

TCPware 6.1 Installation & Configuration Guide

September 2023

This document provides the system manager with the procedures for installing, configuring, and starting up TCPware.

Operating System/Version: OpenVMS VAX V5.5-2 or later

OpenVMS Alpha V6.2 or later

OpenVMS Itanium V8.2 or later

Software Version: TCPware 6.1

**Process Software
Framingham, Massachusetts
USA**

The material in this document is for informational purposes only and is subject to change without notice. It should not be construed as a commitment by Process Software. Process Software assumes no responsibility for any errors that may appear in this document.

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.

Third-party software may be included in your distribution of TCPware, and subject to their software license agreements. See www.process.com/products/tcpware/3rdparty.html for complete information.

All other trademarks, service marks, registered trademarks, or registered service marks mentioned in this document are the property of their respective holders.

TCPware is a registered trademark and Process Software and the Process Software logo are trademarks of Process Software.

Copyright ©2021 Process Software Corporation. All rights reserved. Printed in USA.

If the examples of URLs, domain names, internet addresses, and web sites we use in this documentation reflect any that actually exist, it is not intentional and should not to be considered an endorsement, approval, or recommendation of the actual site, or any products or services located at any such site by Process Software. Any resemblance or duplication is strictly coincidental.

Preface

Introducing This Guide

This guide describes the TCPware software installation, configuration, and startup procedures. It is for system managers, administrators, or operators.

What You Need to Know Beforehand

Before using TCPware, you should be familiar with:

- The TCPware for OpenVMS products, components, features, and capabilities (see the *User's Guide* for more information)
- Computer networks in general
- HPE's OpenVMS operating system and file system

How This Guide Is Organized

This guide has the following contents:

- Chapter 1, *Before You Begin*, explains the installation and configuration procedures, and what you need to prepare for an installation.
- Chapter 2, *Installing TCPware*, provides a step-by-step procedure for executing the software installation.
- Chapter 3, *Configuring the TCP/IP Core Environment*, explains how to configure the TCP-OpenVMS component (the TCP/IP core environment).
- Chapter 4, *Configuring the TCP/IP Services*, provides step by step procedures for configuring each of the TCP/IP Services components.
- Chapter 5, *Starting and Testing TCPware*, explains how to get TCPware up and running and to test its configuration.
- Appendices, including a sample installation and configuration, and a list of installed files.

Online Help

You can use help at the DCL prompt to find the following:

- Topical help - access TCPware help topics by typing:

```
$ HELP TCPWARE [topic]
```

The topic entry is optional. You can also enter topics and subtopics at the following prompt and its subprompts:

```
TCPWARE Subtopic?
```

Online help is also available from within certain TCPware components: FTP-OpenVMS Client and Server, Network Control Utility (NETCU), TELNET-OpenVMS Client, NSLOOKUP, and TRACEROUTE. Use the HELP command from within each component.

Example:

```
NETCU>HELP [topic]
```

- Error messages help—Access help for TCPware error messages by typing:

```
$ HELP TCPWARE MESSAGES
```

If the error message is included in the MESSAGES help, it identifies the TCPware component and provides a meaning and user action. See the instructions under MESSAGES.

Obtaining Customer Support

You can use the following customer support services for information and help about TCPware and other Process Software products if you subscribe to our Product Support Services. (If you bought TCPware products through an authorized TCPware reseller, contact your reseller for technical support.) Contact Technical Support directly using the following methods:

Electronic Mail

E-mail relays your question to us quickly and allows us to respond as soon as we have information for you. Send e-mail to support@process.com. Be sure to include your:

- Name
- Telephone number
- Company name
- Process Software product name and version number
- Operating system name and version number
- Process Software support contract number

Describe the problem in as much detail as possible. You should receive an immediate automated response telling you that your call was logged.

Telephone

If calling within the continental United States or Canada, call Process Software Technical Support toll-free at (800) 394-8700. If calling from outside the continental United States or Canada, dial +1 (508) 628-5074. Please be ready to provide your name, company name, Process Software support contract number, and telephone number.

World Wide Web

There is a variety of useful technical information available on our World Wide Web home page, <http://www.process.com/>

License Information

TCPware for OpenVMS includes a software license that entitles you to install and use it on one machine. Please read and understand the *Software License Agreement* before installing the product. If you want to use TCPware on more than one machine, you need to purchase additional licenses. Contact Process Software or your distributor for details.

Maintenance Services

Process Software offers a variety of software maintenance and support services. Contact us or your distributor for details about these services.

Documentation Set

The documentation set for TCPware consists of the following:

- **Installation & Configuration Guide** - For system managers and those installing the software. The guide provides installation and configuration instructions for the TCPware products.
- **Management Guide** - For system managers. This guide contains information on functions not normally available to the general network end user. It also includes implementation notes and troubleshooting information.
- **Network Control Utility (NETCU) Command Reference** - For users and system managers. This reference covers all the commands available with the Network Control Utility (NETCU) and contains troubleshooting information.
- **Programmer's Guide** - For network application programmers. This guide gives application programmers information on the callable interfaces between TCPware and application programs.
- **Release Notes** for the current version of TCPware - For all users, system managers, and application programmers. The *Release Notes* are available online on your TCPware media and are accessible before or after software installation.
- **User's Guide** - For all users. This guide includes an introduction to TCPware products as well as a reference for the user functions arranged alphabetically by product, utility, or service.

Conventions Used

Convention	Meaning
host	Any computer system on the network. The local host is your computer. A remote host is any other computer.
monospaced type	System output or user input. User input is in reversed bold type. Example: Is this configuration correct? YES Monospaced type also indicates user input where the case of the entry should be preserved.

<i>italic type</i>	Variable value in commands and examples. For example, <i>username</i> indicates that you must substitute your actual username. Italic text also identifies documentation references.
[<i>directory</i>]	Directory name in an OpenVMS file specification. Include the brackets in the specification.
[<i>optional-text</i>]	(Italicized text and square brackets) Enclosed information is optional. Do not include the brackets when entering the information. Example: START/IP line address [info] This command indicates that the info parameter is optional.
{ value value }	Denotes that you should use only one of the given values. Do not include the braces or vertical bars when entering the value.
Note	Information that follows is particularly noteworthy.
Caution	Information that follows is critical in preventing a system interruption or security breach.
key	Press the specified key on your keyboard.
Ctrl+key	Press the control key and the other specified key simultaneously.
Return	Press the Return or Enter key on your keyboard.

1. Before You Begin

Introduction

This chapter introduces you to and prepares you for TCPware product installation, configuration, startup, and testing. It is for the OpenVMS system manager or technician responsible for product installation and configuration.

