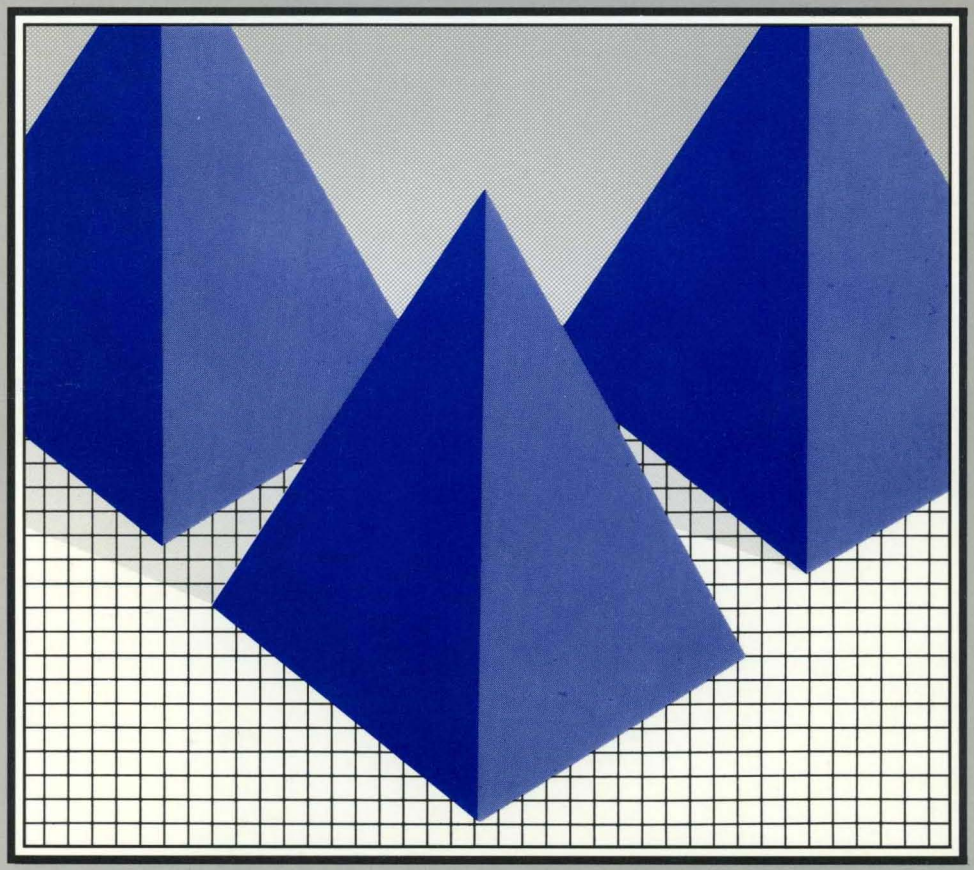
HEWLETT-PACKARD

HP 9000 Series 300 and 800 Computers

Installing and Administering Network Services



HP 9000 Series 300 and 800 Computers

Installing and Administering Network Services

Manual Part Number: B1012-90001
Printed in U.S.A., September 1989

Notice

Hewlett-Packard makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Restricted Rights Legend

Use, duplication or disclosure by the Government is subject to restrictions as set forth in paragraph (b)(3)(B) of the Rights in Technical Data and Software clause in DAR 7-104.9(a).

This software and documentation is based in part on the Fourth Berkeley Software Distribution under license from the Regents of the University of California.

MS-DOS® is a registered trademark of Microsoft Corp.

UNIX® is a U.S. registered trademark of AT&T in the U.S.A. and other countries.

Hewlett-Packard Co.
3404 E. Harmony Rd.
Fort Collins, CO 80525 U.S.A.

Printing History

First Edition . . . . . September 1989

Conventions

NOTATION	DESCRIPTION
Boldface	Boldface is used for emphasis.
`Computer Text`	Words in syntax statements which are not in italics must be entered exactly as shown. Punctuation characters other than brackets, braces and ellipses must also be entered exactly as shown. For example: `# cd mydirectory`
`italics`	Words in syntax statements which are in italics denote a parameter which must be replaced by a user-supplied variable. For example: `# CLOSE filename` Italics are also used for manual titles.
Return	This font is used to indicate a key on the computer's keyboard.
CTRL-D	This conventions is used to indicate a combination of keys to press simultaneously for a desired function.
[ ]	An element inside brackets in a syntax statement is optional. Several elements stacked inside brackets means the user may select any one or none of these elements. For example: [A] [B] User may select A or B or neither.

{ }

When several elements are stacked within braces in a syntax statement, the user must select one of those elements. For example:

{A}
{B}
{C} User must select A or B or C.

. . .

A horizontal ellipsis in a syntax statement indicates that a previous element may be repeated. For example:

[,*itemname*]...;

In addition, vertical and horizontal ellipses may be used in examples to indicate that portions of the example have been omitted.

underlining

Brackets, braces or ellipses appearing in syntax or format statements which must be entered as shown will be underlined. For example:

LET *var*[[*subscript*]] = *value*

Table of Contents

1

Product Overview

HP 9000 Network Services (NS) enable Hewlett Packard (HP) and non-HP computers to communicate using HP-defined user-level services over a Local Area Network connection.

Note The information contained in this manual applies to both the Series 300 and Series 800 HP 9000 computer systems. Any differences in installation, configuration, or operation are specifically noted.

The link product must be installed for NS to function. The link provides all the necessary hardware and software to interface between an HP 9000 Series 300 or 800 computer and an IEEE 802.3 or Ethernet Local Area Network.

ARPA Services and NFS Services also require link software. ARPA Services, NFS Services, and NS can run concurrently on the same node, but this is not required.

Note For a detailed overview of the AdvanceNet products available for the HP 9000 Series 300 and 800 systems, refer to the *HP 9000 Series 300 and 800 Networking Overview*.

Software Components

The NS product has only software components. When you purchase the NS product, you receive a tape that contains all of the NS software. The NS software includes the NS user services **Network File Transfer (NFT)** and **Remote File Access (RFA)**. The following descriptions of the NS user services serve as an overview only. For more information on these services, refer to *Using Network Services*.

- **Network File Transfer (NFT)** enables you to copy files between nodes in the network. NFT can be used between Series 300 or 800 systems and other systems. Refer to *Networking Overview* and to *NS Cross-System NFT Reference* for details on cross-system NFT.
- **Remote File Access (RFA)** allows you to use HP-UX commands and system calls to access files and directories on other HP-UX nodes on the network. Unlike NFT, which offers only a fast file copy mechanism, RFA allows you to execute general HP-UX commands and calls on remote HP-UX files and directories.
- **Vt3k** is an application that allows you to log into a remote MPE (HP 3000) host from a local HP-UX host. *Vt3k* uses NetIPC and works with either MPE V or MPE XL.

2

Installing NS

This chapter describes how to install the NS networking product on your system.

Note **For those customers who have previously installed NS:** Refer to the installation instructions provided in the "Read Me First" document when updating your system to a new revision of the NS software.

The link product must be installed before installing NS. For information on link installation, refer to the link installation manual.

Installation Steps

To install the NS product, you must perform the following steps in order:

1. Update your network map.
2. Install the NS software.
3. Configure the NS software.
4. Check the NS software installation.

Each of these steps is described in detail in this chapter.

1. Updating Your Network Map

Before you install the NS product, it is important to take the time to update your network map to indicate that NS is installed on your node. A network map provides you with information about the configuration of computers on your network. As a node manager, it is your responsibility to keep the network map up to date when you add or delete computers or make cable changes.

Refer to the link installation manual for detailed information about creating and maintaining a network map.

