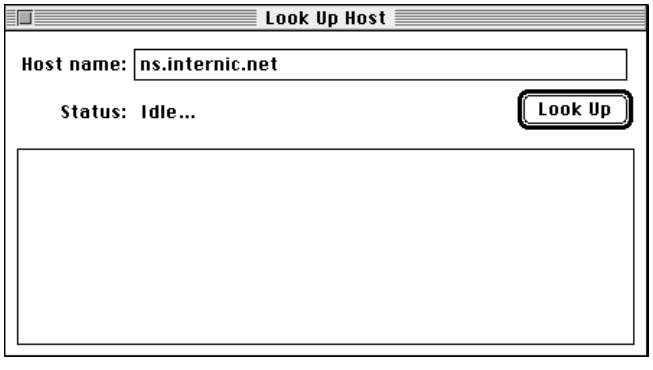
Looking up host addresses

You can use MacDNS to look up information about other hosts. To do so:

1. **Choose Look Up Host from the Window menu.**

   The Look Up Host window appears.

2. **Type the name of the Internet host for which you want information in the "Host name" text box.**



3. **Click Look Up.**

   MacDNS will first query its own database; if necessary, it will then look on the Internet for an answer to the query.

   All the information that returns for the host for which the query was made is displayed in the box at the bottom of the Look Up Host window. Error indications appear in the Status area in the middle of the window.

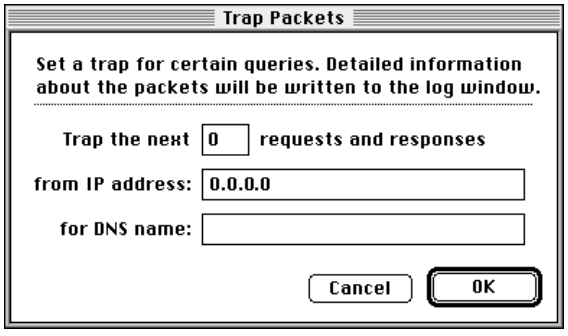
Trapping packets

To identify and solve DNS problems, you may find it's helpful to watch the contents of packets going to and from the MacDNS server. As an alternative to an expensive "packet sniffer," MacDNS offers a two-stage trap facility for displaying certain packets. The data and detailed processing information of the trapped packets is written to the Message Log window.

To trap packets:

1 **Choose Trap Packets from the Stats menu.**

The Trap Packets dialog appears.



2 **Type a number in the "Trap the next" box to indicate the number of packets to examine.**

3 **Type a number in the "from IP address" text box to indicate the IP address of the device that sent the query; or leave the field blank to trap packets from any IP address.**

4 **Type a name in the "for DNS name" text box to indicate the DNS name in the query; or leave the field blank.**

5 **Click OK.**

Note: You can leave either the IP address or DNS name fields (or both) empty. In this case, an empty field will match any packet. If both an IP address and DNS are specified, only packets matching both criteria will be trapped.

Result codes for trapped packets

The following abbreviations may appear in the Message Log window after you've set the Trap Packets option and a query has been made to the name server; an explanation of each of the abbreviations is provided.

ID A 16-bit identifier assigned by the program that generates any kind of query. This identifier is copied the corresponding reply and can be used by the requester to match up replies to outstanding queries.

QR A one-bit field that specifies whether this message is a query (0) or a response (1).

OPCODE A four-bit field that specifies kind of query in this message. This value is set by the originator of a query and copied into the response. The values are:

0	a standard query (QUERY)
1	an inverse query (IQUERY)
2	a server status request (STATUS)
3–15	reserved for future use

AA Authoritative Answer; this bit is valid in responses, and specifies that the responding name server is an authority for the domain name in question section.

Note that the contents of the answer section may have multiple owner names because of aliases. The AA bit corresponds to the name that matches the query name, or the first owner name in the answer section.

TC TrunCation; specifies that this message was truncated due to length greater than that permitted on the transmission channel.

RD Recursion Desired; this bit may be set in a query and is copied into the response. If RD is set, it directs the name server to pursue the query recursively. Recursive query support is optional.

RA Recursion Available; this bit is set or cleared in a response, and denotes whether recursive query support is available in the name server.

Z Reserved for future use. Must be zero in all queries and responses.