Steps to Get TCPware Up and Running

To get TCPware up and working, you must perform the following steps:

Step	Task	Instructions
1	Install the software (see the following section to prepare for installation).	See Chapter 2, <i>Installing TCPware</i>
2	Configure the TCP/IP core environment.	See Chapter 3, <i>Configuring the TCP/IP Core Environment</i>
3	Configure the individual TCP/IP components.	See Chapter 4, <i>Configuring the TCP/IP Services</i>
4	Start and test the software.	See Chapter 5, <i>Starting and Testing TCPware</i>

Prepare for Installation

TCPware installation involves using HPE's VMSINSTAL procedure. Preparing for installation involves:

- Understanding the hardware and software requirements
- Determining if you have sufficient disk space and global pages for the installation
- Determining where to install the software
- Deciding which TCPware products to install

Note: You must shut down all other TCP/IP products previously running on the system without executing any of the other products' startup files, and reboot the system.

Hardware Requirements

TCPware requires one or more of the following devices:

- HP Ethernet, FDDI, Token Ring (except DEQRA), LAN Emulation over Asynchronous Transfer Mode (ATM), or Classical IP over ATM controller
- IP-over-X.25 controller; all HP interfaces supported by VAX PSI (for VAX)
- HP controller for VAX WAN Device Drivers
- Network Systems HYPERchannel controller (for VAX)
- Proteon proNET-10/80 controller (VAX), or proNET-4/16 EISA NIC controller (Alpha)

Software Requirements

TCPware requires at least the following operating system versions:

- OpenVMS Alpha V6.1 and later
- OpenVMS VAX V5.5-2 and later
- OpenVMS Itanium V8.2 and later

Disk Space and Global Pages

The destination device for your TCPware software must have enough disk space so that you can run the software. The disk space requirements are documented in the TCPware Release notes.

You should also have at least 50,000 free global pages (GBLPAGES) on your system before installing TCPware 6.0. Use **SHOW GBLPAGES** in the SYSGEN utility to determine the parameter value and change it using **SET GBLPAGES** if necessary.

Insufficient GBLPAGES can abort the installation and leave your system command tables disconnected. The only way to recover is through a system reboot.

General Requirements

Check at this point that you:

- Have OPER, SYSPRV, or BYPASS privileges
- Can log in to the system manager's account
- Are the only user logged in (recommended)
- Backed up your system disk on a known, good, current, full backup (recommended)
- Need to reinstall TCPware after performing a major VMS upgrade
- If TCPware is currently running, shut it down. This is mandatory.

Where to Install TCPware

Install TCPware in a location depending on the following:

- Generally, on your system disk, but you can install TCPware anywhere, just answer the question when it appears. This is also where you would keep your "common" files. Node-specific files should always be on your system disk.
- If the machine is in a single node cluster, on a common disk.
- If the machine is in a mixed node cluster, once on the Alpha system disk (or disks), once on the VAX common system disk, and once on the Itanium common system disk.

Which TCPware Components to Install

Be careful to install only those components for which you have a license. If you install a product for which you do not have a license, it still consumes disk space, but you cannot use that product.

Release Notes and Online Documentation

The TCPware *Release Notes* provide important information on the current release. A PDF version of the documentation set is available on the TCPware CD-ROM; both PDF and HTML versions of the documentation are publicly available on the Process Software web site at www.process.com.

2. Installing TCPware

Introduction

This chapter takes you through the TCPware product installation procedure and certain post-installation tasks. It is for the OpenVMS system manager, administrator, or technician responsible for product installation.

To prepare for installation, see Chapter 1, *Before You Begin*.

Note: Once you have installed TCPware, you need to reinstall it after you have done a major VMS upgrade.

To install TCPware:

1. Load the software.
2. Run the `VMSINSTALL` procedure.
3. Install other products, if needed, and perform post-installation tasks.

Load the Software

There are three steps to loading the TCPware software:

1. Log in to the system manager's account.
2. If TCPware is currently running, shut it down:

```
$ @TCPWARE : SHUTNET
```

If you are installing on a VMScluster, shut down TCPware on each node in the cluster:

```
$ RUN SYS$SYSTEM:SYSMAN
SYSMAN>SET ENVIRONMENT/CLUSTER
SYSMAN>DO @TCPWARE : SHUTNET
SYSMAN>EXIT
```

3. Physically insert the TCPware CD-ROM into the appropriate device.
 - In a VMS cluster environment, if you want to access the media from more than one node, enter the following:

```
$ MOUNT/CLUSTER/SYSTEM device volume-label
```

- On a standalone system, or if you want to prevent multiple users from accessing the software, enter the following:

```
$ MOUNT device volume-label
```

Note: If you install TCPware on a VMS cluster that has a common system disk, install the software on only one node in the cluster. **If reinstalling or upgrading TCPware, first shut down TCPware on all nodes in the cluster.**

If you install TCPware on a mixed architecture cluster, make sure you have TCPware licenses for all of the architectures in the cluster and install TCPware once on each architecture.

Start VMSINSTAL

VMSINSTAL is OpenVMS's installation program for layered products. VMSINSTAL prompts you for any information it needs. Here are the first steps to follow:

Step	For this task...	Enter this response...
1	Make sure that you are logged in to the system manager's account, and invoke VMSINSTAL	@SYS\$UPDATE : VMSINSTAL
2	Specify the directory where you want the common files installed	Return if accepting default of SYS\$COMMON or

		The device and directory of your choice.
3	Specify the directory where you want the node specific files installed	Return if accepting default of SYS\$SPECIFIC or The device and directory of your choice.

Starting VMSINSTAL:

```

$ @SYS$UPDATE:VMSINSTAL TCPWARE061
      VAX/VMS Software Product Installation Procedure V7.3

It is 1-JUN-2023 at 07:50.

Enter a question mark (?) at any time for help.

The following products will be processed:

  TCPWARE V6.1

      Beginning installation of TCPWARE V6.1 at 07:50

%VMSINSTAL-I-RESTORE, Restoring product save set A ...
%VMSINSTAL-I-RELMOVED, Product's release notes have been moved to SYS$HELP.

TCPware(R) for OpenVMS Version 6.1-0

Copyright (c) by Process Software

Refer to the "Installing TCPware" chapter of the TCPware(R) for OpenVMS
Installation & Configuration Guide.

You can specify the directory where you want the TCPware common files
installed.  The default location for the TCPware common files is
SYS$COMMON.  A [.TCPWARE] subdirectory will be created in the
directory you specify.

* Where do you want to install the TCPware common files [SYS$COMMON]:

You can specify the directory where you want node specific files
installed.  This directory must not be used by any other nodes
in a cluster.  The default location is SYS$SPECIFIC:[TCPWARE].

```

A [.TCPWARE] subdirectory will be created in the directory you specify.

* Where do you want to install the TCPware node specific files [SYS\$SPECIFIC]:

TCPware 6.1-0 will be installed.

This concludes the question and answer portion of the installation.

Your system will now be updated to include TCPware for OpenVMS. This will take a short while.

For a complete sample installation, see *Appendix A, Sample Installation*.

Installing TCPware on Multiple System Disks

Because TCPware creates files in some of the system directories like SYS\$LIBRARY and SYS\$SYSTEM, you need to install TCPware on each system disk. Because nodes of the same architecture can share the TCPware common files, be sure to specify a common directory when the installation instructions ask where to install the TCPware common files.

