HEWLETT PACKARD

HP 9000 Computers

Installing and Administering Network Services

HP 9000 Computers

Installing and Administering Network Services

Customer Order Number: B1012-90014
Printed in U.S.A., October 1992

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

Hewlett-Packard Company
19420 Homestead Road
Cupertino, CA 95014 U.S.A.

Contents

Figures

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 all HP 9000 computers. Any differences in the installation, configuration, operation, or troubleshooting of different series of the HP 9000 are specifically noted.

The link product must be installed for NS to function. The link product provides all the necessary hardware and software to interface between HP 9000 computers 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 HP 9000 computers, refer to the *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 **Virtual Terminal for the HP 3000 (VT3K)**. 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 HP 9000 systems and other systems. Refer to *Networking Overview* and to *NS Cross-System NFT Reference* for details on cross-system NFT.
- 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.

Note Remote File Access (RFA) is no longer included with the Network Services product. In order to maintain distributed file access, you *must* use NFS Services. For more information, see Appendix B.

Node Names

Each computer system or node in an NS network has a name. You must specify **node names** when using the *User Services*. Node names at NS nodes have the following syntax:

node[.*domain*[.*organization*]]

Domain and *organization* names may be useful for grouping nodes and collections of nodes, but they currently have no special meaning regarding the structure of the network within the NS product. When all three parts of the node name are specified, it is called a *fully-qualified node name*.

Each node, domain, and organization name is a maximum of 16 characters long. The maximum total length of a fully-qualified node name is 50 characters. All alphanumeric characters are allowed, including the underscore (_) and dash (-) characters, but the first character of each parameter must be alphabetic. Upper and lower case characters are not considered distinct. For example: `ANIMAL.DCL.IND` would indicate node `ANIMAL` in the `DCL` lab (domain) of the `IND` division (organization).

Note

Nodename and *hostname* may have the same name but are used by different services. For Network Services, the *nodename* must be configured properly and the *hostname* is ignored. The ARPA Services product uses the *hostname*.

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.

Files Created During Software Installation

When the NS software is installed, two symbolic links, one daemon, one server, two binaries, and one message catalog are created.

Table 2-1. Files Created During Software Installation

Files	Function
/etc/nftdaemon	Symbolic link to /usr/bin/nftdaemon
/etc/nftserver	Symbolic link to /usr/bin/nftserver
/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/bin/vt3k	VT3K binary.
/usr/lib/nls/C/ns.cat	NS error message catalog.

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.

When you have successfully installed the NS software:

- You *can* modify your system's NS node name.
- If you plan to use the NS software through a gateway, you *must* create the *probe proxy table*.

Modifying Your System's NS Node Name Using SAM

SAM stands for **System Administration Manager**, a menu-driven utility for performing system administration tasks, including configuration of networking software. When you use SAM to modify this system's NS node name, you are replacing the `/bin/nodename` command in the `/etc/netlinkrc` file. The `/etc/netlinkrc` file is installed during the link product installation.

Tips for Using SAM

Remember the following tips when you use SAM:

- Use your keyboard's cursor control and editing keys to navigate and edit forms.
- Access the on-line help screens whenever you need more information, such as how or where to obtain a required configuration value.

Procedure for Using SAM to Modify the NS Node Name

The following steps tell you how to use SAM to modify your system's NS node name.

1. At the HP-UX prompt, type:

   ```
   sam
   ```

   Wait for SAM's main menu to appear.

2. Select the Networking/Communications menu item.
3. Select Services Enable/Disable.
4. Select the Modify NS Nodename action.
5. Fill in the form according to its instructions. View the Help screens for information about filling in the form. Select OK to enter any changes.
6. From the Services Enable/Disable screen, go to the previous level by selecting Exit from the List menu. At the Networking Communications screen, either exit to the previous level by selecting Previous Level or exit from SAM by selecting Exit SAM.

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 or across an X.25 network. 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 or X.25 network needs to establish a connection with a remote node that exists on a different network or subnetwork or an X.25 network (it does not matter if it is different or the same), 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 and/or X.25 network as the probe proxy server. The probe proxy server can be a gateway, or any other node on the network.