2. Installing the NS Software

Before you begin the following installation procedure, make sure you have the correct software versions on your computer. **The HP-UX operating system, the required link software and the NS software must all be the same version.** Otherwise, the network may malfunction. Use the `uname -a` command to check your HP-UX operating system version number.

You install the NS software using the HP-UX `update` program.

Using update

The `update` program is fully documented in the HP-UX installation manual. You should read this manual before attempting to install the NS software using `update`.

After you are certain that the required HP-UX and link software is installed, use the `update` program to install the NS software. If `update` returns an error message, check the error message information provided in Appendix A of this manual.

Your next step depends on the following information:

- If you have just updated previously-existing NS software on a Series 300 system, then you have completed installing the NS product. Proceed to "Files Created During Software Installation" later in this chapter.
- If you have just updated a Series 300 system to add NS software for the first time, **and** you are **not** using SAM's Networks/Communications menus to configure your LAN card(s) or NS software, you must now configure a new kernel to include NS. To configure a new kernel, refer to the next section.
- On a Series 800 system, you have completed installing the NS product, and you do not need to configure a new kernel **unless the update program failed to generate a new kernel.** To configure a new kernel, refer to the next section. Otherwise, proceed to "Files Created During Software Installation" later in this chapter.

Configuring a New Kernel

To prepare the NS product for use, you must configure the HP-UX operating system kernel to include NS if:

- you are installing NS software for the first time on a Series 300 (your kernel has not already been configured to include NS) or
- the `update` program failed to generate a new kernel on a Series 800.

If your kernel is based upon the standard kernel file (`/etc/conf/dfile` on a Series 300 or `/etc/conf/gen/S800` on a Series 800), you can use SAM (System Administration Manager) to configure a new kernel that includes NS.

If your kernel is based upon a customized kernel file, you must manually configure a new kernel. On a Series 300, your kernel file must contain the uncommented entry

```
rfa
```

On a Series 800, your kernel file must contain the uncommented entry

```
include nsrfa0;
```

Refer to the HP-UX System Administrator's Manual for instructions on configuring a new kernel.

Files Created During Software Installation

When the NS software is installed, four symbolic links, two daemons, two servers, one binary, one message catalog, and one library routine are created.

Table 2-1. Files Created During Software Installation

Files	Function
/etc/rfadaemon	Symbolic link to */usr/bin/rfadaemon*
/etc/rfaserver	Symbolic link to */usr/bin/rfaserver*
/etc/nftdaemon	Symbolic link to */usr/bin/nftdaemon*
/etc/nftserver	Symbolic link to */usr/bin/nftserver*
/usr/bin/rfadaemon	The Remote File Access (RFA) daemon process. This daemon must be running to use inbound RFA, but outbound RFA requests can be initiated without running this daemon.
/usr/bin/rfaserver	RFA server process.
/usr/bin/nftdaemon	The Network File Transfer (NFT) daemon process. This daemon must be running to use inbound or outbound NFT.
/usr/bin/nftserver	NFT server process.
/usr/bin/dscopy	NFT initiator process.
/usr/lib/nls/c/ns.cat	Ns error message catalog.
/lib/libn.a	The library routine used for programmatic Remote File Access (RFA).

The NS initialization script `/etc/netnssrc` automatically starts the NS daemons when the system reboots. This script is invoked from the LAN initialization script `/etc/netlinkrc`. No changes need to be made to `/etc/netnssrc`.

3. Configuring the NS Software

There are no configuration files that are unique to the NS product. NS uses configuration files that are provided with the link software or created during network configuration. **No further editing of these files is necessary.**

Configuration Tasks

Once you have successfully installed the NS software, you must perform the following configuration tasks:

- Create **network special files** for Remote File Access (RFA). (RFA is not supported on the X.25 network.)
- Create the **probe proxy table** if you plan to use the NS software through a gateway.

Creating Network Special Files

Remote File Access (RFA) allows you to use certain HP-UX commands and system calls to manipulate files and directories on remote HP 9000 Series 300, 500, and 800 systems.

Note RFA is not supported over the X.25 network.

To access a remote computer's file system using RFA, your local computer must have a network special file that represents the remote computer. As super-user, you must create a **network special file** on your local computer for each remote node that you want your local computer to access. The network special file acts as a path from your local file system to a particular remote file system.

Use SAM to automatically create network special files or manually create them with the *mknod(1M)* command. If you are unfamiliar with the procedure of creating network special files, it is easier and more efficient to use SAM. If you are already familiar with the `mknod` command, it is faster to use the command. The `mknod` command also lets you customize the names of your system's network special files, if desired.

Note HP recommends that you assign each network special file its corresponding remote node name, and that you keep all network special files in a directory called `/net`. The node name is assigned during LAN software initialization. Refer to *Installing and Administering LAN* for more information.

Using SAM to Create Network Special Files

Note Although some of the NS product's functionality is supported over both the LAN link and the X.25 link, SAM does not currently support configuration of the X.25 link. Therefore, SAM allows configuration of NS only when you have the LAN link product.

Tips for Using SAM

SAM stands for System Administration Manager, a menu-driven utility for performing system administration tasks, including configuration of networking software.

Remember the following tips for using SAM:

- Use your keyboard's cursor control and editing keys to navigate and edit forms.
- You may select a menu item by typing enough of its first word to uniquely identify it. In some cases, this is simply the first letter of the menu item. This method does not work for menu items that start with the same word.
- Access the on-line help screens whenever you need more information, such as how or where to obtain a required configuration value! Note that the RESULT and HOW USED sections of the on-line help screens explain what SAM will do "behind the scenes," such as what files SAM will create or modify, or what commands SAM will execute automatically.

Procedure

The following steps tell how to use SAM to automatically create network special files:

1. At the HP-UX prompt, type:

   ```
   sam
   ```

   and wait for SAM's main menu to appear.

2. Select the `Networks/Communications` menu item.

3. Select the NS (Network Services) Configuration menu item.

4. Select the Add Connectivity to a Remote System menu item.

Note The Remove Connectivity to a Remote System menu item lets you delete a network special file.

---

5. Fill in the form with the node name of the remote system for which you are creating the network special file. View the help screens for information about filling in the form.

6. Press the Perform Task softkey.

7. Repeat steps 5 and 6 to create additional network special files.

8. Press the Main Menu softkey when you are finished.

9. Press the Exit SAM softkey to exit from SAM.

Verification

To view the list of network special files, which provide connectivity to the remote systems they are named after, type the following command at the HP-UX prompt:

```
ls /net
```

To verify the operation of the network special files, see the "Checking the NS Installation" section at the end of this chapter.

What Else You May Need to Do

If you are using NS to communicate with remote systems through a gateway, you will need to create the probe proxy table on one of the nodes on your LAN, as explained later in the "Creating the Probe Proxy Table" section of this chapter.

Using mknod to Create a Network Special File

The format of the *mknod(1M)* command is:

Syntax

```
mknod /net/net_spcl_f n remote_node_name
```

net_spcl_f	Name of the network special file. *net_spcl_f* is a string of alphanumeric characters and underscores (_) where the first character is alphanumeric. The maximum length of *net_spcl_f* is 255 characters. HP recommends that the *net_spcl_f* name match the remote node name.
n	Indicates that the file is a network device file.
remote_node_name	Name of the remote node that the network special file represents. Names are case insensitive. If you do not include the environment and organization names, the system uses those of the local node.

Example 1

The following command creates a network special file for the remote computer with the node name PC_Design2.LAB.ACO.

```
mknod /net/PC_Design2 n PC_Design2.LAB.ACO
```

Example 2

If the current node is in the same domain as the target node, then you do not need to specify the domain name and organization name.

```
mknod /net/PC_Design2 n PC_Design2
```

Refer to *Using Network Services* for information on how to use RFA once the network special files have been created.