Installing TCPware on Mixed Platform Clusters

In a mixed platform cluster of VAX, Alpha and Itanium systems, the cluster needs to be set up to share the data files. You can do this by having separate TCPWARE_LOGICALS.COM files for the VAX, Alpha and Itanium nodes.

On the VAX nodes, the TCPWARE_LOGICALS.COM file looks something like this:

```
$ DEFINE/SYSTEM/NOLOG/EXEC TCPWARE_COMMON SYS$COMMON:, -  
ALPHA$DKA300:[VMS$COMMON.]  
$ DEFINE/SYSTEM/NOLOG/EXEC TCPWARE_SPECIFIC SYS$SPECIFIC:  
$ DEFINE/SYSTEM/NOLOG/EXEC TCPWARE_ROOT SYS$SYSROOT:, -  
ALPHA$DKA300:[VMS$COMMON.]  
$ DEFINE/SYSTEM/NOLOG/EXEC TCPWARE "TCPWARE_ROOT:[TCPWARE]"  
$ DEFINE/SYSTEM/NOLOG TCPWARE_INCLUDE -  
"TCPWARE_ROOT:[TCPWARE.INCLUDE]"
```

On the Alpha nodes, the TCPWARE_LOGICALS.COM file looks something like this (being the “primary”):

```
$ DEFINE/SYSTEM/NOLOG/EXEC TCPWARE_COMMON SYS$COMMON:
$ DEFINE/SYSTEM/NOLOG/EXEC TCPWARE_SPECIFIC SYS$SPECIFIC:
$ DEFINE/SYSTEM/NOLOG/EXEC TCPWARE_ROOT SYS$SYSROOT:
$ DEFINE/SYSTEM/NOLOG/EXEC TCPWARE "TCPWARE_ROOT:[TCPWARE]"
$ DEFINE/SYSTEM/NOLOG TCPWARE_INCLUDE -
"TCPWARE_ROOT:[TCPWARE.INCLUDE]"
```

On the Itanium nodes, the TCPWARE_LOGICALS.COM file looks something like:

```
$ DEFINE/SYSTEM/NOLOG/EXEC TCPWARE_COMMON SYS$COMMON:, -
ALPHA$DKA300:[VMS$COMMON.]
$ DEFINE/SYSTEM/NOLOG/EXEC TCPWARE_SPECIFIC SYS$SPECIFIC:
$ DEFINE/SYSTEM/NOLOG/EXEC TCPWARE_ROOT SYS$SYSROOT:, -
ALPHA$DKA300:[VMS$COMMON.]
$ DEFINE/SYSTEM/NOLOG/EXEC TCPWARE "TCPWARE_ROOT:[TCPWARE]"
$ DEFINE/SYSTEM/NOLOG TCPWARE_INCLUDE -
"TCPWARE_ROOT:[TCPWARE.INCLUDE]"
```

The common files reside on ALPHA\$DKA300:[VMS\$COMMON.TCPWARE...], the Alpha system disk.

Keep in mind:

- Before you install a new version of TCPware, "restore" the logicals to their original values. Upon startup, TCPware checks for the logicals TCP, UDP, IP, INET, RMT, RCD, BG, and QX. If any of these logicals have been previously defined on your system, the following warning is generated:

```
%TCPWARE-W-BADLOGICAL
```

- After installing TCPware on VAX and Itanium systems, make sure to delete (or rename) the SYS\$SYSROOT:[TCPWARE...]*_CONTROL.COM files. Otherwise, TCPware fails to start because it finds two sets of the control files and tries to execute each set, which can cause problems.
- After installing on VAX and Itanium systems, delete any of the data files TCPware creates during installation and which it can no longer locate because of the new logical definitions.
- For the VAX and Itanium systems, restore the TCPWARE_LOGICALS.COM file to that shown above.

Installing Other Products

You can install other products at the same time you install TCPware.

INGRES/Net

Install and start TCPware before you install INGRES/Net.

After TCPware installation, configuration, and startup, see Chapter 6, *Starting and Testing TCPware*, the *Installing and Configuring INGRES/Net* section.

Oracle's SQL*Net

Install and operate TCPware before installing SQL*Net.

After TCPware installation, configuration, and startup, see Chapter 6, *Starting and Testing TCPware*, the *Installing and Configuring Oracle's SQL*Net* section.

Post-Installation Tasks

If you are reinstalling or upgrading TCPware or the OpenVMS operating system, there are some additional tasks to perform. Perform these tasks after you get confirmation of a successful installation:

1. Unload the distribution media from the device.
2. Reboot the system.

Caution! Do not use the `STOP PROCESS/ID` command to stop TCPware or any of its components. Use the `SHUTNET` command as described in Chapter 5.

Note: Be aware that TCPware provides new versions of the existing `TCPWARE:NETWORKS.`, `TCPWARE:SERVICES.`, and `TCPWARE:PROTOCOLS.` files. Any customizations that you made to these files should be merged with the new versions.

3. Configuring the TCP/IP Core Environment

Introduction

This chapter describes the steps you need to take before using CNFNET to configure TCPware's core environment. This chapter is for the OpenVMS system manager or operator responsible for the TCP/IP core environment configuration.

This chapter covers the TCP/IP core configuration only. You later configure the individual TCPware components in Chapter 4, *Configuring the TCP/IP Services*.

Pre-Configuration Steps

Before you run CNFNET, there are certain things you need to do first:

1. Define the file location logicals.
2. Obtain Internet addresses for your network devices.

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

CNFNET Procedure

You run the CNFNET.COM procedure file to configure the TCPware core environment and the TCPware components. You can access CNFNET using either of two options. Each option provides different configuration choices.

Define the File Location Logicals

TCPware file definitions include a number of logicals. You can define these logicals using the `SYS$SYSROOT:[TCPWARE]TCPWARE_LOGICALS.COM` command file. The VMSINSTALL procedure (from the previous chapter) generates this command file.

Note: Execute `TCPWARE_LOGICALS.COM` before performing any other TCPware procedure.

The below table shows the TCPware logicals and how they relate to OpenVMS system logicals. The system logical equivalents apply only if the TCPware installation is on the default locations on the system disk.

This logical...	Has this system logical equivalent...
<code>TCPWARE_ROOT:</code>	<code>SYS\$SYSROOT:</code>
<code>TCPWARE:</code>	<code>SYS\$SYSROOT:[TCPWARE]</code>
<code>TCPWARE_INCLUDE:</code>	<code>SYS\$SYSROOT:[TCPWARE.INCLUDE]</code>
<code>TCPWARE_SPECIFIC:</code>	<code>SYS\$SPECIFIC:</code>
<code>TCPWARE_COMMON:</code>	<code>SYS\$COMMON:</code>

You can also set customized filenames and locations for TCPware component files by using a customized logicals command file. This can help prevent duplicate databases in mixed architecture systems. TCPware provides a `CUSTOM_LOGICALS.TEMPLATE` file containing logicals (such as `TCPWARE_NFS_PROXY_DB`) you can redefine from their given defaults. Rename this file to `CUSTOM_LOGICALS.COM` to put the new file locations into effect on a system-wide basis.