RCODE Response code; this 4-bit field is set as part of responses. The values have the following interpretation:

- 0 No error condition.
- 1 Format error. The name server was unable to interpret the query.
- 2 Server failure. The name server was unable to process this query due to a problem with the name server.
- 3 Name error. Meaningful only for responses from an authoritative name server, this code signifies that the domain name referenced in the query does not exist.
- 4 Not implemented. The name server does not support the requested kind of query.
- 5 Refused. The name server refuses to perform the specified operation for policy reasons. For example, a name server may not wish to provide the information to the particular requester, or a name server may not wishto perform a particular operation (for example a zone transfer) for particular data.
- 6–15 Reserved for future use.

QDCOUNT An unsigned 16-bit integer specifying the number of entries in the question section.

ANCOUNT An unsigned 16-bit integer specifying the number of resource records in the answer section.

NSCOUNT An unsigned 16-bit integer specifying the number of name server resource records in the authorityrecords section.

ARCOUNT An unsigned 16-bit integer specifying the number of resource records in the additional records section.

Appendix
How the Domain Name System Works

Internet host computers are assigned IP (which stands for *Internet Protocol*) addresses by their administrators. These addresses must be globally unique within the Internet. When connecting to the Internet, a site receives a range of IP addresses from its Internet service provider. The site's administrator then assigns these addresses to the individual host computers at the site.

However, numeric addresses are awkward to deal with. A much better way to identify hosts is to use a name and employ a mechanism to convert the host name to its corresponding address. A *domain name server* provides such a mecnanism—it manages the mapping between names and IP addresses. The server is a program running on a computer that receives queries about a particular host, finds information about that host, and sends that information back to the requester.

A hierarchy of names

The Internet is believed to comprise somewhere between 3 and 20 million host computers. It would be quite unworkable to have a single database of names and addresses for all these hosts. Not only would there be an astonishing flow of information, but it would always be out of date. Instead of using a central database, the Domain Name System (DNS) is a distributed database.

The DNS universe of names is divided into *domains*, which are further divided into *subdomains*. The top-level is divided into a few hundred domains: there are the familiar "edu", "com", "gov", "net", and "org" domains, as well as two-letter domains for each country ("us" for the United States, "it" for Italy, and so forth). Each of these top-level domains is *delegated* to a particular organization called an *authority*. An authority may then delegate subdomains to other organizations. This delegation process continues downward until it gets to the level of an organization such as a company.

Each authority runs a DNS server, and is responsible for entering the names of its subdomains. Furthermore, that DNS server keeps the address of each of its subdomains' DNS servers in its database. The information kept in a DNS server is called its *zone* of authority.

When a request for a host in a particular subdomain arrives, the authority's DNS server directs the query to the next server "down the line." That's where MacDNS comes in: it's the DNS server for an organization. The Internet service provider for a site will have delegated responsibility for your zone to a particular DNS server—MacDNS. Your site's administrator can then enter the names, addresses, and other information about the computers that are to be "visible" on the Internet. Any request for a host in your subdomain will be sent to the MacDNS program. MacDNS will use its database to determine the proper response.

A word about notation

Domain names

Domain names are composed of a sequence of *labels*, separated by periods (".") Labels may consist of letters, digits, and the dash ("-") character, and may not start or end with a dash. Names are not case-sensitive—that is, "milk" is equivalent to "MILK," or even "MiLk."

The labels of a DNS name follow directly from the sequence of delegated domains and subdomains. To read a domain name for any host, start on the right. The "root" (or parent) of all domain names is given the name "." (that's a period, all by itself). Each subdomain is separated from the next with another "." Thus, the name "whitehouse.gov." is a host in the top-level "gov" (for government). The name "Rocky-Road.Rockville.MD.US." represents a host called "Rocky-Road" in the "Rockville" subdomain which is part of the "MD" (Maryland) subdomain, which itself is part of the top-level U.S. domain.

DNS names are generally pronounced as a sequence of words, with the word "dot" between the labels. Thus the previous entry would be read aloud as "rocky dash road dot rockville dot em dee dot you ess dot."

IP addresses

An IP address is a globally unique, 32-bit number. Each host connected to the Internet is assigned a unique number. These IP addresses are usually written in the form of four decimal numbers, separated by dots, such as 129.170.16.4. Each of these numbers (between the dots) is in the range 0 to 255 (an eight-bit number).

