

3.2 Release Notes: Network and file system configuration

Netmask configuration in Release 3.2

The way netmask configuration is handled has been changed for Release 3.2 to provide better conformance with RFC1122 and to eliminate problems of excessive network traffic generated when large clusters of computers boot at the same time.

About netmasks

The network mask, or netmask, is a configuration item used to support IP subnetting, a feature that helps organizations partition their networks and use routers to connect the subnetworks. Whether or not IP subnetting is used (and it isn't typically used in small networks), each computer has a netmask.

Each NEXTSTEP computer on the network gets its netmask from one of three sources:

- Default. Once the computer obtains its IP address at boot time, either from local

configuration information or from a BOOTP server on the network, it computes a subnet mask appropriate for that IP address. This is a good option for a network where you haven't explicitly chosen to use IP subnetting.

- Automatic. At boot time, a netmask query is broadcast to the network, and the netmask is returned by some other computer on the network. If no response is received, the default value described above is used.
- Explicit. A specific netmask value you enter yourself.

You set the netmask source with the HostManager or SimpleNetworkStarter application, and your setting is reflected in the **/etc/hostconfig file**.

Changes in Release 3.2

In previous releases, each NEXTSTEP computer responded to each netmask query received from the network, forwarding its current netmask no matter how it was obtained. In Release 3.2, only computers that have a netmask explicitly configured will respond to queries. Since a much smaller number of computers will be responding to queries, computers that don't receive any responses will retry their requests four additional times before giving up. On computers with an Automatic netmask setting, a delay is inserted between retries to avoid congestion when many computers boot simultaneously. If no responses to any of the queries are received, system booting is delayed by about 20 seconds.

To avoid this delay, you can do one of these two things:

- Use HostManager's Local command to configure a specific netmask for one or more servers on each network (or on each IP subnet if IP subnetting is used). In the Local Configuration panel, click the button under Netmask that's next to the text field. If you're not using IP subnetting and the computer already has its IP address, it fills in the proper value for you. If you are using IP subnetting, you need to type the proper netmask value for your site.
- Avoid automatic netmask configuration either by leaving each computer's netmask configuration in its default state (or returning it to its default state if it's been changed), or by setting the netmask configuration of each NEXTSTEP computer on the subnet to an explicit value. You set the netmask configuration with HostManager's Local command.

Known problems

The following are known problems with configuring a NEXTSTEP file system or network.

- Some Ethernet boards—including the 3COM Etherlink III and SMC Ethernet boards—have small buffers. This can cause the board to drop incoming NFS packets, which can slow down NFS performance. To improve performance with Ethernet boards that have small buffers, you can modify the NFS mount options for servers you use often, such as the server containing your home directory, to match the characteristics of these boards. To do so, use the NFSManager application in **/NextAdmin** as follows: Use the Expert Options button in the Imported Directories window to set the Read buffer size to 1024 bytes.

- Make sure to give Owner Read permission to any file or folder that's in a directory the Workspace Manager searches and that's also exported by an NFS®server. For example, **/LocalApps**. If, when you're logged in as **root**, the Workspace Manager tries to read a file in an NFS-mounted directory and the file doesn't have Owner Read permission, the Workspace Manager might crash.
- Multiple UNIX file system partitions on a local disk may cause problems with Workspace Manager. Don't create multiple partitions on a single local, automounted device.
- When starting up a new computer on a network that uses automatic host configuration, make sure to give the computer a host name when you're prompted to. If, instead, you type Control-C to avoid giving a host name, the computer will be unusable. If you really don't want to supply a host name at the prompt, you should restart the computer, disconnected from the network.
- The **mailDBupdate** command reads user account and alias information from NetInfo databases and writes it to files named *passwd* and *aliases* respectively. This information is used by the Addresses panel of the Mail application. Page 170 of *NEXTSTEP Network and System Administration* incorrectly states that the command for updating the Mail application's aliases database is **/usr/bin/mailDBUpdate**. The correct command is **/usr/bin/mailDBupdate**. Also, options have been added to the command, as follows:

```
nescorna [~]-61% mailDBupdate -help
usage: mailDBupdate [-A] [-a aliases_domain] [-u users_domain] [-o dir]
```

The flags are interpreted as follows:

- A** Append to the output file, rather than overwriting (default is to overwrite)
- a *aliases_domain*** Specifies the NetInfo domain to obtain the aliases information from (default is the root domain).
- u *users_domain*** Specifies the NetInfo domain to obtain the users information from (default is the root domain).
- o *dir*** Indicates the directory that will contain the output files (default is **/LocalLibrary/Images/People**).