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 *HP-UX Reference* and the link installation manual. For more information about the `/etc/hosts` file, refer to *hosts*(4) in *HP-UX Reference* and the link installation manual.

How Probe Proxy Servers Work with NS

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

- You can initiate a connection from a node on Network A to another node on Network A without a proxy server (see Example 1).
- You can initiate a connection from a node on Network B to another node on 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 a node on Network A to a node on Network B (see Example 3).
- You must have a proxy server on Network B to establish a connection from a node on Network B to a node on Network A that was initiated by a Network A node, 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.

A probe proxy server stores information about other nodes on other networks or subnetworks in a probe proxy table.

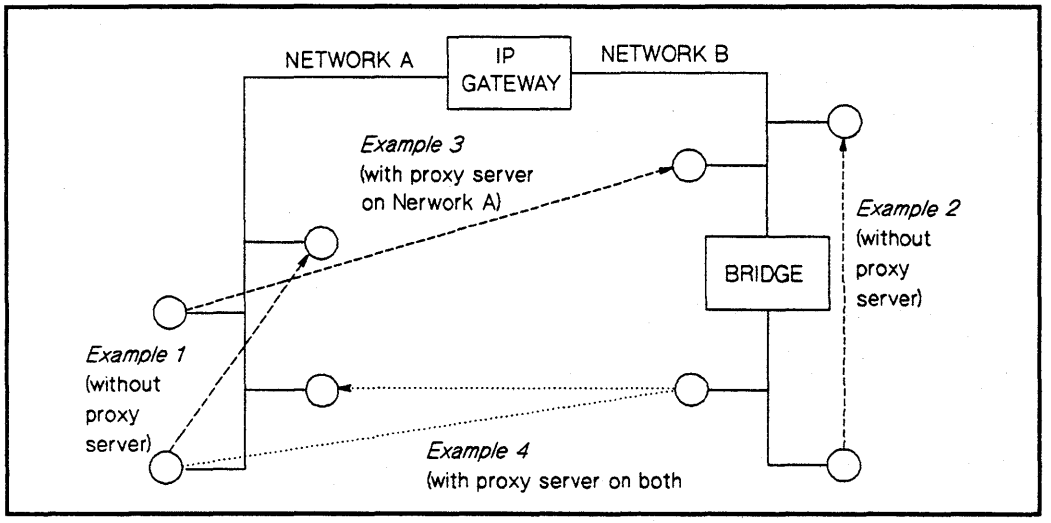

Figure 2-1. How Probe Proxy Servers work with NS

Figure 2-2 illustrates that for X.25, each node intiating the NS connection must be a proxy server and must have a proxy table entry for the remote interface. The IP-to-X.121 address mapping entries must be present on the local and remote nodes.

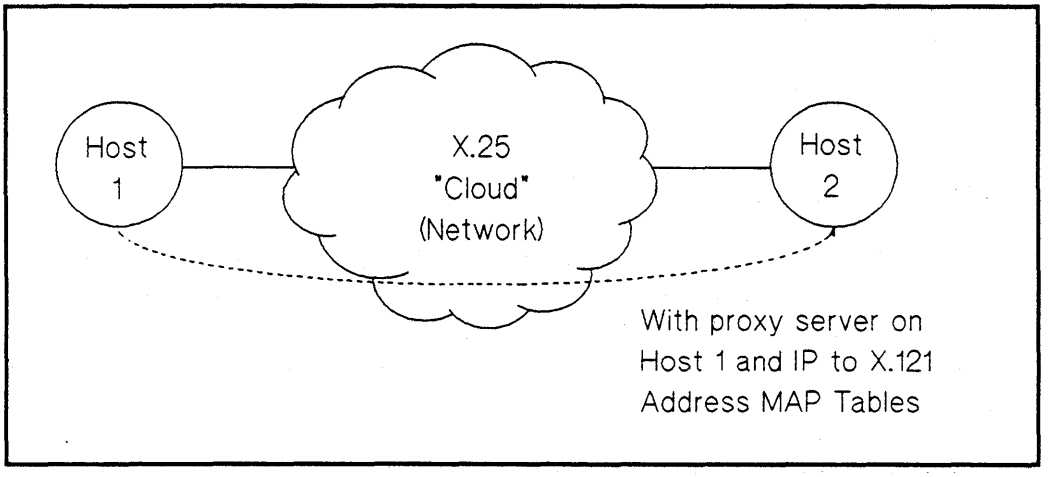

Figure 2-2. An X.25 Example

You manipulate the probe proxy table with the `proxy` command (see *proxy*(1M) in the *HP-UX Reference*) described next.