Creating the Probe Proxy Table

Note Perform this step only if you plan to use the NS product through a gateway.

The Probe proxy server enables NS to operate through a LAN-to-LAN gateway. NS uses the **Probe protocol** for name-to-IP-address resolution. By itself, the Probe protocol can only obtain information about nodes on the same network or subnetwork. If you need information on another network or subnetwork, the probe proxy server contains IP addressing information about other nodes on other networks. If another node on the LAN needs to establish a connection with a remote node that exists on a different network or subnetwork, the probe proxy server can provide the sending node with addressing information about the remote node. The sending node then uses this addressing information with its routing table to determine the correct route to a node on a remote network.

You must specify one node on the LAN as the probe proxy server. The probe proxy server can be a gateway, or any other node on the network.

Figure 2-1 illustrates how probe proxy servers work with Network Services.

- You can initiate a connection from Network A to Network A without a proxy server (see Example 1).
- You can initiate a connection from Network B to Network B, even through a bridge, without a proxy server (see Example 2).
- You must have a proxy server on Network A to initiate a connection from Network A to Network B (see Example 3).
- You must have a proxy server on Network B to initiate a connection from Network B to Network A by the request of Network A, even though Network A has a proxy server (see Example 4).

If you put the proxy server on the gateway, it will serve both Network A and Network B.

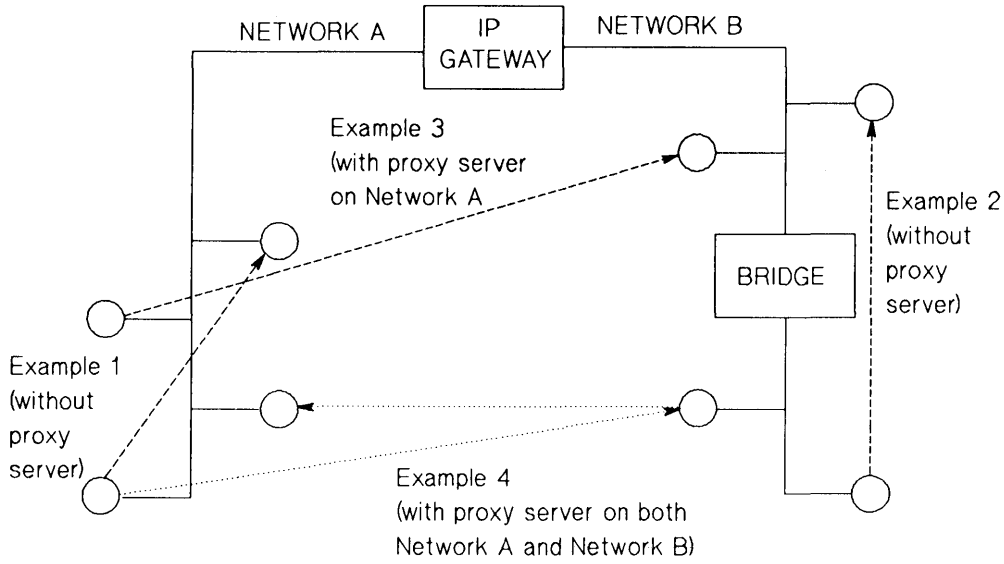


Figure 2-1. How Probe Proxy Servers work with NS

A probe proxy server stores information about other nodes on other networks or subnetworks in a probe proxy table. You manipulate the Probe proxy table with the *proxy(1M)* command described next.

Setting Up NS Gateway Access

You can access the NS gateway using the *proxy(1M)* command. This command manipulates the NS Probe proxy table.

Note You need to do this step each time you reboot the proxy server.

Syntax

```
proxy { add    nodename domain ip_address medium}
      { append nodename domain ip_address medium}
```

or

```
      { on                }
      { off               }
proxy { delete nodename
      { show   nodename
      { flush             }
      { list              }
```

Options

`on`	Enables Probe proxy on a node. You must use this option before being able to change the probe proxy table. Requires super-user capability.
`off`	Disables the proxy server. The Probe proxy table is not flushed. Requires super-user capability.
`add`	Adds a new entry to the Probe proxy table. Requires super-user capability. The following parameters are required: *nodename*

		Fully-qualified NS node name. Domain and organization are required. Node names are assigned during link software initialization. Refer to the link installation manual for more information about node names.
	domain	The internet domain. The only supported domain is HPDSN.
	ip_address	IP address of the remote node being mapped by *nodename*. The IP address must be in decimal internet "dot" format. See the *inet(3N)* entry in the *LAN/X.25 Reference Pages* for a description of internet "dot" format, or refer to link installation manual.
	medium	The physical link transmission protocol. Can be either `ieee` or `ether`.
`append`		Appends an additional path report to an existing Probe proxy table entry. Use this option if a remote node runs on a network that supports both IEEE 802.3 and Ethernet link mediums. "Add" to the Probe proxy table a node running on the `ieee` medium, then "append" the same node to the Probe proxy table as a node running on the `ether` medium. You can also use the `append` option if a node on a remote network or subnetwork contains more than one network interface accessible by your local node. `Append` requires the same options as `add` above. You must have super-user capability to use this option.

`delete` *nodename*	Deletes *nodename* from the Probe proxy table and all the path reports associated with *nodename*. *Nodename* is a fully-qualified NS node name. You must have super-user capability to use this option.
`flush`	Clears the Probe proxy table, deleting all entries. You must have super-user capability to use this option.
`show` *nodename*	Sends path report information for *nodename* to standard output. For each path report associated with *nodename*, the following information is returned: node name, IP Address, Medium, Services, and Transports. The Services and Transports fields always contain the value FFFF, meaning all services and transports default to **on**.
`list`	Returns information for all entries in the Probe proxy table. `Proxy list` is equivalent to issuing a `proxy show` command for all node names in the Probe proxy table.

Proxy Command Description

The Probe proxy table is the NS equivalent of the ARPA Services `/etc/hosts` file. The Probe proxy table associates IP addresses with NS node names; the `/etc/hosts` file associates IP addresses with mnemonic host names.

Like the `/etc/hosts` file, the Probe proxy server does not provide all the addressing information needed to route data to a node on a remote network. When a requesting node receives addressing information from a Probe proxy server, the requesting node must consult its network routing table to determine the correct route to the node on the remote network.

For more information about the network routing table, refer to *routing(7)* in the *Network Reference Pages* and the link installation manual. For more information about the `/etc/hosts` file, refer to *hosts(4)* in *Network Reference Pages* and the link installation manual.

4. Checking the NS Installation

Once the NS software is installed, configured and initialized, you should make sure that NS is operating correctly by running the NS verification script. The syntax for the NS verification script is as follows:

Syntax

```
/usr/nettest/nsverify/ver_ns [-r nodename net_spec_file login[:[password]]]
```

Options

`-r` *nodename*	an option used to test communication to other HP 9000 computers. The node name you assigned to your system during LAN initialization is *nodename*.
net_spec_file	an RFA special file described in "Creating Network Special Files" earlier in this chapter.
login and *password*	are a valid login and password for the remote node specified in *nodename*.

If the NS verification script encounters problems, it prints error message and recovery information to your terminal screen.

Manually Testing the Installation

If you cannot locate the NS verification script, you can perform the following verification tests manually.

- Use the NS Quick Verification strategy. Use the *dscopy(1)* command to copy a file from the Series 300 or Series 800 to a remote node, then copy the same file back. Execute the HP-UX `cmp` command to verify that the copied file is identical to the original file. This exercise tests NS and LAN from the Application Level (OSI Layer 7) down to the Physical Level (OSI Layer 1).
- If NFT or RFA fail, test that the NS daemons are running. Issue the following command:

  ```
  /bin/ps -ef | grep daemon
  ```

  You should see one entry per network daemon in the table of statistics returned to standard output. If you don't see an entry for a daemon, start it by typing the daemon name (as an absolute pathname) on the command line. You must be super-user to start a network daemon. **Required NS Daemons:** `nftdaemon`, `rfadaemon`.

