HP 9000 Networking

Using Internet Services

HP Part No. B2355-90111
Printed in U.S.A.
E0696

Edition 5

Legal Notices

The information in this document is subject to change without notice.

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

Warranty. A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

Restricted Rights Legend. Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Hewlett-Packard Co.
19420 Homestead Road
Cupertino, CA 95014 USA

Use of this manual and flexible disk(s) or tape cartridge(s) supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and back-up purposes only. Resale of the programs in their present form or with alterations, is expressly prohibited.

Copyright Notices

Trademark Notices

Preface

This manual describes how to use the HP 9000 Internet Services product. It is intended for people who have experience with HP-UX and access to the HP-UX man pages.

For information on administering the Internet Services, see *Installing and Administering Internet Services*.

For information on how to use **`elm`** and **`mailx`**, see *Mail Systems: User's Guide*.

Contents

Contents

1

Logging into a Host with `telnet`

`telnet` is used to log into a remote HP-UX, UNIX, or non-UNIX host that supports the ARPA services. It allows you to do work on the remote host as if you were using a terminal directly attached to the remote host. For more information, type **`man 1 telnet`** at the HP-UX prompt.

Checking Your Local Terminal Configuration

Before you log into a remote host with **telnet** or **rlogin**, ensure that your local terminal configuration settings are correct for the type of remote communication you intend to perform. Two factors determine whether you need to change your local terminal configuration settings:

- The type of remote host you intend to log into.
- The type of applications you intend to run on the remote host.

Follow these guidelines if you have an HP terminal attached to an HP 9000 computer as your local host:

- Whenever you log into a remote DEC VAX VMS host, the HP terminal should be set to ANSI compatibility mode. Set the ANSI terminal configuration to map **DEL** (ASCII 127) to the backspace key and to use the **XON/XOFF** protocol handshake.
- Whenever you communicate with a remote HP host, the HP terminal should be set to HP compatibility mode. Set the HP terminal configuration to map **BS** (ASCII 8) to the backspace key and to use the **ENQ/ACK** protocol handshake.

These terminal configuration settings ensure that both screen-oriented and line-oriented applications work properly when run on a remote host through **telnet** or **rlogin**. Other terminal configuration settings do not need attention.

In general,

- Remote line mode applications work well over **telnet** or **rlogin** regardless of your local terminal's compatibility mode setting.
- Remote screen mode applications require your local terminal and the remote host to use the same commands to control cursor movement.
- Remote block mode applications do not work over **telnet** or **rlogin** and are not supported.

For more details, see the terminal documentation for the hosts with which you work.

Using `telnet`

1 Type **`telnet`** at the HP-UX prompt.

```
telnet
```

This starts **`telnet`** in its command state. In command state, **`telnet`** displays the **`telnet>`** prompt. From command state, you can execute **`telnet`** commands. Type **`?`** at the **`telnet>`** prompt for a list of **`telnet`** commands.

2 At the **`telnet>`** prompt, type **`open`** ***`hostname`*** or **`open`** ***`IP_address`***, as in the following example, to connect to a remote host:

```
telnet> open hpabsa
```

3 Type your user name and password when the remote host prompts you for it. If you are using the Secure Internet Services version of **`telnet`** you will not be prompted for a login or password. You *must* have a valid login to the remote host in order to connect to it with **`telnet`**.

After you log into the remote host, **`telnet`** is in input state. When **`telnet`** is in input state, you can use the remote host as if your terminal or workstation were physically connected to that host.

If certain keystrokes do not do what you expect them to do, or if your display does not look right, see “Checking Your Remote Terminal Configuration” on page 11.

4 When you have finished working on the remote host, type the **`telnet`** escape character to return to command state. The escape character is **`CTRL-]`** if you have not changed it with the **`telnet escape`** command.

5 At the **`telnet>`** prompt, type **`close`** ***`hostname`***, as in the following example, to disconnect from the remote host:

```
telnet> close hpabsa
```

6 Type **`quit`** to exit from **`telnet`**.

```
telnet> quit
```

A Faster Way to Use `telnet`

1 Type **`telnet`** ***`hostname`*** or **`telnet`** ***`IP_address`*** at the HP-UX prompt, as in the following example:

```
telnet hpabsa
```

2 Type your user name and password when the remote host prompts you for it. If you are using the Secure Internet Services version of **`telnet`** you will not be prompted for a login or password. You *must* have a valid login to the remote host in order to connect to it with **`telnet`**.