Setting Up NS Gateway Access

You can access the NS gateway using the `proxy` command. This command manipulates the NS Probe proxy table.

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

Syntax for Probe Proxy Command

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

or

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

Options for Probe Proxy Command

`on` — Enables Probe proxy on a node. You must use this option before being able to change the probe proxy table. Requires superuser capability.

`off` — Disables the proxy server. The probe proxy table is not flushed. Requires superuser capability.

`add` — Adds a new entry to the probe proxy table. Requires superuser 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. (This is a different domain than the Network Information Service (NIS) domain included with the NFS Services product.)
ip_address	IP address of the remote node being mapped by *nodename*. The IP address must be in decimal internet "dot" format. See *inet*(3N) in the *HP-UX Reference* for a description of internet "dot" format, or refer to the link installation manual.
medium	The physical link transmission protocol. Can be either `ieee`, `ether` or `X.25`.

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 superuser 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 superuser capability to use this option.
`flush`	Clears the probe proxy table, deleting all entries. You must have superuser 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.

---

4. Checking the NS Installation

When you have installed, configured and initialized the NS software, make sure that NS is operating correctly on your node by running the NS verification script. The syntax for the NS verification script is as follows:

Syntax for NS Verification

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

Options for NS Verification

`-r` *nodename*	This is an option used to test communication to other HP 9000 computers. *nodename* is the remote system name with which you are testing communications.

login and *password*	These are valid logins and passwords 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

You can test your NS installation manually as follows:

- Use the NS Quick Verification strategy. Use the `dscopy` command to copy a file from an HP 9000 computer to a remote node, then copy the same file back. (See *dscopy*(1) in the *HP-UX Reference*.) 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 fails, test that the NFT daemon is running. Issue the following command:

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

  You should see one network daemon in the table of statistics returned to standard output. If you don't see an entry for the daemon, start it by typing the daemon name (as an absolute pathname) on the command line. See the following example:

  ```
  /usr/bin/nftdaemon
  ```

  You must be superuser to start a network daemon. In order for NFT to work, `nftdaemon` must be running .

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

3

Maintaining NS

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

- Setting up security for NS.
- Modifying the probe proxy table.
- Reference: networking daemons and special files.

The first two sections describe the tasks involved in maintaining the NS product and the commands used to perform these tasks. The third section contains a quick reference list of the daemons provided with the NS product and link product configuration files relevant to the NS product.

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 can 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` command syntax. (For more information on `dscopy`, see *dscopy*(1) in the *HP-UX Reference*.) 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` 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*. In general, do not allow anyone to have permission to access files that they have no reason to use.

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 `dscopy` command. You can alleviate this problem by setting low access capabilities for `who` and `date`, or by removing these logins from the `/etc/passwd` file. The latter solution makes it impossible to execute `who` and `date` without logging in.

Disabled Services

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

You can halt all network traffic on a node by issuing the `/etc/ifconfig lan`*n* `down` command. To halt all network traffic, you must execute an `/etc/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.

Note You can also halt all network traffic on a node by issuing the `x25stop -d dev`. For more information refer to the *Installing and Administering X.25/9000.*

You can prevent access to NFT on HP 9000 computers by not starting the daemon processes. You can use the System Administration Manager (SAM) to enable and disable these processes. The procedure for using SAM is described in the next section.

Note Specific security recommendations for the network diagnostics are documented in *Installing and Administering LAN.* The `ifconfig` command is documented in *Installing and Administering LAN* and in the *ifconfig*(1M) section of the *HP-UX Reference.*

Using SAM to Disable NFT

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

Disabling NFT with SAM. The following steps take you to the `NS (Network Services) Configuration` menu where you can use SAM to disable the `nftdaemon` daemon, preventing anyone from using NFT on this NS node (whether over a LAN or X.25):

1. At the HP-UX prompt, type:

   ```
   sam
   ```

   and wait for SAM's main menu to appear.