When a site receives a domain name from their internet service provider, they will also receive a range of IP addresses from which to assign host computers.

Caches and time-to-live values

As mentioned earlier, the Domain Name System relies on DNS servers to provide information about the hosts at a site. Whenever a person wants to use a service anywhere on the Internet, the person's computer sends a request to a local DNS server, which might query several other DNS servers before receiving an answer (the IP address of the remote computer).

Doesn't this pose a significant amount of traffic on the network? Actually, yes it does. But a simple mechanism keeps this traffic down. DNS servers can keep a copy of the information they receive in memory called a *cache.* Just as a RAM cache speeds up access to data on a hard drive, this cache of DNS information speeds up the response to certain queries. In addition, the cache decreases the number of times that a request must be sent out across the network for any piece of information.

But won't the information in the server's cache become out of date? Yes, again. To prevent this from being a problem, each piece of information in a DNS server is given a "time to live" (TTL). The TTL is the number of seconds a server is allowed to cache and use a particular piece of information. A site administrator assigns a TTL to each host when setting up the other information. Each response returning from a remote DNS server contains that TTL, and the information is only kept in the cache while the TTL is valid.

In general, TTLs for host computers should be at least one day.

Zone transfers

MacDNS acts as a primary name server. That means that it is the "true" authority for a particular zone. For robustness, the Domain Name System allows secondary servers to keep a copy of the zone's information. The secondary server obtains its information from the primary server for a zone. Rather than attempting to query the primary server for each of its hosts, one at a time, there is a zone transfer mechanism that moves all the information in a single operation. (You cannot configure MacDNS to be a secondary server, though you can control how often MacDNS distributes information to secondary servers.)

The zone transfers happen on a periodic basis. The secondary server uses three parameters to control the timing:

The *refresh* timer tells the secondary how often to query the primary server to see if new information is available. If something has changed, the secondary then does a zone transfer.

The *retry* timer tells how long the secondary should wait before reattempting to contact the primary if the first attempt failed.

The *expire* timer tells how long to cache the zone information in the event that the primary cannot be reached. If this timer lapses, then the secondary server removes all information about the primary from its database.

Information in a DNS server's database

A DNS server keeps a database of all the hosts in its zone. In addition to a host's DNS name and IP address, a DNS server can store hardware and software information, its aliases, and mail exchanger information about the host. Note that each of these pieces of information have an associated time to live. These items will be explained in the following paragraphs.

A host's *hardware* and *software* information is a general description of the hardware and operating system for a host. The standard types listed in the DNS specification and other standards documents don't usually provide exact information about a particular computer. For example, the allowed hardware types for a Macintosh computer are: MAC-II, MAC-POWERBOOK, and MACINTOSH; the allowed software type for a Macintosh is simply MACOS (that is, the Macintosh Operating System).

A host may have one or more *aliases*—alternate names that are treated the same as a reference to the host's real (or *canonical*) name. The DNS server will return the requested information for that host, as if the query came in for the canonical name. Aliases are convenient for decoupling a service name from a host's real name. That is, an administrator can give out an alias for a service. People use that alias to connect to the host. As the load on the server grows, the administrator can move the server to another (presumably faster) computer. By reassigning the alias, the administrator can redirect queries to the new computer without requiring users to make changes.

A DNS server keeps *mail exchanger* information about its hosts. When E-mail is sent, it is often relayed through several host computers until it reaches the ultimate destination. These relay hosts are called *mail exchangers.* An administrator assigns different priorities to each of the mail exchanger hosts, depending on how desirable that host is. For example, the most desirable host is, obviously, the destination host. But if that host is down, or not reachable (perhaps it's on a dial-up line), mail to that destination could be sent to a "closer" host that has agreed to relay the messages. (For more information about mail exchangers, see the last section in this appendix.)