After you log into the remote host, **`telnet`** is in input state. When **`telnet`** is in input state, you can use the remote host as if your terminal or workstation were physically connected to that host.

If you notice that certain keystrokes do not do what you expect them to do, see “Checking Your Remote Terminal Configuration” on page 11.

3 When you have finished working on the remote host, type **`exit`** to log out of the remote host and exit from **`telnet`**.

```
exit
```

Checking Your Remote Terminal Configuration

After you have connected to the remote host, if you are using an HP terminal or an HP terminal emulator (like a terminal window in HP VUE), follow this procedure to check your terminal settings on the remote host.

1 Issue the following command at the remote host's command prompt to make sure your terminal type is set to **hp**:

```
echo $TERM
```

2 If your terminal type is not set to **hp**, issue the following command:

```
eval ‘tset -s hp‘
```

Be sure to use backticks, not regular single quote marks.

3 Issue the following command at the remote host's command prompt to check your terminal settings:

```
stty
```

You should have the following terminal settings (among others):

```
intr = ^C
erase = ^H
kill = ^U
```

4 If your terminal settings are not correct, issue the following command to set them:

```
stty intr \^C erase \^H kill \^U
```

Type **man 1 stty** or **man 1 tset** for more information.

Changing the Behavior of Carriage Returns

When some remote hosts send a carriage return to your local host, your local host may need to change the carriage return into a carriage return-line feed combination.

1 Watch for the following behaviors, which indicate that **telnet**'s carriage return mode setting is wrong for the type of remote host to which you are connected:

- If pressing **Return** produces double-spaced lines (indicating an extra line feed), you need to disable carriage return mode.
- If pressing **Return** moves the cursor to the beginning of the same line so that the same line keeps getting overwritten (indicating no line feed), you need to enable carriage return mode.

2 If you are not at the **telnet>** prompt, enter the **telnet** escape character (usually **CTRL-]**) to display the prompt.

3 At the **telnet>** prompt, type the following:

```
toggle crmod
```

If carriage return mode was on, **telnet** turns it off and displays the following:

```
Won't map carriage return on output.
```

If carriage return mode was off, **telnet** turns it on and displays the following:

```
Will map carriage return on output.
```

If you are connected to a remote host, **telnet** returns you to the remote host. To redisplay the remote host's prompt, press **Return**.

Obtaining Help

You can obtain summary information about **telnet** commands with **telnet**'s **?** command. You can either list the commands or get information about a specific command.

Listing the telnet Commands

1 If you are not at the **telnet>** prompt, enter the **telnet** escape character (usually **CTRL-]**) to display the prompt.

2 At the **telnet>** prompt, enter the following:

```
?
```

telnet lists its commands.

NOTE: If you were connected to a remote host and want to redisplay its prompt, press **Return** twice.

Getting Information about a Specific telnet Command

1 If you are not at the **telnet>** prompt, enter the **telnet** escape character (usually **CTRL-]**) to display the prompt.

2 At the **telnet>** prompt, enter the following:

```
? telnet_command
```

For example, if you typed **? open**, **telnet** would display the following information about the **open** command:

```
connect to a site
```

NOTE: If you were connected to a remote host and want to redisplay its prompt, press **Return** twice.

2

Logging into a Host with `rlogin`

`rlogin` is used to log into a remote HP-UX or UNIX host from your local host. It allows you to do work on the remote host as if you were using a terminal directly attached to the remote host. For more information, type **`man 1 rlogin`** at the HP-UX prompt.