Configuration Methods

Depending on how you want to configure the TCPware core environment and the TCPware components, you can choose either a command-driven method or a menu-driven method. Using either method, you can perform a basic, full, or component configuration.

However, if you are configuring TCPware for the first time, you need to configure the core environment first.

- The basic configuration allows you to configure the core environment and some of the basic component settings.

- The full configuration allows you to configure the core environment and the full set of components.
- The component configuration allows you to specify a component to configure. Use this if you are not configuring TCPware for the first time and you need to configure certain service components only.

The CNFNET .COM procedure creates the configuration data file,
 TCPWARE_SPECIFIC:[TCPWARE]TCPWARE_CONFIGURE.COM.

Command-driven Method

To use the command-driven method, enter the CNFNET command followed by the option choice you want:

```
$ @TCPWARE:CNFNET option
```

Your option choices and description are listed in the table below:

Use this option...	If you want to...
TCPWARE or TCP or (no option)	Configure core environment plus TCPware component defaults
BASIC	Configure core environment plus basic TCPware components
PRODUCT	To do a full configuration on a specific product or component (product can be ALL).
FULL	Configure core environment plus full TCPware components
@TCPWARE:CNFNET TCP	Change the IP address without reinstalling TCPware. Change a subnet mask. (You must wait for the prompt.)

Menu-driven Method

The menu-driven method provides configuration options as convenient menu selections. Your selection choices are shown in the above table. The menus that appear as you make your choices move from one

function to the next, and you can back up and make corrections as you go. You can use the menus to configure the TCPware core environment specifically.

To describe the configuration process for the core environment, this chapter uses the menu-driven method.

Start the Configuration Process

These are the steps to the TCP/IP core environment configuration:

1. Start CNFNET.
2. Enter your Maintenance Agreement Number.
3. Enter line identification codes for the network devices.
4. Enter host addresses for the network devices.
5. Enter the default gateway host address.
6. Enter the local time zone.
7. Enter the local hostname or update the HOSTS . file.

Start CNFNET

To start CNFNET using the menu-driven method:

1. At the DCL prompt, enter:

```
$ @TCPWARE:CNFNET MENU
```

2. Press **Return** at the prompt:

Type <return> to continue...

The menu with configuration options appears:

```
TCPware(R) for OpenVMS Configuration Menu
Configuration Options:
 1 - Configure TCPware Services

 2 - Startup/Restart all TCPware Services
 3 - Shutdown all TCPware Services

 L - Display the software licensing information (PASSWORD)
 E - Exit the configuration procedure (changes will be saved)
```

Enter configuration option: **1 Return**

3. Enter **1** at the prompt. CNFNET displays the TCPware Services Configuration Menu.

```
TCPware Services Configuration Menu
Configuration Options:
  1 - Core environment for TCP/IP services
  2 - Configure all TCP/IP components
  3 - Configure a specific TCP/IP component

  4 - Startup/Restart TCP/IP services
  5 - Shutdown TCP/IP services
  6 - Startup/Restart a specific TCP/IP component
  7 - Shutdown a specific TCP/IP component

  E - Exit to previous menu
Enter configuration option: 1 Return
```

4. Enter **1** (Core environment for TCP/IP services) at the prompt. CNFNET displays the message and prompt:

```
Configuring the core TCP/IP environment...
Enter your Maintenance Agreement (MAS) number []:
```

Enter Your Maintenance Agreement Number

If you have a maintenance agreement with Process Software, you can find your "Master Agreement No." (MAS) on your *Software Maintenance and Support Acknowledgment* form. The MAS number helps in future communications with Process Software.

Note: If you decided to start the configuration using either the `@TCPWARE:CNFNET TCPWARE` or `@TCPWARE:CNFNET TCP` command, a different screen appears. It contains a message that CNFNET creates the `TCPWARE_SPECIFIC:[TCPWARE]TCPWARE_CONFIGURE.COM` file to reflect your configuration. Press **Return** to continue and the MAS number request prompt appears. CNFNET purges up to the last five versions of the `TCPWARE_CONFIGURE.COM` file. **You are strongly advised not to edit this file directly.**

Entering your Maintenance Agreement Number:

This procedure creates the configuration data file, TCPWARE_SPECIFIC:[TCPWARE]TCPWARE_CONFIGURE.COM, to reflect your system's configuration.

Please enter your Process Software Maintenance Agreement (MAS) number if you have one and have it available. This number can be found on the top of your Software Maintenance and Support Acknowledgment form.

If you do not have this number, press <RETURN> at the prompt. If you would like to enter this information later, you can set it using the command:

```
$ @TCPWARE:CNFNET MAS
```

Enter your Maintenance Agreement (MAS) number []: **M123456** **Return**

Enter the MAS number now, or later using the @TCPWARE:CNFNET MAS command. Once entered, this number appears when you use the NETCU SHOW VERSION /ALL command.

CNFNET prompts you for the necessary information during the rest of the procedure. Default answers, if available, are provided in square brackets as part of some prompts, based on information extracted from your environment. If you want to accept the default, press **Return**. If not, enter the value or information you need and then press **Return**.

Enter Line Identification Codes

You now need to define the network devices and information for each device. Entering line identification codes is the first step.

CNFNET displays the text and prompt:

You need to enter the line identifications for the available network devices. The following is a partial list of the network devices that are supported:

```
Line Id      Network Device
```

```
-----
```

```
QNA-n      for Digital's DELQA, DESQA, or DEQNA (XQDRIVER)
UNA-n      for Digital's DELUA or DEUNA (XEDRIVER)
BNA-n      for Digital's DEBNI, DEBNA, or DEBNT (ETDRIVER)
SVA-n      for Digital's DESVA (ESDRIVER)
MNA-n      for Digital's DEMNA (EXDRIVER)
ISA-n      for Digital's VAX 4000 (EZDRIVER)
MFA-n      for Digital's DEMFA FDDIcontroller 400 (FXDRIVER)
FZA-n      for Digital's DEFZA FDDIcontroller 700 (FCDRIVER)
PRO-n      for Proteon's proNET (PNDRIVER)
HYP-n      for NSC's HYPERchannel (NxDRIVER)
SLIP-n     for (static) Serial Line IP (any terminal device)
DECNET-n   for IP over DECnet (requires DECnet)
```

DSB-n for Digital's DSB32 (SLDRIVER)
 DST-n for Digital's DST32 (ZSDRIVER)
 DSV-n for Digital's DSV11 (SJDRIVER)
 X25-n for VAX P.S.I. (IP over X.25)
 LPB-0 for local loopback (no device driver)
 EIA-0 for HP's i82558 10/100 Ethernet interface
 EWA-0 for HP's DEGXA gigabit interface

Unless your system has more than one controller, n is 0.