Mail exchangers

DNS provides a facility for designating that E-mail for a site should be sent to one of several hosts. When E-mail is to be delivered to a site, the sender attempts to deliver it to the ultimate destination. If that computer is down, or if it is not available at the moment (possibly because it establishes a dial-up connection to receive mail), the sender can deliver messages to an alternate host that will, in turn, attempt to deliver the message at a later time. The site's administrator could define a series of these hosts (known as "mail exchangers" or "MX hosts") with different priorities:

```
company.com        MX    10 E-mail.company.com
company.com        MX    20 Our-ISP.net
```

In this example, the administrator has specified that the most important mail exchanger (MX host) for company.com is the host named E-mail.company.com. You can tell this because the priority (10) is *lower* than any other hosts. (This seems backwards, but it's the normal usage of the DNS.) The other host, Our-ISP.net, is to be used as a backup, and it has been given a lower priority (a *higher* number).

This allows the site administrator to assign people E-mail addresses that use the person's name with "@company.com" as a suffix. Thus, the receptionist for the hypothetical company could be:

chris.jones@company.com

When someone sends a message to that address, the sending computer queries for the mail exchangers for company.com, and learns that there are two choices. If a message can't be sent directly to the host E-mail.company.com, a sender will instead send the message to the computer named Our-ISP.net. Presumably, the administrator of company.com has arranged for mail forwarding service with that administrator of Our-ISP.net.

An example of DNS at work

Within an organization, there's a strong similarity between the Domain Name System and a telephone directory. Each provides a mechanism for assigning a human-readable name to a device (a telephone or a computer) that needs a numeric value (a telephone number or an IP address) before the actual "communication" can take place.

Let's take an example of a hypothetical company with several employees, and compare it to computers using a DNS server. In the company, each employee has a telephone, and each has a unique telephone number. Employee perform one (or many) tasks: for example, the receptionist answers calls from the outside, and might also be responsible for running the fax machine, and scheduling the conference rooms. The company's directory, in part, would look like this:

Chris Jones	(Receptionist)	ext. 23
Susan Blodgett	(Sales)	ext. 45
Ron Smith	(Sales)	ext. 47
Sam Twiddle	(Sales)	ext. 19
Jen Smythe	(Net administrator)	ext. 32

Receptionist	ext. 23
Fax	ext. 23
Conference Room	ext. 23
Sales Department	ext. 50
Network Repair	ext. 32

Notice that the tasks of the Receptionist, Fax, and Conference Room scheduling are all handled by Chris Jones at extension 23.

The Domain Name System works much the same way. Let's imagine a company that has three computers that act as electronic mail, FTP, Web, Gopher, and DNS servers. The site administrator is a gourmet cook, so has chosen to name the computers after spices. The name and IP address assignments for that site might then be:

sage.company.com	127.30.50.1
thyme.company.com	127.30.50.2
parsley.company.com	127.30.50.3

The information above means that host sage.company.com has the IP address of 127.30.50.1, and that thyme.company.com has IP address 127.30.50.2.

These computer names are directly analogous to the names and telephone extensions shown in the company's directory above—each (real) person has been assigned a unique telephone number, and each computer has a unique name and address.

In addition to assigning addresses and names to the computers, the site administrator must also assign the tasks of FTP, Web, Gopher, E-mail, and so forth to these computers. Rather than use the computer's IP address, the Domain Name System allows each function to be assigned an alias that specifies a "real" (or "canonical") name, which in turn specifies the IP address of the computer. The site's administrator might create these aliases for the following services:

FTP.company.com	sage.company.com
WWW.company.com	thyme.company.com
E-mail.company.com	thyme.company.com
Gopher.company.com	parsley.company.com

Each line above means that the name on the right is the "real name" for the name on the left. Equivalently, this may be read that the name on the left is an alias for the name on the right.

Thus, when a request for the IP address of FTP.company.com arrived at the site's DNS server, it would first discover that FTP.company.com was an alias for sage.company.com, which in turn has the IP address of 127.30.50.1. The DNS server would then return that address to the requester.

Notice that WWW.company.com and E.mail.company.com are both aliases to the same computer—thyme.company.com. This implies that the administrator has set up both a World Wide Web and E-mail server on that computer.

MacDNS Administrator's Guide

A Domain Name Server for the Mac OS

Apple Computer, Inc.

Every effort has been made to ensure that the information in this manual is accurate. Apple is not responsible for printing or clerical errors.

Apple Computer, Inc.
1 Infinite Loop
Cupertino, CA 95014-2084
(408) 996-1010

Simultaneously published in the United States and Canada.

Contents