For a more formalized network testing technique, refer to link installation manual.

3

Maintaining NS

This chapter provides information that helps you maintain the NS product on your system. This information is presented in two sections:

- Maintenance Tasks
- Networking Daemons and Special Files

The first section describes the tasks involved in maintaining the NS product and the commands used to perform these tasks. The second section contains a quick reference list of the daemons and library routines provided with the NS product.

Maintenance Tasks

The NS maintenance tasks are as follows:

- Setting up spooling to printers on remote computers. This is done using the HP-UX commands *mkdir(1)*, *chmod(1)*, and *lp(1)* commands.
- Setting up security for NS. This is done using the HP-UX *chmod(1)* command.
- Modifying the Probe proxy table. This is done using the NS *proxy(1M)* command.

Setting Up Spooling to Printers on Remote Computers

Note Perform this step only if you intend to use remote devices from your local node.

The HP-UX *lp(1)* command does not allow spooling to a printer (or other device) that is connected to a remote computer on the network. If there is already a spooler daemon for the device on the remote computer, you can implement spooling to that remote device. You must be super-user to perform this task. Once you have executed the following steps for a specific device on a remote computer, anyone can spool files to that device.

The following example illustrates how to set up remote spooling to a printer attached to a remote computer called `PC_Design1`.

Example

First, create a directory on PC_Design1 in /usr/spool using the following commands:

```
mkdir /usr/spool/rlp

chmod 777 /usr/spool/rlp
```

Rlp is a sample directory name. You may use any legal HP-UX file name for your remote spooling directory. You can make the security on this directory stricter than 0777, but all users must be allowed to create and write to files in that directory, and the spooler daemon must be allowed to read and delete files from the directory.

Next, edit PC_Design1's /usr/lib/crontab file by issuing the following command:

```
/usr/lib/crontab -l  outfile
```

Then add the following entry to PC_Design1's outfile file:

```
0,10,20,30,40,50 * * * * find /usr/spool/rlp -perm 0614
-exec lp -r {} \;
```

If your lp spooler does not have an option to remove the file after printing it, you must modify this entry by changing find so that the file is removed after the spooler has been run. If you do not make this change, the file is spooled repeatedly. The following command shows the change:

```
0,10,20,30,40,50 * * * * find /usr/spool/rlp -perm 0614
-exec lp -r {} \; -exec rm {} \;
```

Then issue the command:

```
/usr/lib/crontab outfile
```

The permission setting (-perm 0614) is used for synchronization. If you do not set permission at 614, the spooler could start up before a file is completely copied into the spooling directory. The portion of the file not copied into the spooling directory when the spooler started would be lost.

In this example, the spooler is set to run every ten minutes. This means that a delay of up to ten minutes can occur between the time a file is spooled and the time the printing starts, even if the remote printer is not busy.

The spooler could be set to run more often, but it would use more CPU time. For example, if the spooler runs every minute, approximately three percent of the CPU time would be overhead for running the spooler.

Finally, create a shell script on your local node to move a local file to the spooling directory on the remote computer. **Although any user can move a file to the spooling directory with `cp`, it is not recommended, because it bypasses synchronization.** The following commands must be included in your shell script:

```
umask 111
SPOOLFILE=/net/PC_Design1/usr/spool/rlp/rlp$$
cp $1 $SPOOLFILE
chmod 614 $SPOOLFILE
```

The file name generated and sent to `lp` has a unique file name because of the shell variable $$. However, if two computers each have a process that spools to the same file name before the spooler runs again, one file would be lost.

This shell script allows only one file to be spooled each time the `lp` command is used. You can add more commands to increase the usefulness of spooling to devices on remote computers.

Note Files spooled on the remote system print with the "root" banner, not the banner of the local account.

Setting Up Security for NS

When you connect a computer to a network, you should consider the security of the resources on your computer. Although you may adequately protect certain files from the users on your own system, you may need to protect those files from users on other computers on the network. There are three types of file protection:

- Local and Remote Logins
- Access Rights
- Disabled Services

The following subsections describe these file protection methods.

Note For information on C2 Security, refer to *A Beginner's Guide to HP-UX*, *A Beginner's Guide to Using Shells*, and the *HP-UX System Security* manual.

Local and Remote Logins

The assignment of user logins and passwords for access to the **local** file system offers direct security for your local computer. The assignment of user logins and passwords for access to **remote** file systems is a part of network-wide security.

For NFT commands, the user login and password are a part of the *dscopy(1)* command syntax. A valid login and password must be provided with each `dscopy` request. Access rights are limited to those of the remote login account specified in `dscopy`.

Access Rights

The assignment of access permission (with the *chmod(1)* command) limits accessibility of certain files to certain users. **HP strongly recommends that you limit the assignment of public access rights to files that everyone on the network can safely use.** You should also restrict (to super-user only) **write** access to RFA network special files. In general, do not allow anyone to have permission to access files that they have no reason to use.

For RFA commands, users specify a login and password by executing the `netunam` command. For NFT commands, users specify a login and password in the `dscopy` command. The login and password specified are checked against the entries in the `/etc/passwd` file on the remote file system. This means that entries such as `who` and `date` are valid system logins when used in a `netunam` or `dscopy` command. You can alleviate this problem by setting low access capabilities for `who` and `date`, or by removing these commands from the `/etc/passwd` file. The latter solution makes it impossible to execute `who` and `date` without logging in. Accessibility to the RFA network special files is a unique case. No matter what access mode is set on a network special file, RFA can still be used to access the node represented by the network special file. If this is a problem, you can set up more than one `/net` directory (for example: `/net1`, `/net2`...) and use access permissions on these individual directories to restrict access to particular nodes.

Disabled Services

An extreme method of network security is to disable services. In the examples below access is not limited, it is nonexistent. No one on a node can use the network services.

You can prevent access to RFA and NFT on Series 800 and 300 computers by not starting the daemon processes. You can use SAM to enable and disable these processes.

Procedure

The following steps tell how to use SAM to disable RFA and/or NFT daemons, preventing access to these services on an NS node:

1. At the HP-UX prompt, type:

   ```
   sam
   ```

   and wait for SAM's main menu to appear.

2. Select the `Networks/Communications` menu item.

3. Select the `NS (Network Services) Configuration` menu item.

4. Select the `Allow or Deny Access to Local Services` menu item.

5. Fill in the form according to its instructions. View the help screens for information about filling in the form.

Note You can use this form to re-enable RFA and/or NFT daemons.

---

6. Press the `Perform Task` softkey.

7. Press the `Main Menu` softkey.

8. Press the `Exit SAM` softkey to exit from SAM.

Note Since SAM modifies the networking startup file `/etc/netnssrc`, even if you reboot the system, the service(s) you disabled (or enabled) will remain disabled (or enabled).

Verification

To verify that the service you disabled is no longer running, at the HP-UX prompt, type:

```
ps -ef | grep daemon
```

The far right column should **not** show an `/etc/rfadaemon` and/or an `/etc/nftdaemon` process, depending on which one(s) you disabled.

Note You may still see `rfaserver` processes in a `ps -ef` listing. RFA connections that existed before you stopped the RFA daemon are not affected by the daemon's shutdown.

There are also different ways of disabling services:

You can stop RFA access to Series 800, 300 and 500 computers by not supplying network special files for specific nodes.

You can halt all network traffic on a node by issuing the `ifconfig lan0 down` command. To halt all network traffic, you must execute an `ifconfig lan`*n* `down` command for every network interface on the node, where *n* is the logical unit number of the network interface. All upper-level service requests on the node eventually time-out.