Using `rlogin`

If you have an account on a remote host, you can use **`rlogin`** to log into the remote host. Follow these steps:

1. Before you log into a remote host with **`rlogin`**, ensure that your local terminal configuration settings are correct for the type of remote communication you intend to perform. See “Checking Your Local Terminal Configuration” on page 8.
2. Issue the following command:

   ```
   rlogin remote_hostname [-l remote_login_name]
   ```

   Use the **`-l`** ***`remote_login_name`*** option if your login name on the remote host is different from the login name for your local account.
3. Type the login name and password for your account on the remote host when you are prompted for it. If you are using the Secure Internet Services version of **`rlogin`** you will not be prompted for a password.

   If certain keystrokes do not behave the way you expect them to, or if your display does not look right, see “Checking Your Remote Terminal Configuration” on page 11.
4. When you have finished your work on the remote system, log out as you ordinarily do (for example, by typing **`exit`** or **`CTRL-D`**).

   `rlogin` logs you out of the remote host, disconnects from the remote host and returns you to the HP-UX prompt on your local host.

If the system administrator for the remote host has configured your local host’s name in the remote host’s **`/etc/hosts.equiv`** file, and if your login name on the local host matches your login name on the remote host, you do not have to supply a password when you log in.

You can configure a **`.rhosts`** file in your home directory on the remote host that allows you to log in from the local host without supplying your remote login name and password. See “Creating a $HOME/.rhosts File on a Remote Host” on page 17.

Creating a $HOME/.rhosts File on a Remote Host

If you have an account on a remote host, you can set up the account so that you can log into the remote host without having to supply your remote login name and password. Follow these steps:

1 If you do not know where your home directory is, log into the remote host and issue this command to find out:

```
echo $HOME
```

2 Create a file called **.rhosts** in your home directory on the remote host, if it does not already exist, and add the following line to it:

```
your_local_host's_name  your_local_login_name
```

3 Issue the following command to make sure that your remote **.rhosts** file is owned by you, the user:

```
ls -l .rhosts
```

4 Issue the following command to protect your remote **.rhosts** file so only you can read it:

```
chmod 0400 .rhosts
```

5 Move to the parent directory of your home directory, and issue the following command to protect your remote home directory so that no one else can write to it:

```
chmod 0755 your_home_directory
```

Type **man 4 hosts.equiv** for more information on the **.rhosts** file.

CAUTION: A **$HOME/.rhosts** file creates a significant security risk. Because of this, its functionality may be disabled by the system administrator on the remote host. If it has been disabled, your **$HOME/.rhosts** file will not work even if it exists on your system.

3

Transferring Files with `ftp`

With **`ftp`**, you can transfer files among HP-UX, UNIX, and non-UNIX network hosts that support ARPA services. For more information, type **`man 1 ftp`** at the HP-UX prompt.

Using `ftp`

1 Issue the following command to establish a connection with the remote host:

```
ftp remote_host_name or remote_IP_address
```

2 Type your user name when prompted for it by the remote host. If you do not have an account on the remote host, type **`anonymous`** or **`ftp`** as the user name to get access to the anonymous **`ftp`** directory. Anonymous **`ftp`** allows you access *only* to the directory that is set up for anonymous **`ftp`**.

3 Type your password when prompted for it by the remote host. If you are logging in as **`anonymous`**, type your user name and local host name as the password:

```
user_name@local_host_name
```

Note that if you are using the Secure Internet Services version of **`ftp`** you will not be prompted for a password.

4 Set the transfer type, if necessary. The **`binary`** type may be used to transfer all types of files. To find out the current transfer type, type **`status`** at the **`ftp>`** prompt. To set the transfer type to binary, type **`binary`** at the **`ftp>`** prompt.

5 You can perform directory operations on the remote host, by issuing commands like **`pwd`**, **`cd`**, and **`ls`**. For a list of **`ftp`** commands, type **`?`** at the **`ftp>`** prompt. For help on a specific command, type **`? command`** at the **`ftp>`** prompt.

To perform directory operations and other shell commands on the local host, put an exclamation point before the command, for example, **`!ls`**.

6 At the **`ftp>`** prompt, use the **`put`** or **`get`** command to transfer files between the local and remote systems:

```
ftp> put filename [destination_filename]
ftp> get filename [destination_filename]
```

The **`put`** command transfers a file from the local host to the remote host. The **`get`** command transfers a file from the remote host to the local host. If you do not specify a ***`destination_filename`***, the copy of the file will have the same name as the original.