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

3. Select `Services Enable/Disable`.

4. Select NS-NFT and choose the Disable action.
5. Answer "Yes" to the question in the pop-up window.

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

---

6. From the Services Enable/Disable screen, go to the previous level by selecting Exit from the List menu. At the Networking Communications screen, either exit to the previous level by selecting Previous Level or exit from SAM by selecting Exit SAM.

Verifying the Service is Disabled

To verify that the NFT 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 /usr/bin/nftdaemon process.

Modifying the Probe Proxy Table

You can use the NS proxy command to modify, add, append, delete and list entries in the probe proxy table. The proxy command is described in Chapter 2.

Reference: Networking Daemons and Special Files

This section provides a quick reference list of the daemons provided with the NS product and link product configuration files relevant to the NS product.

Daemons

When you bring the system up, the `/etc/netnssrc` initialization script starts the `nftdaemon` daemon process (if it is 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*.
`nftdaemon`	The daemon used by Network File Transfer (NFT). This daemon must be running to use inbound or outbound NFT. The `nftdaemon` daemon is located in the `/usr/bin` directory.

Note The `netisr` daemon must run at a higher priority than other network services on the same node.

Configuration Files

There are no configuration files that are unique to the NS product. However, the following configuration files are provided by the link product and include information relevant to the NS product:

`/etc/hosts`	This file contains the internet addresses, host 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 command errors. Some problems require more investigation.

Once identified, most problems can be resolved by the 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 that 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 problems.
- Diagnosing gateway and repeater problems.
- Flowchart format.
- Troubleshooting Network Services.

- Contacting your HP support 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? Can the problem be reproduced? Did the problem occur under any of the following circumstances:
   - 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 `lan`*n*, 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.
- 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`	A nodal management command which returns statistical information regarding your network. (See *netstat*(1) in the *HP-UX Reference*.)
`landiag`	A diagnostic program that tests LAN connections between HP 9000 computers.
`linkloop`	A diagnostic program that runs link-level loopback tests between the HP 9000 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`	A diagnostic program that verifies the physical connection to a remote host and reports the round-trip communications time between the local and remote hosts. (See *ping*(1M) in the *HP-UX Reference*.)

Table 4-1. Diagnostic Tools

Tool	Function
`psidad`	A utility under DUI that can help to identify problems on the PSI/800 board/card.
`rlb`	A diagnostic program which tests LAN connections to other HP 9000 computers. `rlb` does not test a connection to an HP 1000 computer. (See *rlb*(1M) in the *HP-UX Reference*.)
`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 Problems

The first step in investigating interactive 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, although some of the explanations refer to internal procedures comprehensible only to qualified HP representatives. You are not expected to understand these explanations, but should follow the actions documented in the manuals.

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

- *Syntax errors or invalid options*. These errors occur when you incorrectly issue a command. To correct the error, check for the correct syntax and reissue the command.
- *Warnings*. Warnings are issued when a command is still executable but the results may not be what you intended. These occur when you specify conflicting options. 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, notify the network manager.
- *Internal Errors*. These errors indicate that the software is malfunctioning. If they ever occur, have your network manager help to notify your HP representative. Follow the steps outlined in "Contacting Your HP Representative" at the end of this chapter.

For more information on command syntax errors and warnings, see the *HP-UX Reference*.

Diagnosing Gateway and Repeater Problems

If you are using a gateway or repeater and you are having difficulty communicating with a host that resides on the other side of the gateway or repeater, then a gateway or repeater failure may have occurred.

Locating the problem can get complicated if you are dealing with a Local Area Network (LAN) as well as a Wide Area Network (WAN). Diagnostic tools are available in the LAN and WAN link products that can help you isolate the problem. For information on these tools, refer to *Installing and Administering LAN/9000* or *Installing and Administering X.25/9000*.

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.