Specific security recommendations for the network diagnostics are contained in *Installing and Administering LAN*. The *ifconfig(1M)* command is also explained in *Installing and Administering LAN*.

Modifying the Probe Proxy Table

You can use the NS *proxy(1M)* command to modify, add, append, delete and list entries in the Probe proxy table. The syntax for the *probe(1M)* command is shown in Chapter 2 in the "Creating the Probe Proxy Table" section.

Networking Daemons and Special Files

This section provides a quick reference list of the daemons, library routines and configuration files that are provided and/or used by the NS product.

Daemons

When the system is brought up, the `/etc/netnssrc` initialization script starts the `rfadaemon` and `nftdaemon` daemon processes (`if they are executable`). The `/etc/netnssrc` script is invoked from the LAN initialization script `/etc/netlinkrc`.

netisr	The network interface daemon. It is provided with LAN. It allows for system wide performance improvements, particularly real time responses. For more information about `netisr` refer to *Installing and Administering LAN.*
rfadaemon	The daemon used for Remote File Access (RFA). This daemon must be running to use inbound RFA, but outbound RFA requests can be initiated without running this daemon. *rfadaemon* is located in the `/usr/bin` directory.
nftdaemon	The daemon used by Network File Transfer (NFT). This daemon must be running to use inbound or outbound NFT. *nftdaemon* is located in the `/usr/bin` directory.

Note `Netisr` must run at higher priority than other network services on the same node.

Library Routines

The following library routine is provided by the NS product.

netunam(3N)	The library routine used for programmatic Remote File Access (RFA).

Configuration Files

There are no configuration files that are unique to the NS product. However, NS does use several configuration files that are provided by the link product.

/etc/hosts	This file contains the internet addresses, hosts names and aliases of remote hosts on the network.
/etc/networks	This file contains the network addresses and names of networks known by the local host.
/etc/services	This file associates each service name and aliases with the port number and protocol that each service uses.
/etc/protocols	This file contains the protocol names of all the protocols known by the local host.

4

Troubleshooting Network Services

Troubleshooting data communications problems can be a very involved process since there are many hardware and software components to be investigated. Some problems can be quickly identified and resolved. These include invalid software installation, version incompatibilities, insufficient HP-UX resources, corrupt configuration shell scripts, and programming or command errors. Some problems require more investigation.

Once identified, most problems can be resolved by the programmer, user, or node manager, using the suggestions in this chapter or the instructions provided in the error message appendix (Appendix A). However, there may be problems which require you to contact your HP support representative. As a result, this chapter also provides guidelines to follow when submitting an HP Service Request (SR).

Chapter Overview

The strategy and tools to use while investigating the software and hardware components are provided in this chapter.

This chapter contains the following sections:

- Characterizing the Problem
- Diagnostic Tools Summary
- Diagnosing Interactive and Programmatic Problems
- Diagnosing Repeater and Gateway Problems
- Flowchart Format
- Troubleshooting the Network Services
- Contacting Your HP Representative

Characterizing the Problem

It is important to ask questions when you are trying to characterize a problem. Start with global questions and gradually get more specific. Depending on the response, you ask another series of questions, until you have enough information to understand exactly what happened. Key questions to ask are:

1. Does the problem seem isolated to one user or program? Can the problem be reproduced? Did the problem occur under any of the following circumstances:
   - When running a program?
   - When issuing a command?
   - When using a nodal management utility?
   - When transmitting data?
2. Does the problem affect all users? The entire node? Has anything changed recently? The possibilities are:
   - New software and hardware installation?
   - Same hardware but changes to the software. Has the configuration file been modified? Has the HP-UX configuration been changed?
   - Same software but changes to the hardware.
   - Do you suspect hardware or software?

It is often difficult to determine whether the problem is hardware or software related. The symptoms of the problem which mean you should suspect the hardware are:

- Intermittent errors.
- Network-wide problems after no change in software.
- Link level errors, from logging subsystem LAN0, logged to the console.
- Data corruption—link level trace that shows that data is sent without error but is corrupt or lost at the receiver.

The symptoms which mean you should suspect the software are:

- Network services errors returned to users or programs.
- Data corruption.
- Logging messages at the console.

Knowing what has changed recently may also indicate whether the problem is software or hardware related.

Diagnostic Tools Summary

The diagnostic tools that you will use most frequently are listed in Table 4-1. These tools are documented in link installation manuals.

Table 4-1. Diagnostic Tools

Tool	Function
netstat(1)	A nodal management command which returns statistical information regarding your network.
landiag	An HP 9000 Series 300 diagnostic program which tests LAN connections to other HP 9000 computers.
linkloop	A diagnostic program that runs link-level loopback tests between the HP 9000 Series 300 systems. *Linkloop* uses IEEE 802.3 link-level test frames to check physical connectivity with the LAN. This diagnostic tool is different from the loopback capability of *landiag* because it tests only the link-level connectivity and not the transport-level connectivity.
ping(1M)	A diagnostic program which tests connections to other computers running ARPA, NS or LAN software.
psidad	A utility under DUI that can help to identify problems on the PSI/800 board/card.
rlb(1M)	A diagnostic program which tests LAN connections to other HP 9000 computers. `rlb` does not test a connection to an HP 1000 computer.
x25check *x25server*	These two work in tandem. *x25server* runs on the logically remote host (could be same physical host) and echoes packets sent to it over the X.25 network by *x25check*.
x25stat	A nodal management command that returns status and information of the X.25 device/card. It provides interface status configuration information and virtual circuit statistics.
x25upload	This is used to upload the firmware in case of problems with the firmware on the board.
Event Logging	A utility that sends informational messages regarding network activity to the system console or to a file.
Network Tracing	A utility that traces link-level traffic to and from a node. HP recommends that you enable tracing only when troubleshooting a problem unsolved by other means.

Diagnosing Interactive and Programmatic Problems

The first step in investigating interactive or programmatic problems is to get copies of the networking manuals for the networking products installed on ;your system. Error messages are included in the appendices of these manuals.

If you have received a specific error message, find it in the manual and take the action recommended. Most error messages are easily understood by the user or programmer, although some of the explanations refer to internal procedures comprehensible only to qualified HP representatives. Users are not expected to understand these explanations, but they should follow the actions documented in the manuals. The discussion below provides additional information about the possible causes of these problems and the actions that may be required to resolve them. It is intended to supplement the documentation, not to replace it.

Programmatic Errors

If the user is doing networking programming and a system call completes with an error, the recovery procedure depends upon the system call. How you check for the error code depends on which service you are using. For example:

- If a NetIPC system call returned a completion code indicating an error, you can gain additional information by looking up the error number in the error message appendix of *NetIPC Programmer's Guide*.
- If a file system call returned an error, use the `errno` global variable to see if a networking error occurred. The `errno` error values are listed in the *errno(2) Network Reference Pages*. If the `errno` system call shows that a networking error occurred, then the `errnet` system call can be used to obtain additional details. The `errnet` error messages appear in the error message appendix of *Using Network Services*.

Therefore to ensure programmatic error recovery, always issue the appropriate system call to receive an error. If the system call receives an error, refer to the appropriate manual for an explanation and recovery for the error.

Interactive Errors

If the user is using the interactive capabilities of NS and receives an error, refer to the error message appendix of *Using Network Services*. The command errors fit into four categories:

- Syntax errors or invalid options. These errors result from user errors when issuing the command. They are readily corrected by checking for the correct syntax and reissuing the command.
- Warnings. Warnings are issued when a command is still executable but the results may not be what you intended. These result from cases where conflicting options are specified. The warning informs you which option was actually used (or not used).
- Resource Errors. These errors occur when a system resource needed for the execution of the command is not available. They should be rare. If they occur, you can wait and reissue the command later, when the resource may be available. If resource errors happen frequently, the network manager may need to investigate further.
- Internal Errors. These errors indicate that the software is malfunctioning. If they ever occur, notify your HP representative. The network manager should follow the steps outlined in "Contacting Your HP Representative" at the end of this chapter.