7 To exit from **`ftp`** and return to the HP-UX prompt on your local host, type **`quit`** at the **`ftp>`** prompt.

Setting Up Automatic Remote Login for `ftp`

If you have an account on a remote host, you can create a **`.netrc`** file in your local home directory that allows you to log into the remote host without supplying your remote login name and password. The **`.netrc`** file can be useful for programs that need to perform **`ftp`** operations unattended. Follow these steps:

1 Create a file called **`.netrc`** in your home directory on the local host, if it does not already exist, and add the following line to it:

```
machine host_name login login_name password password
```

The following example allows you to use **`ftp`** to log into host **`basil`** as user **`andy`** without supplying the user name or the password, which is **`pre10der`**.

```
machine basil login andy password pre10der
```

2 Issue the following command to make sure that your **`.netrc`** file is owned by you, the user:

```
ls -l .netrc
```

3 Issue the following command to protect your **`.netrc`** file so only you can read it:

```
chmod 0400 .netrc
```

4 Move to the parent directory of your home directory, and issue the following command to protect your home directory so that no one else can write to it:

```
chmod 0755 your_home_directory
```

For more information, type **`man 4 netrc`** at the HP-UX prompt.

CAUTION: The **`.netrc`** file creates a security risk. Passwords in this file are unencrypted.

4

Transferring Files with `rcp`

With **`rcp`**, you can copy files between HP-UX or UNIX hosts. **`rcp`** can copy the contents of an entire directory, including the contents of all subdirectories within that directory. From your local host, you can also copy files between two remote hosts. Type **`man 1 rcp`** for more information.

Enabling `rcp`

Before you can use **`rcp`** to copy files to or from a remote host, the remote host must be configured in one of two ways:

1. You must have an account on the remote host with the same login name as your local login name, *and* the name of your local host must be in the remote host's **`/etc/hosts.equiv`** file.
2. You must have an account on the remote host, *and* the name of your local host and your local login name must be in a **`.rhosts`** file in your home directory on the remote host.

   See "Creating a $HOME/.rhosts File on a Remote Host" on page 17.

Using `rcp`

You can use **`rcp`** to copy one or more files or directories from the local host to a remote host, as in the following example:

```
rcp /tmp/memo1 /tmp/memo2 basil:/home/basil/roger
```

This example copies **`/tmp/memo1`** and **`/tmp/memo2`** from the local host to user **`roger`**'s home directory on host **`basil`**. The last path on the command line is taken as the destination path, and all paths before it are copied to the destination.

You can use **`rcp`** to copy one or more remote files or directories to the local host. With the **`-r`** (recursive) option, you can use **`rcp`** to copy the contents of a directory and all its subdirectories, as in the following example:

```
rcp -r sage:/home/sage/gwen /home/dill/gwen
```

This example copies the contents of user **`gwen`**'s home directory from host **`sage`** to the directory **`/home/dill/gwen`** on the local host.

If you do not specify a full path name, the path name is interpreted relative to your home directory, as in the following example:

```
rcp memo* *mail sage:june_mail
```

This example copies all files whose names begin with **`memo`** and all files whose names end with **`mail`** from the user's local home directory to the directory **`june_mail`** in the user's home directory on host **`sage`**.

NOTE: Any output generated by commands in a **`.login`**, **`.profile`**, or **`.cshrc`** file on the remote host can cause **`rcp`** errors.

CAUTION: Do not attempt to copy a file over itself, as in the following example:

```
rcp /home/cheryl/.profile /home/cheryl/.profile
```

This can corrupt the file's contents.

5

Executing Commands with `remsh`

`remsh` allows you to execute commands on a remote HP-UX or UNIX host on the network. **`remsh`** is the same command as **`rsh`** in 4.2 BSD and later versions. Type **`man 1 remsh`** for more information.

Enabling `remsh`

Before you can use **`remsh`** to execute commands on a remote host, the remote host must be configured in one of two ways:

1. You must have an account on the remote host with the same login name as your local login name, *and* the name of your local host must be in the remote host's **`/etc/hosts.equiv`** file.
2. You must have an account on the remote host, *and* the name of your local host and your local login name must be in a **`.rhosts`** file in your home directory on the remote host.