Enter the line identifications [LPB-0,SVA-0]: **Return**

For a full list of supported network devices, see the below table:

This controller...	Has line ID...	For device driver
Classical IP over ATM	CLIP- <i>n</i>	CLDRIVER
PMAD Communications Link	MXE- <i>n</i>	ECDRIVER
LAN Emulation Driver ²	ELA- <i>n</i>	ELDRIVER
EISA Bus Adapter (DE422/425) ²	ERA- <i>n</i>	ERDRIVER
DESVA VAXstation 2000/3100/4000	SVA- <i>n</i>	ESDRIVER
DEBNA/DEBNI/DEBNT VAXBI Ethernet ¹	BNA- <i>n</i>	ETDRIVER
PCI Bus Adapter (TULIP) ²	EWA- <i>n</i>	EWDRIVER
DEMNA XMI Ethernet	MNA- <i>n</i>	EXDRIVER
VAX 4000 Ethernet (SGEC ¹ , TGEC ²)	ISA- <i>n</i>	EZDRIVER
DE600-AA, DE602-AA (NC3123, NC3131) ²	EIA- <i>n</i>	EIDRIVER
DEFAA FDDIcontroller	FAA- <i>n</i>	FADRIVER
DEFTA/DEFZA FDDIcontroller	FZA- <i>n</i>	FCDRIVER
DEFQA FDDIcontroller ¹	FQA- <i>n</i>	FQDRIVER
DEFEA FDDIcontroller ²	FEA- <i>n</i>	FRDRIVER
DEFPA FDDIcontroller	FPA- <i>n</i>	FWDRIVER
DEMFA FDDIcontroller	MFA- <i>n</i>	FXDRIVER

DETRA TRNcontroller 700 ²	TRA- <i>n</i>	ICDRIVER
DEGXA gigabit controller ³	EWA- <i>n</i>	EW5700
i82558 10/100 Ethernet controller ³	EIA- <i>n</i>	EIDRIVER
Proteon PROnet-4/16 EISA NIC (DW300) ²	TRE- <i>n</i>	IRDRIVER
HYPERchannel H269	HYP- <i>n</i>	N _x DRIVER ⁴
Proteon proNET-10/80	PRO- <i>n</i>	PNDRIVER ⁴
HP WAN DSV11	DSV- <i>n</i>	SJDRIVER ⁴
HP WAN DSB32	DSB- <i>n</i>	SLDRIVER ⁴
DELUA/DEUNA UNIBUS Ethernet ¹	UNA- <i>n</i>	XEDRIVER
DELQA/DEQNA/DEQTA/DESQA Q-BUS Ethernet ¹	QNA- <i>n</i>	XQDRIVER
HP WAN DST32	DST- <i>n</i>	ZSDRIVER ⁴
IP-over-DECnet	DECNET- <i>n</i>	DECnet
Serial lines	SLIP- <i>n</i>	various
IP-over-X.25	X25-0	VAX P.S.I.
Local loopback	LPB-0	

¹VAX-specific

²Alpha-specific

³Itanium-specific

⁴PNDRIVER, N_xDRIVER, SJDRIVER, SLDRIVER, and ZSDRIVER are not provided as part of OpenVMS. Purchase the proNET driver directly from Proteon, Inc. The HYPERchannel drivers include NADRIVER for Q-BUS and UNIBUS, NBDRIVER for MASSBUS, and NCDRIVER for VAXBI; you must purchase the H269 drivers directly from Network Systems Corporation. Purchase the HP WAN drivers directly from HPE.

Line Identification Codes

The network device line identification (line ID) consists of a line name and controller number combination, such as QNA-0 or UNA-1.

1. Find each network device over which you plan to run TCPware on your system and note its line ID.
2. Enter the line ID or IDs at the following prompt:

```
Enter the line identifications [default-lines]:
```

The system displays any default line IDs that exist on your system in the square brackets. Press **Return** to accept them or add additional devices. You can enter up to sixteen devices, separated by commas.

Always enter the local loopback device (LPB-0) first. This is a pseudo-device not associated with any physical device. TCPware uses the loopback device only if no other hosts are connected to the network. TCPware always configures the LPB-0 device unless you specify not to do so.

For example, to support the DELQA controller (QNA) and a HYPERchannel (HYP) device, enter:

```
LPB-0 , QNA-0 , HYP-0
```

Note: If your system runs Oracle software with TCPware as the transport, make sure that you configure the **LPB-*n*** device. Otherwise, Oracle sends a message stating that it cannot connect. Note that you must have TCPware fully installed and operating before you can install Oracle's SQL*Net.

HYPERchannel Lines

If you are configuring HYPERchannel devices, respond to the prompt:

```
What is the local HYPERchannel address for line...:
```

The format of the 32-bit HYPERchannel address combination is *aa-bb-cc-dd*.

For each HYPERchannel device selected, also enter the Address Resolution Protocol (ARP) server's HYPERchannel address for line *HYP-*n** at the prompt:

```
What is the ARP server's HYPERchannel address?
```

You can enter **NONE** or press **Return** at the prompt if there is no ARP server address.

See the *Management Guide*, Chapter 1, *Common Interfaces*, the *HYPERchannel* section for further information. Also see the *NETCU Command Reference*, Chapter 2, *NETCU Commands*, the `ADD ARP` command for populating ARP tables.

IP-over-DECnet Lines

If you are configuring IP-over-DECnet devices, use the following format at the prompt:

```
What is the DECnet link information: node-name::"TASK=object-name"
```

If you enter **N** at the prompt:

```
Is this the LISTENER end of the DECnet link?
```

TCPware assumes that you are issuing commands for the master node. See the *Management Guide*, Chapter 1, *Common Interfaces*, the *IP-over-DECnet* section for further information.

IP-over-X.25 Devices

CAUTION! HPE no longer supports the VAX PSI product. Process Software can provide no support for this feature, which is provided as-is.

Oracle Software

If your system will be running Oracle software with TCPware as the transport, make sure that you configure the `LPB-n` device. Otherwise, Oracle sends a message stating that it cannot connect. Note that you must have TCPware fully installed and operating before you can install Oracle's SQL*Net.

Serial Line IP (SLIP) Devices

If you are configuring Serial Line IP (SLIP) devices, you can use any valid OpenVMS terminal device as a SLIP line. Unlike other line ID controller numbers, the one for SLIP lines is not related to the actual device name. To configure SLIP devices, respond to the prompt with:

```
What is the device name for line...:
```

You can also create the `TCPWARE:SLIP_SETUP.COM` file. The network startup command procedure executes this command procedure, if it exists, before starting the SLIP lines. `SLIP_SETUP.COM`

should contain the commands necessary to configure the terminal devices for proper operation. Typically, it would include `SET TERMINAL` commands to set the baud rate and other terminal characteristics.

See the *Management Guide*, Chapter 1, *Common Interfaces*, the *Serial Line IP (SLIP) Interface* section for further information. See Chapter 6 in the *Installation and Configuration Guide*, the *System Parameters* section.