For syntax errors and warnings, consult the reference pages on that command for the correct syntax and options. Refer to this manual or to the appropriate network services manual. The node manager needs to take the appropriate action if users receive internal errors when issuing commands.

Diagnosing Repeater and Gateway Problems

If you are using a repeater and hosts on either side of the repeater are having difficulty communicating with each other, a repeater subsystem failure may have occurred. In the illustration below, all of the systems on side A are able to communicate with one another. All the systems on side B are able to communicate with each other. If communication is cut from side A to side B, the repeater subsystem is suspect for causing the fault, since it is the medium by which side A and side B communicate.

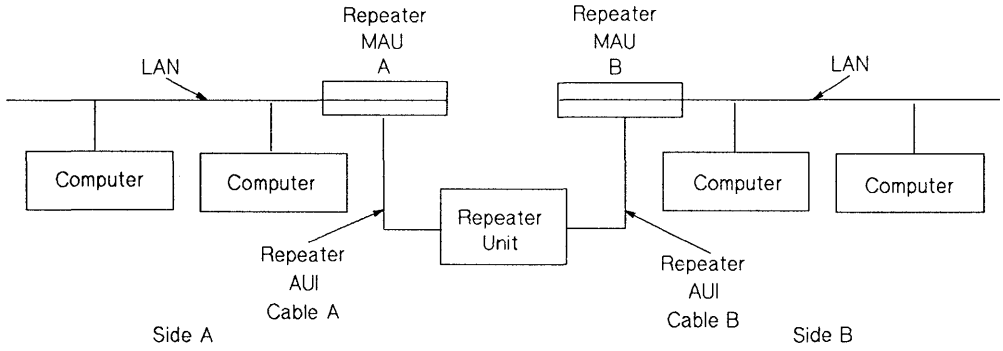


Figure 4-1. Troubleshooting Networks that Use Repeaters

The same concept holds for communication through a gateway. If you suspect a gateway problem, try the following procedures:

- To determine if you are set up to communicate with the desired node, execute:

  ```
  netstat -r
  ```

- To obtain routing statistics, execute:

  ```
  netstat -rs
  ```

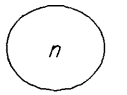
  The statistics could indicate a bad route, suggesting a problem with a gateway node.

- Check with the node manager of the gateway node to ascertain proper operation of the gateway.

For more information on troubleshooting gateways, refer to *Installing and Administering LAN*. For information on repeaters, refer to *HP-PB LAN Interface Controller (LANIC) Installation Manual*.

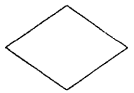
Flowchart Format

The flowchart on the following page has a corresponding set of labeled explanations. You can follow the flowchart alone, or follow the flowchart and read the explanations for more detail. The explanations are on the pages following the flowchart.



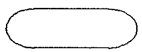
Start of flowchart n; re-enter current flowchart

Go to and enter flowchart n



Make a decision

Perform an action



Exit flowchart

Troubleshooting the NS Services

Use this section if you have trouble using the Network File Transfer (NFT) command, if Remote File Access (RFA) is malfunctioning, or if your NetIPC applications return unexpected errors.

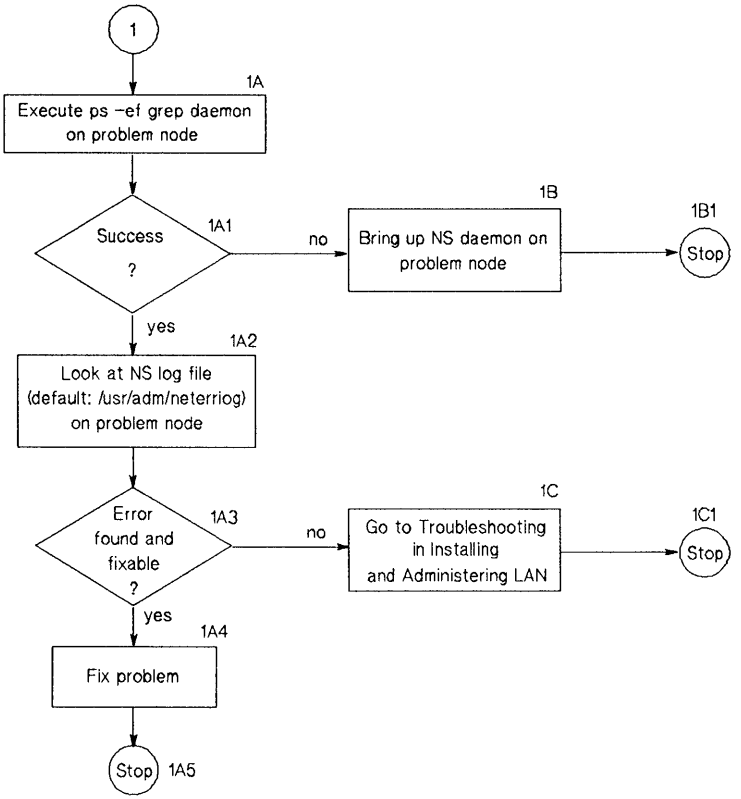


Figure 4-2. Troubleshooting NS Services

Flowchart 1. NS Troubleshooting

1A **Execute** `ps -ef|grep daemon` on `problem` node. A service daemon entry, in addition to the `grep` entry, returned to standard output ensures that the NS daemon is active on the problem node. Proceed to 1A1.

1A1 **Success?** If so, proceed to 1A2 to examine the NS log file for specific log messages; otherwise, proceed to 1B to activate the NS daemon on the problem node.

1A2 **Look at the NS Log File** on the problem node for specific NS subsystem log messages. The log messages for the specific NS service may be interspersed with other NS log messages. Explanations of the log messages appear in the error message appendix of *Installing and Administering LAN*. The default log file for NS log messages is `/usr/adm/neterrlog`. You may want to stop logging and then restart it with more logging classes enabled to give you more information. See *Installing and Administering LAN* for details on NS event logging. Proceed to 1A3.

1A3 **Error found and fixable?** If so, proceed to 1A4; otherwise, proceed to 1C to examine lower-level NS software.

1A4 **Fix Problem.** Explanations of the log messages appear in the error message appendix of *Installing and Administering LAN*. Proceed to 1A5.

1A5 **Stop.** If you solved your NS problem, stop troubleshooting.

1B **Bring up NS daemon on problem node.** Execute

```
/etc/ns_daemon
```

where *`ns_daemon`* is the NS service daemon which you are troubleshooting: `rlbdaemon` for the `rlb` diagnostic, `nftdaemon` for the NFT daemon, `rfadaemon` for the RFA daemon, or `sockregd` for the NetIPC socket registry. Retry the NS activity which prompted you to troubleshoot. Proceed to 1B1.

1B1 **Stop.** If you solved your NS problem, stop troubleshooting.

1C **Go to** *Installing and Administering LAN* to check LAN Link connectivity and lower-level software integrity.

1C1 **Stop**

Contacting Your HP Representative

If you have no service contract with HP, you may follow the procedure described below, but you will be billed accordingly for time and materials.

If you have a service contract with HP, document the problem as an Service Request (SR) and forward it to your HP Service Representative. Include the following information where applicable:

- A characterization of the problem. Describe the events leading up to and including the problem. Attempt to describe the source of the problem. Describe the symptoms of the problem and what led up to the problem.