   See "Creating a $HOME/.rhosts File on a Remote Host" on page 17.

Using remsh

The **remsh** command has the following syntax:

```
remsh remote_host [-l remote_login_name] command[\;command...]
```

If you do not give any commands on the **remsh** command line, **remsh** interprets any options in the command line as **rlogin** options and runs **rlogin**.

Shell metacharacters (like <, |, or >>) are interpreted on the local host, unless you enclose them in double quotes. For example, the following command creates **newfile** on host **basil**. Without the quotes, it would create **newfile** on the local host.

```
remsh basil cat my_message ">" newfile
```

CAUTION: Do not use **remsh** to run an interactive command, such as **vi** or **more**. With some interactive commands, **remsh** hangs. To run interactive commands, log into the remote host with **rlogin**.

The following example uses the **find** command to look for the file **status.july** in the **project** directory on remote host **basil**:

```
remsh basil find /project -name status.july -print
```

In the following example, a user on the local system uses **remsh** to create a file called **hi_mike** in user **mike**'s home directory on remote host **sage**:

```
remsh sage cd /home/sage/mike\;echo Hi, Mike! ">" hi_mike
```

In the following example, a user uses **remsh** to log into user **paula**'s home directory on host **basil** and mail the **meeting_minutes** file to the members of the **proj_team** mailing list:

```
remsh basil -l paula mailx proj_team "<" meeting_minutes
```

6

Listing Hosts with `ruptime`

`ruptime` lists status information about HP-UX or UNIX hosts on the local area network. This information is useful in identifying which network hosts you can use and how responsive each host is likely to be over the network.

Using `ruptime`

For each network host, **`ruptime`** displays a status line with the following format:

```
hostname up|down days+hours:minutes n users load n.nn, n.nn, n.nn
```

`hostname`	The name of a host on the network. One line is displayed for each host on the local network that is running the **`rwhod`** daemon.
`up|down`	The status of the host. If the local host stops hearing from a remote host's **`rwhod`** daemon, that host is considered down.
`days+hours:minutes`	The length of time the host has been up or down.
`n` **`users`**	The number of users logged into the host.
`load`	The average number of jobs in the run queue over the last 5, 10, and 15 minutes.

By default, **`ruptime`** displays status lines sorted in alphabetical order by host name. You can use different command-line options to sort the status lines by different fields, in increasing or decreasing order.

By default, **`ruptime`** lists the number of active users logged in. **`ruptime`** does not count users who have not used the system for an hour or more. To include idle users in status lines, use the **`-a`** option:

```
ruptime -a
```

For more information, type **`man 1 ruptime`** at the HP-UX prompt.

NOTE: **`ruptime`** is not supported across X.25 links or networks using the PPL (SLIP) product.

`ruptime` Examples

The following example lists hosts in alphabetical order and includes idle users in the output:

```
ruptime -a

hpabca    down    14+08:34
hpabcb    down        1:13
hpabcc    up       1+17:40,   6 users,   load 0.18, 0.13, 0.09
hpabcd    up      14+06:49,   3 users,   load 0.10, 0.38, 0.49
```

The following example lists hosts sorted by increasing load average. Idle users are not included.

```
ruptime -r -l

hpabca    down    14+08:34
hpabcb    down        1:13
hpabcd    up      14+06:49,   3 users,   load 0.10, 0.38, 0.49
hpabcc    up       1+17:40,   4 users,   load 0.18, 0.13, 0.09
```

7

Listing Users with `rwho`

`rwho` lists information about HP-UX or UNIX hosts on the local area network. This information is useful in identifying who is logged into the hosts on the network and who is likely to be at their terminal or workstation.

Using rwho

For each user logged into a network host, **rwho** displays an information line with the following format:

```
user  host.line  month day  hours:minutes  hours:minutes
```

user The user's login name.

host The host to which the user is logged in. Only hosts running the **rwhod** daemon will be displayed.

line The user's terminal line.

month day The date the user logged in.

hours*:*minutes The time the user logged in (in 24-hour clock notation).

hours*:*minutes The amount of time the user has been idle (in 24-hour clock notation).