Wide Area Network (WAN) Device Drivers

If you are configuring HP WAN device drivers, the configuration options include the protocol, type of duplex mode, clocking method, type of CRC, line speed, number of receive buffers, and retransmission time to use. To configure HP WAN devices, respond to the prompt:

```
What are the configuration options for line...:
```

See the *Management Guide*, Chapter 1, *Common Interfaces*, the *HP Wide Area Network (WAN) Device Drivers* section for further information.

Enter Network Device Addresses

The next step in defining your network devices is to enter the local host internet address, hostname, and host subnet mask for each device (see the example later in this section):

1. Enter each network device's local host internet address.
 - The local loopback device (LPB-0) automatically gets an internet address of 127.0.0.1.
 - Each network device connects the host to a different network. The host must have a unique internet address on each connected network.
 - For most lines, the internet address is not related to the physical address. For some interfaces, the Address Resolution Protocol (ARP) resolves the mapping between internet and physical addresses.
2. Enter each network device's local hostname. (You may have to enter the fully qualified domain name.)
 - If you are using Domain Name Services to resolve hostnames, enter the fully qualified domain name (including the machine name) of the local host. If not using the Domain Name Services, enter just the machine name as it appears in the local `TCPWARE:HOSTS` file.
 - Enter the host name only once. Its case is preserved.
 - You do not need to enter a name for each network. Indicate only the "primary" network.
3. Enter each network device's local host subnet mask (if it exists). See the "Internet address classes" table below for details.

- If a device is on a subnet, you should assign a subnet mask. This mask "extends" the network portion of the address to cover part of the host portion to divide the latter into subnets. For example, host 192.168.4.56 is on a subnet of network 192.168.0.0 encompassing addresses 192.168.4.1 through 192.168.7.254 (comprising 1022 hosts). The mask to use would be 255.255.252.0.
 - The subnet mask must include at least the network mask.
 - Do not use a subnet mask with an unnumbered interface. See the next section for details.
4. Respond to the prompt asking if you want trailer packet (default=NO) and Reverse ARP (RARP) support (default=YES) for the configured network line. This does not apply to VMS Communications Interface (VCI) support.

For details on RARP and trailer packets, see the *Management Guide*, Chapter 1, *Common Interfaces*, the appropriate subsections under the *Ethernet, FDDI, Token Ring, and ATM Interfaces* section.

5. Indicate whether the configuration is correct. If the answer is N, start the network device configuration process over again

Internet address classes:

Address Class	First Byte Range	Network Mask
Class A	1. - 127.	255.0.0.0
Class B	128. - 191.	255.255.0.0
Class C	192. - 223.	255.255.255.0
Class D	224. - 239.	None

Example of entering host address information:

You need to supply the following information for each network:

- The internet address for this host
- The host name for the local internet address
- The subnet mask for the network
- The line specific information (depends on line)

If a network is not subnetted, press return at the subnet mask prompt. Otherwise, enter the subnet mask for the network as an internet address. These are the default subnet masks for each network class:

Network Class	Default Subnet Mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Using LOOPBACK (127.0.0.1) as host name for line LPB-0.

What is the local host's INTERNET ADDRESS for line SVA-0: **198.168.1.56**

Return

What is the HOST NAME for line SVA-0: **MAIL.EXAMPLE.COM** **Return**

What is the SUBNET MASK for line SVA-0 [255.255.255.0]: **Return**

Do you want to enable TRAILER packet support for line SVA-0 [NO]: **Return**

Do you want to enable RARP (Reverse ARP) support for line SVA-0 [YES]:

Return

The network devices are configured as follows:

Line	Address	Name	Options
LPB-0	127.0.0.1	LOOPBACK	
SVA-0	198.168.1.56	MAIL.EXAMPLE.COM	/FLAGS=(NOTRAILERS)

Is this configuration correct [YES]: **Return**

Define the Default Gateway

The next step is to define the internet address of your default gateway (see the below example).

Enter the internet address of the default gateway, if the network or networks connected to your host connect to other networks, for example.

The address must be on a network to which your host is directly connected. If the network has more than one gateway, enter the gateway that is "closest" to the networks with which you will communicate most frequently.

If you want to remove a previously assigned default gateway, or if your network does not have a gateway, enter 0.0.0.0 as the default gateway internet address.

If your network is connected to other networks, you need to enter the internet address of a default gateway. If your network has more than one gateway, enter the gateway "closest" to the networks that you will be connecting to most frequently. The (sub)network portion of the internet address for the gateway MUST match that of a locally connected (sub)network.

Enter 0.0.0.0 if you need to remove a previously defined default gateway or your network does not have any gateways.

Your routing requirements might be more complex if your network has several gateways. Handle this by adding the appropriate NETCU commands (such as ADD ROUTE) to the TCPWARE_COMMON:[TCPWARE]ROUTING.COM command procedure.

For more information on routing, refer to the TCPware(R) for OpenVMS documentation.

Enter the internet address of the default gateway [0.0.0.0]: **Return**

Daylight Savings Time Support

Support for automatic Daylight Savings Time (DST) changes has now been added to the existing method of specifying time zone information. You can configure time zone and DST information, which can be used by the Network Time Protocol (NTP) to change the system clock and the time offset information automatically.

To understand time zone configuration, time zone offset, and the hardware clock in relation to choosing the time zone settings you need, please read the following sections.

Time Zone Configuration and Hardware Clock Overview

By convention, the hardware clock is usually set to the local time, but network protocols represent time in Greenwich Mean Time (GMT), also known as Universal Coordinated Time (UTC).

To convert between local time and GMT, TCPware uses built-in rules or rules provided by the system manager. Each country or geographical area has its own names for time zones and its own rules for Daylight Savings Time (DST). The names for these time zones and rules are not necessarily unique; for example, “EST” could refer to the United States Eastern Standard Time, the Canadian Eastern Standard Time (which uses different DST rules), or the Australian Eastern Standard Time (which is a different offset from GMT as well).

TCPware uses the name of the local time zone specified by a system manager to calculate the offset between the local time and GMT, so it is important that an appropriate set of time zone rules be selected for your area.

TCPware assumes that the hardware clock is always set exactly to local time. For a smooth transition to and from Daylight Savings Time (DST), the hardware clock must be reset at the appropriate time. If NTP is used to synchronize the clock to a time server, NTP adjusts the clock automatically when the Daylight Savings Time transition occurs. Note that using a military time zone or an explicit GMT offset disables automatic Daylight Savings Time transitions.

TCPware Time Zone Support

It is not possible to consider every country or area in which TCPware might be used, and because the Daylight Savings Time rules are subject to change by local governmental action, you can write your own site-specific time zone rules.

Time zone rules are either compiled-in or defined in the time zone rule definition file and converted by the time zone rule logical at startup, or by entering a specific NETCU command (`DEFINE TIMEZONE`).

- Compiled-in rules are geographically centered on the United States but also include foreign time zones having names that do not conflict with the U.S. time zones.
- User-defined rules are specified by using the NETCU command `DEFINE TIMEZONE`. Use the NETCU command to override the compiled-in rules.