  Your characterization should include: HP-UX commands; communication subsystem commands; job streams; result codes and messages; and data that can reproduce the problem.

  Illustrate as clearly as possible the context of any message(s). Prepare copies of information displayed at the system console and user terminal.

- Obtain the version, update and fix information for all software. Your host node should be running NS and LAN/HP 9000 Series 800 (3.0 Version or later) or LAN/HP 9000 Series 300 (6.0 Version or later).

  To check your NS or LAN version, execute the `what` *file_name* command, where *file_name* is one or more of the following sets:

  NFT: */usr/bin/dscopy*, */usr/bin/nftdaemon*, */usr/bin/nftserver*
  RFA: */usr/bin/rfadaemon*, */usr/bin/rfaserver*

  To check the version of your kernel, execute `uname -r`.

  This allows Hewlett-Packard to determine if the problem is already known, and if the correct software is installed at your site.

- Record all error messages and numbers that appear at the user terminal and the system console.

- Save all network log files.

  Prepare the formatted output and a copy of the log file for your Hewlett-Packard representative to further analyze.

- Prepare a listing of the HP-UX I/O configuration you are using for your

Hewlett-Packard representative to further analyze.

- Try to determine the general area within the software where you think the problem exists. Refer to the appropriate reference manual and follow the guidelines on gathering information for problems:
  - *Using Network Services (NS)*
  - *LAN Link Hardware Troubleshooting Manual*
- Document your interim, or "workaround" solution. The cause of the problem can sometimes be found by comparing the circumstances in which it occurs with the circumstances in which it does not occur.
- Create copies of any NS or LAN link trace files that were active when the problem occurred for your Hewlett-Packard representative to further analyze.
- In the event of a system failure, a full memory dump must be taken. Use the HP-UX utility `/etc/savcore` to save a core dump. Refer to *System Administrator's Manual* for details. Send the output to your HP representative.

5

Installing and Configuring Vt3k

Vt3k is an application that allows you to log into a remote MPE (HP 3000) host from a local HP-UX host. *Vt3k* uses NetIPC and works with either MPE V or MPE XL.

This chapter covers:

- Installing Vt3k
- Configuring Vt3k
- Troubleshooting Vt3k

Installing Vt3k:

The HP 9000, HP 3000, and your local network should be properly configured for Network Services. If `dscopy` works between your HP 9000 and HP 3000 systems, then your network has been set up properly.

Because *vt3k* is a user level program, it requires no other special installation procedures. It does not require any special configuration files or daemons.

Configuring Vt3k:

Vt3k does not require any special configuration files or daemons. It is supported on the following configurations:

- HP 2392 or HP 700/92 terminal connected via RS-232 to a Series 800 (connected via LAN to an HP 3000).
- Series 300 workstation (connected via LAN to an HP 3000)

`Hpterm` (only HP-UX 7.0 or later) offers HP Block Mode terminal emulation if you use X-Windows on a Series 300 workstation.

Vt3k is supported on HP-UX Release 7.0 or later. The HP-UX `ifconfig` command parameters must be set for IEEE in addition to Ethernet.

On MPE, *vt3k* requires at least MPE V V-Delta-5 or MPE/XL 1.2. The LAN Link and Network Services products are required on the HP 3000. NS Virtual Terminal Services must be running.

Vt3k can cross gateways, but this requires a proxy server machine on your local network with routing information for systems off your local network.

To test if your HP 9000 and HP 3000 are talking, try a remote loop back *(rlb(1))* from HP-UX to your HP 3000 and ensure *dscopy(1)* is working between the two systems.

Troubleshooting Vt3k

Most *vt3k* errors are reported via NetIPC error codes. For a complete list of error codes and corrective actions, refer to *NetIPC Programmer's Guide.*

The most common NetIPC error reported is "NSR_NO_NODE (40) node does not exist." This error may stem from the following conditions:

- Remote HP 3000 is not up.
- Node name is incorrect.
- Remote node is on a different network.
- Remote node is running an incorrect version of MPE
- Remote node is not listed on the local network routing tables.

Table 5-1 defines each of the *vt3k* termination codes.

Table 5-1. Vt3k Termination Codes

Codes	Description
Connection Terminated [0]	Result of a normal logoff.
Connection Terminated [1]	Indicates that someone has issued an ABORTJOB on the MPE session.
Connection Terminated [2]	Indicates that the network has shut down.
Connection Terminated [8]	Indicates that the remote MPE host has no vt ports available.

A

Error Messages

This appendix lists and describes the error messages that can be produced during LAN, NS and ARPA Services software installation and configuration. The error messages listed in this appendix are divided into the following categories:

- **Configuration Error Messages.** This section includes error messages that are returned by the LAN *ifconfig(1M)* and *nodename(1)* commands.
- **Software Installation Messages for Series 800 Only.** This section includes error messages that are returned by the `update` utility program when the networking software is installed.

Configuration Error Messages

The following error messages may be returned by the nodal management commands *nodename(1)*, *route(1M)*, *netstat(1)*, and *ifconfig(1M)*.

Message	**`permission denied`**
Cause	Permission to execute either the *nodename(1)* or *ifconfig(1M)* commands was denied.
Action	You must be a super-user to use the *nodename(1)* command to configure a node name or to set flags; you must also be a super-user to use the *ifconfig(1M)* command to configure an IP address or set flags.

Message	**`invalid node name syntax`**
Cause	The syntax specified for the node name was invalid.
Action	Check the syntax and try again.

Message	**`nodename not yet configured`**
Cause	The *nodename(1)* command was used to print the node name before the *nodename(1)* command was used to configure the system node name.
Action	Use *nodename(1)* to configure the system node name.

Message	**unexpected error returned from IPC:*errno***
Cause	A node management command invoked a NetIPC call that returned an error. A NetIPC error code is returned in *errno*.
Action	Refer to the error codes listed in *NetIPC Programmer's Guide* for the meaning of *errno*.

Message	**no such interface**
Cause	The interface name passed to *ifconfig(1M)* does not exist on the system.
Action	Check the spelling and names of interfaces on the system.

Message	**invalid internet address**
Cause	The internet address specified was not in the proper form.
Action	Check the syntax and try again.

Message	**IPCCREATE returned error: *errno***
Cause	The NetIPC call *ipccreate()* returned an error. The error code is returned in *errno*.
Action	Refer to the error codes listed in *NetIPC Programmer's Guide* for the meaning of *errno*.

Message	**message catalog can't be opened/accessed for language *lang*. Language n-computer will be used instead.**
Cause	This error can be returned from the *ifconfig(1M)*, *netstat(1)*, *nodename(1)*, *route(1M)*, and *rlb(1M)* commands. The message catalog for language *lang* isn't in /usr/lib/nls/*lang*.
Action	Verify that the $LANG variable is set to the correct language. If so, you need to install the desired message catalog.

Message	**ipaddr must be set also**
Cause	The super-user attempted to set the subnet mask with *ifconfig(1M)* without specifying an IP address.
Action	Execute the *ifconfig(1M)* command again, specifying both the IP address and the subnet mask.

Message	**ifconfig option *bad_opt* is not supported**
Cause	Option *bad_opt* is invalid.
Action	Check spelling and names of network interfaces on the system and try again.

Message	**route: socket: permission denied**
Cause	A non-super-user attempted to alter the route table.
Action	Gain super-user access rights or contact the node manager to alter the route table.

Message	`not in table`
Cause	The super-user tried to delete entry in the route table that does not exist.
Action	Check destination and gateway addresses or symbolic names and execute the `route delete` command again.

Message	`entry in use`
Cause	The super-user tried to add an entry to the route table that already exists.
Action	Delete the existing route and add a new one.

Message	`routing table overflow`
Cause	You have the maximum number of routes in your routing table.
Action	Delete a route entry no longer used and then add the new entry. Execute the `route delete` command again.