With **rwho**, you can list either of the following:

- Users on network hosts who are active or who have been idle for less than one hour.
- All users logged into network hosts, regardless of the amount of time any of them has been idle.

rwho gets its information by broadcasting a query to the local area network. Only hosts running the **rwhod** daemon will respond to the query.

rwho's list of users can get very long when a large number of users are logged into network hosts.

NOTE: **rwho** is not supported across X.25 links or networks using the PPL (SLIP) product.

For more information, type **man 1 rwho** at the HP-UX prompt.

rwho Examples

The following example lists all active users and all users who have been idle for less than an hour:

```
rwho

acb       hpabcd:ttyp3    Jun 2 08:32    :19
bjt       hpabcf:tty3p3   Jun 2 09:35          <--Active
chas      hpabcd:tty3p3   Jun 2 07:47    :27
cjc       hpabcd:tty1p2   Jun 2 07:55          <--Active
dae       hpabcf:ttyp2    Jun 2 08:28    :57
```

The following example lists all users logged into network hosts, including those that have been idle for more than an hour:

```
rwho -a

acb       hpabcd:ttyp3    Jun 2 08:32     :19
bjt       hpabcf:tty3p3   Jun 2 09:35          <--Active
chas      hpabcd:tty3p3   Jun 2 07:47     :27
cjc       hpabcd:tty1p2   Jun 2 07:55          <--Active
dae       hpabcf:ttyp2    Jun 2 08:28     :57
gen       hpabcd:ttyp4    Jun 2 08:45    5:59
kg        hpabcd:ttyp0    Jun 2 08:09    1:02
scb       hpabce:tty3p1   Jun 2 12:12    3:24
```

8

Secure Internet Services

Secure versions of the **`ftp`**, **`rcp`**, **`remsh`**, **`rlogin`** and **`telnet`** services are available in the optionally installable product **`InternetSvcSec`**. The secure versions of these services implement the Kerberos V5 authentication mechanism and are referred to as the Secure Internet Services.

The main benefit of running the Secure Internet Services is that the user's security is enhanced because user authorization no longer requires transmitting a password in a readable form over the network.

CAUTION: None of the Secure Internet Services encrypts the session beyond what is necessary to authorize the user or authenticate the service. Thus, these services do not provide integrity checking or encryption services on the data or on remote sessions.

Using the Secure Internet Services

1 Identify yourself to the Security Server, also known as the KDC (Key Distribution Center), by issuing the **kinit** command:

```
kinit user_name@realm_name
```

To identify yourself to an HP DCE Security Server, you would generally use the **dce_login** command rather than **kinit**.

2 Start the service (**ftp**, **rcp**, **remsh**, **rlogin** or **telnet**) the same way you would start the non-secure version of the service. The following example starts **ftp**:

```
ftp remote_host_name
```

Note that when you using the Secure Internet Services you will not be prompted for a password.

3 To connect to a host running a non-secure version of the service, use the **-P** option to bypass Kerberos authentication, as in the following example:

```
ftp -P remote_host_name
```

If the **-P** option has been invoked, and if a password is required to access the remote host, the password will be transmitted in a readable form over the network. In this case, you will receive appropriate warning messages.

Note that system administrators have the option of enforcing Kerberos authentication. If this has been done to a host running Secure Internet Services daemons, neither access from a secure client using the **-P** option or access from a non-secure client will be allowed.

4 When you are finished with the secure session, issue the **kdestroy** command to remove the credentials you accumulated during the session:

```
kdestroy
```

If the Secure Internet Services product is installed and enabled on your system, there are several man pages you may wish to consult for more information. See the man page **sis**(5), which contains information common to all the Secure Internet Services including warning and error messages. For information specific to the individual services, see the following man pages: **ftp**(1), **ftpd**(1M), **rcp**(1), **remsh**(1), **remshd**(1M), **rlogin**(1), **rlogind**(1M), **telnet**(1), and **telnetd**(1M). For information on some common Kerberos utilities see the following man pages: **kinit**(1), **klist**(1), and **kdestroy**(1).

Index