TCPware includes a database of the most common loadable rules; you can select these rules as is, or modify them to conform to the correct local time zone rules.

When TCPware searches the time zone rules looking for a zone, it first searches the loaded rules in the order they are selected, and then searches the compiled-in rules.

In addition to the standard one-letter U.S. military time zones and time zones of the form `GMT+hh:mm` or `GMT-hh:mm`, there are compiled-in time zone rules supported by TCPware, which are shown in the table in the next section.

Compiled-In Time Zone Rules

When a time zone is compiled-in, the logical `TCPWARE_ TIMEZONE_ NAME` specifies which rule is to be compiled in; for example, `EST`. The compiled-in time zone rules are listed in the following table.

Time Zone Name	GMT Offset (hours)	DST Rules	Area or Country
EST or EDT	-5	U.S. Federal	Eastern United States
CST or CDT	-6	U.S. Federal	Central United States
MST or MDT	-7	U.S. Federal	Mountain United States
PST or PDT	-8	U.S. Federal	Pacific United States
YST or YDT	-9	U.S. Federal	Yukon

HST	-10	none	Hawaii
NST or NDT	-3:30	Canadian	Canadian Newfoundland
AST or ADT	-4	Canadian	Canadian Atlantic
JST	+9	none	Japan
SST	+8	none	Singapore
GMT	+0	none	Greenwich Mean Time
GMT or BST	+0	British	Britain
WET or WET-DST	0	European	Western Europe
MET or MET-DST	+1	European	Middle Europe
CET or CET-DST	+1	European	Central Europe (Middle Europe)
EET or EET-DST	+2	European	Eastern Europe
NZST or NZDT	+12	New Zealand	New Zealand

User-Defined Time Zone Rules

Loadable time zone rules provided with TCPware are in the text file `TCPWARE:TIMEZONES.DAT`. You can add user-written time zone rules to the file `TCPWARE:TIMEZONES.LOCAL` to override the zones in `TIMEZONES.DAT`. The user-defined time zone rule format has three parts:

- `COUNTRY` is a collection of time zones (`ZONES`); for example, the country `US` selects all U.S. time zones. This provides a convenient way to select groups of time zones.
- `ZONE` is a specification of a particular time zone, including the name of the zone, the GMT offset, the DST rules in effect, and the name to use while DST is in effect.
- `RULE` is a rule for determining when DST is in effect.

Format of COUNTRY Specification

COUNTRY *countryname zonename [zonename . . .]*

The COUNTRY specification gives the name of the geographical area and the names of the time zones associated with it. This provides a way to group time zones so they can be selected more conveniently.

The following example shows the definition of the country “US” listing the zones corresponding to the United States.

```
Country US  US/Eastern US/Central US/Mountain US/Pacific US/Yukon
           US/Arizona
```

Format of ZONE Specification

ZONE *zonename gmtoffset rulename standard-name dst-name [COMPILED_IN]*

In the ZONE specification format:

- *zonename* is the name by which this zone can be selected, or the name by which it is referred to in a COUNTRY specification.
- *gmtoffset* is this zone's standard time offset from GMT.
- *rulename* is the name of the RULE specification that determines when DST is in effect for this zone. The *rulename* may be an underscore (`_`) to indicate that this zone does not use DST.
- *standard-name* and *dst-name* are the names by which this zone is referred to during standard time, and during Daylight Savings Time, respectively. These are the names by which `DEFINE TIMEZONE` selects the local time zone.

If there are no DST rules, the *dst-name* should be specified as an underscore (`_`). The optional `COMPILED_IN` keyword indicates that this rule is compiled-in and need not be loaded, as long as no other rules conflict with it. If you edit a `COMPILED_IN` ZONE specification, you must remove the `COMPILED-IN` keyword to force the ZONE specification to be loaded.

The first of the following examples shows the definition of the normal United States Mountain time zone. The second example, for Arizona, shows the definition of a Mountain time zone that does not observe Daylight Savings Time.

```
Zone  US/Mountain  -7:00  US  MST  MDT  COMPILED_IN
Zone  US/Arizona   -7:00  _   MST
```

Format of RULE Specification

RULE *rulename startyear ruletype save start-date end-date*

The RULE specification describes a set of rules for determining the times DST is in effect:

- *rulename* is the name of the RULE specification in ZONE specifications.
- *startyear* is the year during which this DST rule takes effect. The rule remains in effect until a later *startyear* is specified in a rule with the name *rulename*.
- *ruletype* specifies the type of DST rules. There are three permitted values:
 - DST indicates normal Northern Hemisphere Daylight Savings Time rules, which change at the time and date indicated.
 - REV_DST indicates normal Southern Hemisphere Daylight Savings Time rules.
 - NULL indicates that no Daylight Savings Time is in effect during the specified years.
 - save indicates the difference between Standard Time and DST.
- START DATE
- END DATE

The following example illustrates the United States Federal Daylight Savings Time rules:

```
Rule US 2007 DST 1:00 Sunday >= 8 March 2:00 First Sunday November 2:00
Rule US 1987 DST 1:00 First Sunday April 2:00 Last Sunday October 2:00
Rule US 1976 DST 1:00 Last Sunday April 2:00 Last Sunday October 2:00
Rule US 1975 DST 1:00 23 February 2:00 Last Sunday October 2:00
Rule US 1974 DST 1:00 6 January 2:00 Last Sunday October 2:00
Rule US 1970 DST 1:00 Last Sunday April 2:00 Last Sunday October 2:00
```

Loadable Time Zone Rules Provided with TCPware

The below table shows the loadable rules provided in the TCPWARE:TIMEZONES.DAT file; you may modify or augment as appropriate for your location.

Country Name	Rule Name	Time Zone Name	GMT Offset (hours)
	GMT	GMT	0
	UT	UT*	0
US-Military	US-Military/Z ¹	Z	0
US-Military	US-Military/A ¹	A	-1
US-Military	US-Military/B ¹	B	-2
US-Military	US-Military/C ¹	C	-3

US-Military	US-Military/D ¹	D	-4
US-Military	US-Military/E ¹	E	-5
US-Military	US-Military/F ¹	F	-6
US-Military	US-Military/G ¹	G	-7
US-Military	US-Military/H ¹	H	-8
US-Military	US-Military/I ¹	I	-9
US-Military	US-Military/K ¹	K	-10
US-Military	US-Military/L ¹	L	-11
US-Military	US-Military/M ¹	M	-12
US-Military	US-Military/N ¹	N	10
US-Military	US-Military/O ¹	O	2
US-Military	US-Military/P ¹	P	3
US-Military	US-Military/Q ¹	Q	4
US-Military	US-Military/R ¹	R	5
US-Military	US-Military/S ¹	S	6
US-Military	US-Military/T ¹	T	7
US-Military	US-Military/U ¹	U	8
US-Military	US-Military/V ¹	V	9
US-Military	US-Military/W ¹	W	10