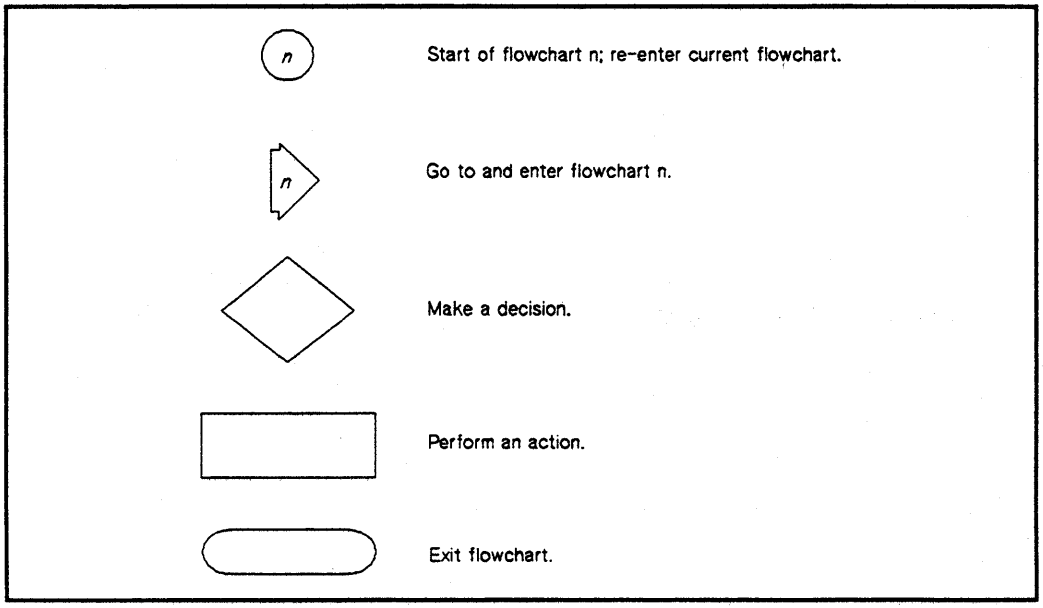

Figure 4-1. Flowchart Format

Troubleshooting Network Services

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

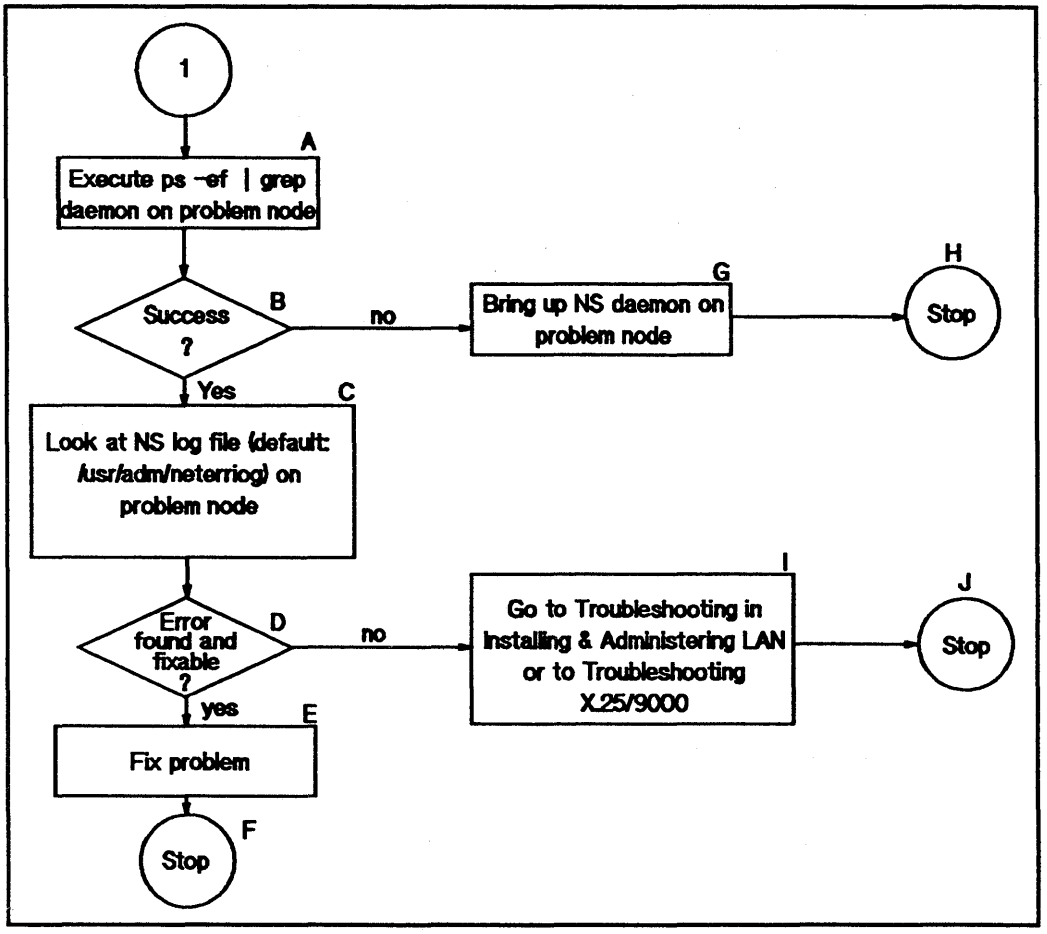

Figure 4-2. Troubleshooting Network Services

Flowchart 1. NS Troubleshooting

A. 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 B.

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

C. 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 D.

D. Error found and fixable? If so, proceed to E; otherwise, proceed to I to examine lower-level NS software.

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

F. Stop. If you solved your NS problem, stop troubleshooting.

G. 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, or `sockregd` for the NetIPC socket registry. Retry the NS activity which prompted you to troubleshoot. Proceed to H.

H. Stop. If you solved your NS problem, stop troubleshooting.

I. Go to *Installing and Administering LAN* to check LAN Link connectivity and lower-level software integrity or go to *Troubleshooting X.25/9000*. Proceed to J.

J. Stop. If you solved your NS problem, stop troubleshooting.

Contacting Your HP Support 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 a Service Request (SR) and forward it to your HP Service Representative. Include the following information where applicable:

- A characterization of the problem: Describe whether or not the system ever worked or if it worked once and then failed. 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 (8.0 Version) and/or X.25/9000 Series 300/800 (8.0 Version).

  To check your NS, LAN, or X.25 version, execute the `what` *file_name* command, where *file_name* is one or more of the following files:

  ```
  /usr/bin/dscopy
  /usr/bin/nftdaemon
  /usr/bin/nftserver
  /usr/bin/vt3k
  ```

  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 network map 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 to gather information about your problem:
  - *Using Network Services*.