If you specify only one of the **-a** or **-u** flags, only that file will be written. So if you specify one flag and want the other to default to the root domain, you must actually specify the root domain in the command. It won't default automatically in this case. You can also specify each flag with a different domain.

If you specify no arguments at all, the command reverts to the previous behavior, which is defined by the defaults specified above.

- The usage line for the **mount(8)** command doesn't list the **-n** option, which mounts the file systems without updating **/etc/mtab**. This option can be useful for recovering from an overly full disk.
- The ypservers map created by **ypinit -m** is incorrect. To create the correct ypservers map, add the following code (in bold) to the default Makefile:

```
all: passwd group hosts ethers networks rpc services protocols \
    netgroup aliases ypservers
```

```
ypservers.time: $(DIR)/ypservers
```

```

@awk '{ print $0, $0 }' $(DIR)/ypservers) | \
    $(MAKEDBM) - $(DIR)/yp/$(DOM)/ypservers
@touch ypservers.time
@echo updated ypservers
@if [ ! $(NOPUSH) ]; then $(YPPUSH) -d $(DOM) ypservers; fi
@if [ ! $(NOPUSH) ]; then echo "pushed ypservers"; fi

```

```

ypservers: ypservers.time
$(DIR)/ypservers:

```

- The default NetInfo "_writers" properties allow users to install printers and fax modems and to export them to the network without help from the system administrator. The user can also configure other parts of the system, such as monitor screens. Because of this, users might be able to gain unauthorized privileges on the system. For example, in the **/printers** and the **/fax_modems** directories, the "_writers" property can permit users to obtain unauthorized **root** access to a system. In the **/localconfig/screens** directory, the "_writers" property can potentially permit a user to deny login access to other users.

To safeguard against these security holes, remove the "_writers" properties from the **/printers**, **/fax_modems**, and **/localconfig/screens** directories in all NetInfo domains on the network, and from all immediate subdirectories of these directories. You can remove the "_writers" properties in either of these ways:

- As **root**, use the **niutil** command-line utility. For example, to remove the "_writers" property from the **/printers** directory, enter:

```
# /usr/bin/niutil -destroyprop . /printers _writers
```

-Use the NetInfoManager application to open the desired domain and directory, select the "_writers" property, choose Delete from the Edit menu, and save the directory.

You might also remove "_writers" from other NetInfo directories, such as **/locations**. Just remember that by doing so, the network and its computers become more secure, but a system administrator's assistance is required where otherwise it isn't.

For more information on "_writers", see *NeXTSTEP Network and System Administration*. Note that the subdirectories of **/users** have "_writers_passwd" set to the user whose account is described by the directory. This is essential if users are to be able to change their own passwords, and this doesn't compromise system security.

- When you install NEXTSTEP, invalid entries for a SCSI tape drive may appear in the **/dev** directory. If this happens, you should ignore these entries. If you attach a tape drive and try to write to it when the invalid entries are there, error messages appear and the information isn't written. When you configure your computer for a SCSI tape drive using the Configure application and then start up the computer with a tape drive attached, any invalid entries are replaced by valid ones and you can successfully use the tape drive. As long as the computer is properly configured, the correct entries are in **/dev** and the tape drive works fine.
- If you have any * entries in the selector portion of the **syslog.conf** file, you should edit the file so that each * entry appears at the beginning of its line. Otherwise, syslog messages might not be delivered correctly. For example, the line:

```
kern.debug;daemon,auth.notice;*.err;mail.crit /usr/adm/messages
```

should be edited to:

```
*.err;kern.debug;daemon,auth.notice;mail.crit /usr/adm/messages
```

For more information, see the UNIX manual page for **syslogd**.