Software Installation Messages for Series 800 Only

The following ASCII messages may be generated when you install the networking software.

Message **Could not change into the new directory *uxgenname*. You will have to perform the kernel generation manually as outlined in the installation guide**

Cause The update program could not change into the new uxgen directory *uxgenname*.

Action Continue the installation manually. If you are installing NS, refer to *Installing and Administering NS*. If you are installing LAN, refer to *Installing and Administering LAN*.

Message **No file named *uxgenname*, consult installation guide**

Cause The update program could not locate the new uxgen file *uxgenname*.

Action Continue the installation manually. If you are installing NS, refer to *Installing and Administering NS*. If you are installing LAN, refer to *Installing and Administering LAN*.

Message	**Parsing of input file failed. You will have to perform the kernel generation manually as outlined in the installation guide.**
Cause	The update program could not remove comment delimiters from your uxgen input file.
Action	Continue the installation manually. If you are installing NS, refer to *Installing and Administering NS*. If you are installing LAN, refer to *Installing and Administering LAN*.

Message	**Storage of new kernel failed. You will need to make enough room in the root partition then restart the update process.**
Cause	The root directory (/) did not contain enough room for the new kernel created with NS/9000 and/or NS/9000 libraries.
Action	Move or remove unneeded files from the root directory. Retry the update program. If you are installing NS, refer to *Installing and Administering NS*. If you are installing LAN, refer to *Installing and Administering LAN*.

Message	**Storage of old kernel failed. You will need to make enough room in the root partition then restart the update process.**
Cause	The root directory (/) did not contain enough room for the backup kernel.
Action	Move or remove unneeded files from the root directory and retry the `update` program. If you are installing NS, refer to *Installing and Administering NS*. If you are installing LAN, refer to *Installing and Administering LAN*.

Message	**Storage of new uxgen input file failed. You will need to make enough room in the root partition then restart the update process.**
Cause	The root directory (/) did not contain enough room for the new `uxgen` input file.
Action	Move or remove unneeded files from the root directory and retry the `update` program. If you are installing NS, refer to *Installing and Administering NS*. If you are installing LAN, refer to *Installing and Administering LAN*.

Message **Storage of old uxgen input file failed You will need to make enough room in the root partition then restart the update process.**

Cause The root directory (/) did not contain enough room for the old `uxgen` input file.

Action Move or remove unneeded files from the root directory and retry the `update` program. If you are installing NS, refer to *Installing and Administering NS*. If you are installing LAN, refer to *Installing and Administering LAN*.

Message **The core kernel has not been updated. Consult the installation guide. Then update the kernel.**

Cause The core kernel has not been updated to the current HP-UX release.

Action Update the core kernel to the current HP-UX release. (See *HP-UX System Administrator's Manual* for details.) Try again.

Message	**The core kernel must be updated first. Consult the installation guide. Then update the kernel.**
Cause	The uxgen input file has not been updated to the current HP-UX software release.
Action	Make sure you have the current HP-UX release software. Update the core kernel to the current HP-UX release. (See *HP-UX System Administrator's Manual* for details. Try again. If you are unsuccessful, contact your HP representative.

Message	**The library libprot.a is not present. This update will not work.**
Cause	The library file /etc/conf/libprot.a was not installed with the other LAN files.
Action	Make sure you have the current LAN software. Retry the installation. If you are unsuccessful, contact your HP representative.

Message	**The library librfa.a is not present. This update will not work.**
Cause	The library file /etc/conf/librfa.a was not installed during LAN installation.
Action	Make sure you have the current LAN software. Retry the installation. If you are unsuccessful, contact your HP representative.

Message **The link library libns.a is not present. This update will not work.**

Cause The library file `/etc/conf/libns.a` was not installed with the other LAN files.

Action Make sure you have the current NS software. Retry the installation. If you are unsuccessful, contact your HP representative.

Message **The link tape has not been updated yet. You must do that first before a new kernel can be created.**

Cause You installed ARPA Services or NS before installing LAN. No harm has been done; the tapes have just been installed out of order.

Action Install LAN before you install NS or ARPA Services.

Message **Uxgen could not complete. You will have to perform the kernel generation manually as outlined in the installation guide.**

Cause The `update` program could not generate a new kernel.

Action Continue the installation manually. If you are installing NS, refer to *Installing and Administering NS*. If you are installing LAN, refer to *Installing and Administering LAN*.

Message **RFA will not be configured into this kernel.**

Cause The `librfa.a` file could not be found. Either RFA is not part of the customer package, or the NS product tape has not yet been installed.

Action If RFA has not been purchased, ignore this message. Otherwise, proceed with the NS installation upon completion of the LAN installation.

Message **You do not have the required lan0 line. You will have to update manually. Consult the installation guide.**

Cause The `update` program could not find the `lan0` line in the `uxgen` input file.

Action Add the following line to your `uxgen` input file:

```
lan0 lu 0 address 4;
```

Continue the installation manually.

Message **You do not have the required nsdiag0 line. You will have to update manually. Consult the installation guide.**

Cause The `update` program could not find the `nsdiag0` line in the `uxgen` input file.

Action Add the following line to your `uxgen` input file:

```
include nsdiag0;
```

Continue installation manually.

Message **You do not have the required nsnsipc0 line. You will have to update manually. Consult the installation guide.**

Cause The update program could not find the nsnsipc0 line in the uxgen input file.

Action Add the following line to your uxgen input file:

```
include nsnsipc0;
```

Continue the installation manually.

Message **You do not have the required nsrfa0 line. You will have to update manually. Consult the installation guide.**

Cause The update program could not find the NS/9000 nsrfa0 line in the uxgen input file.

Action

Add the following line to your uxgen input file:

```
include nsrfa0;
```

Continue the installation manually.

Message **Symbolic link of /etc/yp to /usr/etc/yp failed.**

Cause /etc/yp is already present.

Action

Remove /etc/yp.

Message **You do not have the required NFS line. You will have to update manually. Consult the installation guide.**

Cause The update installation program could not find the NFS Services line in the uxgen input file.

Action Add the following line to your uxgen input file:

```
include nfs;
```

Continue the installation manually.

Message **The library libnfs.a is not present. This update will not work.**

Cause The library file /etc/lib/libnfs.a was not installed with the other NFS Services files.

Action If NFS Services has not been purchased, ignore this message. Otherwise, make sure you have the current NFS Services software. Retry the installation. If you are unsuccessful, contact your HP representative.

Index

L

M

N

P

R

S

T

U

V

Reader Comment Card

HP 9000 Series 300 and 800
Installing and Administering Network Services
B1012-90001

We welcome your evaluation of this manual. Your comments and suggestions will help us improve our publications. Please tear this card out and mail it in. Use and attach additional pages if necessary.

Please circle the following Yes or No:

Is this manual well organized?	☐ Yes	☐ No
Is the information technically accurate?	☐ Yes	☐ No
Are instructions complete?	☐ Yes	☐ No
Are concepts and wording easy to understand?	☐ Yes	☐ No
Are examples and pictures helpful?	☐ Yes	☐ No
Are there enough examples and pictures?	☐ Yes	☐ No

Comments:

Date _____

Name: _____

Title: _____

Company: _____

Address: _____

City & State: _____

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO. 37 LOVELAND,CO

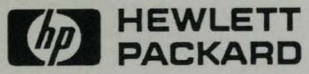
POSTAGE WILL BE PAID BY ADDRESSEE

Hewlett-Packard Company
Colorado Networks Division
3404 East Harmony Road
Fort Collins, CO 80525

ATTN: Network Usability Department

Fold Here

Tape Please do not staple Tape



HP Part Number
B1012-90001
Printed in U.S.A E0989

B1012-90001