  - *Installing and Administering LAN/9000*.
- 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/savecore` to save a core dump. Refer to the *System Administration Tasks* manual for details. Send the output to your HP support 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.

Note VT3K only supports V+ applications.

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 600/800 (connected via LAN to an HP 3000).
- Series 300/400/700 workstation (connected via LAN to an HP 3000) running HPTERM.

`Hpterm` (only HP-UX 7.0 or later) offers HP Block Mode terminal emulation if you use X-Windows on a Series 300/400 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`) from HP-UX to your HP 3000. Ensure `dscopy` is working between the two systems. (See *rlb*(1) and *dscopy*(1) in the *HP-UX Reference*.)

Troubleshooting VT3K

Note If you are using X-Windows, make sure your `hpterm*termId:` is set to `2392A`.

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 occur during NS software installation and configuration.

These error messages may be returned by the LAN nodal management commands `nodename`, `route`, `netstat`, and `ifconfig`. (See *nodename*(1), *route*(1M), *netstat*(1), and *ifconfig*(1M) in the *HP-UX Reference*).

Message `permission denied`

Cause Permission to execute either the `nodename` or `ifconfig` commands was denied.

Action You must be a superuser to use the `nodename` command to configure a node name or to set flags; you must also be a super-user to use the `ifconfig` 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` command was used to print the node name before the `nodename` command was used to configure the system node name.

Action Use `nodename` 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` 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 C will be used.`

Cause This error can be returned from the `ifconfig`, `netstat`, `nodename`, `route`, and `rlb` 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` without specifying an IP address.

Action Execute the `ifconfig` 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 someone other than the 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.

B

Moving from RFA to NFS

Remote File Access (RFA), one of the Network Services, has been discontinued. When you used networks consisting of all HP systems, RFA provided distributed file access among HP 9000 computers. In order to maintain distributed file access, you must move to NFS Services.

Why Move to NFS Services?

Using NFS Services in place of the RFA service has several advantages:

- NFS works with other vendors' equipment and other operating systems.
- NFS is a defacto industry standard.
- NFS allows transparent file access.
- NFS with the Network Information Service (NIS) provides centrally administered databases.

Use this appendix to translate your RFA applications to NFS applications.

Similarities

HP NFS Services and RFA have the following similarities:

- No remote device access.
- Not all UNIX® semantics are fully supported.

Differences

Refer to the following table for a list of differences between HP NFS and RFA.

NFS Services	RFA (Discontinued)
You can run `setuid` programs accessing data on remote file systems.	You cannot run `setuid` programs accessing data on remote file systems.
NFS operates in a heterogeneous operating system environment.	RFA operates on HP-UX operating systems only.
Only the super-user can perform remote NFS mounts.	All users can establish access to remote file systems.
You can centrally administer your databases using NIS.	You have no centrally administered database.
All users with read access to the mount point can read the remote file system.	Only users performing `netunam` can access the remote file systems.
Read and write file caching occurs on the clients; read caching occurs on the servers.	Read and write file caching occurs on the servers; caching does not occur on the clients.
The servers are stateless (do not remember client activities) and therefore, can be rebooted without interfering with client activities. (The client can resume access to the server when it is rebooted.)	The servers have state and therefore, remember the activities in which the client is involved.
One mount gives you access to only one file system.	One `netunam` gives you access to all file systems under the root directory.

Changing Scripts from RFA to NFS

Changing RFA scripts to NFS requires only minor changes. You can change both shell scripts that accept different path names and those that use hard-coded path names.

Shell Scripts that Accept Different Paths

Shell scripts that accept different paths require the following modifications:

- You must perform a remote mount of a file system or directory in *one* of the following ways:
  - As part of the script.
  - Before executing the script.

  Since superuser must execute mounts, the script must be `setuid root` if the mount is performed as part of the script.

Caution Having setuid root scripts is a potential security problem.

If the script's owner does not have superuser permissions, the superuser can configure `/etc/checklist` to automatically mount the remote file systems at boot time. This process allows users to execute scripts without checking to see if the remote file system is accessible.

- Remove all calls to `netunam` from the script. Removing these calls prevents `netunam` failures from causing the scripts to fail.

Shell Scripts with Hard-Coded Paths

You can handle shell scripts with hard-coded path names in two ways:

- Change the path name in the script to correspond to the NFS mount point.
- Create a path name for the NFS mount point which corresponds to the path name in the script.

To mount the remote file system either as part of the script or automatically via `/etc/checklist`, you must modify the shell scripts as described in the previous section, "Shell Scripts that Accept Different Paths."

Change Pathnames

Change the path name in the script to correspond to the NFS mount point.

EXAMPLE: The script has a hard-coded path name of `/net/systemB/project`. Mount the remote directory `/project` on `/user/project` as follows:

```
mount systemB:/project /user/project
```

Now change the script to use the path name `/user/project` in place of `/net/systemB/project`.

Create New Pathnames

Create a path name for the NFS mount point that corresponds to the path name in the script.

EXAMPLE: The script has a hard-coded path name of `/net/systemB/project` which accesses the remote directory `/project`. To keep the path name the same:

1. Remove the network special file `/net/systemB`.

2. Create the directories `/net/systemB` and `/net/systemB/project`:

```
mount systemB:/project /net/systemB/project
```

Note

For RFA, access to the remote system occurred via a network special file. Creating an NFS mount point with the same name as the network special file for the remote system could cause confusion. Problems will not occur if you remove the network special file.

All remote access will then be via mount points that have the same names as the network special files that were removed.

Index

T

U

V

Printed in USA 10/92

Customer Order No.
B1012-90014

Manufacturing No.
B1012-91014
Mfg. number is for HP internal use only

B1012-91014