US-Military	US-Military/X ¹	X	11
US-Military	US-Military/Y ¹	Y	12
US	US/Eastern ¹	EST/EDT	-5
US	US/Central ¹	CST/CDT	-6
US	US/Mountain ¹	MST/MDT	-7
US	US/Pacific ¹	PST/PDT	-8
US	US/Yukon ¹	YST/YDT	-9
US	US/Hawaii ¹	HST	-10
US/East-Indiana	US/East-Indiana ¹	EST	-5
US/Arizona	US/Arizona ¹	MST	-7
Canada	Canada/Newfoundland ¹	NST/NDT	-3:30
Canada	Canada/Atlantic ¹	AST/ADT	-4
Canada	Canada/Eastern	EST/EDT	-5
Canada	Canada/Central	CST/CDT	-6
Canada	Canada/Mountain	MST/MDT	-7
Canada	Canada/Pacific	PST/PDT	-8
Canada	Canada/Yukon	YST/YDT	-9
Canada	Canada/Saskatchewan	CST	-6
Israel	Israel	IST/IDT	+2

Australia	Australia/Tasmania	EST/EST	10
Australia	Australia/Queensland	EST	10
Australia	Australia/North	CST	9:30
Australia	Australia/West	WST	8:00
Australia	Australia/South	CST	9:30
Australia	Australia/Victoria	EST/EST	10
Australia	Australia/NSW	EST/EST	10
Australia	Australia/Yancowinna	CST/CST	9:30
Europe	Britain	GMT/BST	0
Europe	Europe/Western ¹	WET/WET-DST	0
Europe	Europe/Middle ¹	MET/MET-DST	1
Europe	Europe/Central ¹	CET/CET-DST	1
Europe	Europe/Eastern ¹	EET/EET-DST	2
	Poland	MET/MET-DST	2
	Turkey	EET/EET-DST	3
Japan	Japan ¹	JST	+9
Singapore	Singapore ¹	SST	+8
New Zealand	New Zealand ¹	NZST/NZDT	+12

¹This time zone is compiled in.

Define the Local Time Zone

The next step is to define your local time zone information.

Using CNFNET, you need to specify your local time zone information as it relates to the offset from Universal time. You can choose to either:

- Specify a time zone offset or name as a fixed value that you must set manually for each Daylight Savings Time change. This is the existing method.
- Choose to have the Network Time Protocol (NTP) server change the system clock and time offset automatically according to information you provide. This is a new feature and has been added to the configuration prompts.

If you enter an unknown time zone name, the system prompts you for the Universal time offset for the time zone.

For the offset from Universal time, enter `+hhmm` or `-hhmm`, the number of hours (*hh*) and minutes (*mm*) offset from Universal time; + is for east and - is for west of the central meridian. The below example uses an offset for Eastern Standard Time (`-0500`). Make sure the specification is five characters long, so include any leading and trailing zeros.

The following describes the CNFNET process for configuring the time zone:

```
You need to specify local time zone information. Time zones may be specified
as a fixed value, which must be set manually for the Daylight Savings Time
change, or you can use the NTP (Network Time Protocol) server to change the
system clock and time offset
```

```
Do you want to have NTP set the time zone and time offset automatically [N]?
```

If you accept the default [N], then the screen displays:

```
Offset from Universal time in hours and minutes:
+HHMM (east) or -HHMM (west)
```

```
Universal time zone:      UT, UTC, GMT
North American time zone: EST, EDT, CST, CDT, MST, MDT, PST, PDT
Military time zone:      Any single letter A through Z except J
```

```
You may enter a non-standard time zone name, although this is discouraged
for Internet use. If you use a non-standard name, you are prompted to enter
the offset from Universal time as well.
```

```
Enter the offset from UT or the local time zone name [UT]: -0500 Return
```

If you enter an unknown time zone name, you are prompted for the Universal time offset for the time zone.

For the offset from Universal time, enter $+HHMM$ or $-HHMM$, for the number of hours (HH) and minutes (MM) the time is offset. The $+$ is for east of the Central Meridian and the $-$ is for west of the Central Meridian. Your entry must be five characters long, so include any leading or trailing zeros.

If you enter Y at the prompt in the first display, the following appears on the screen:

```
Enter the time zone name and time zone rules (if different from default
rules). TCPWARE:TIMEZONE.DAT contains a list of available time zone rules,
or local definitions may be defined in TCPWARE.TIMEZONES.LOCAL.
```

```
Enter the time zone name: EST
Enter the time zone rule:
```

When you use `CNFNET` to configure time zones, you are prompted for information that defines symbols in the `TCPWARE_CONFIGURATION.COM` file.

- Zone Name
- Time Zone Rule

You can skip the `time zone rule` prompt when a compiled-in time zone is specified.

Define your local time zone information according to its offset from Universal time. You can either manually change the offset as needed or configure the offset to be done automatically. If you have it done automatically, you need to run `NTP`.

Enter your local time zone's offset from Universal time or its symbolic time zone abbreviation. See the below table:

This time zone...	Is abbreviated as...
Universal Time	UT, TUC, or GMT
North American Time	EST, EDT, CST, CDT, MST, MDT, PST, PDT ¹ ¹ Standard "S" times are one hour later than Daylight "D" times; for example, EST is -0500 while EDT is -0400
Military Time	Any single uppercase letter A through Z except J (this format not recommended).

Define the Local Hostname

The next step is to define your local host's name.

Enter the official host-domain name for your local host. Press **Return** if the default shown is correct. Make sure you enter the full host-domain name, especially if you plan to use the Domain Name Services (DNS).

Define the official host-domain name as other hosts on the network know it. Your hostname defines the `TCPWARE_DOMAINNAME` logical that DNS uses to determine the current domain. DNS determines the domain by dropping the hostname and dot from the beginning of the entry you make.

The official name of the local host is usually the same as what you specified at the prompt:

```
What is the HOST NAME for line...
```

in the *Enter Address Information for the Network Devices* section. If your network uses domain-name style hostnames, enter the full domain name for your host. Otherwise, enter the full hostname.

Although the hostname is not case-sensitive, TCPware preserves the case as you enter it.

Below is an example of defining your local host's name:

```
You need to enter the official name of this host as it is known locally and  
by other hosts on the network.
```

```
If your system will use Domain Name Services, you must enter the full domain  
name of the host.
```

```
Enter the official host-domain name for this host [MAIL.EXAMPLE.COM]:  
Return
```

If you are using DNS, continue to the next section. If you are not using DNS, this completes the TCP/IP core configuration. If you need to configure the TCP/IP components, continue to the next chapter.

Update the HOSTS. File

Ignore this section if you are using the Domain Name Services (DNS).

If you are not using DNS, you need to define a host definition (`HOSTS.`) file. Some socket library routines use this file when looking up hostnames and internet addresses. If you configure TCPware for the first time, TCPware creates the `HOSTS.` file automatically.

Follow these steps to update the host definition (`HOSTS.`) file:



Note: If this is not a first-time installation, CNFNET may identify that a `HOSTS .` file already exists and asks if you want to use it or create a new one. The default is `NO` (do not use the existing file). If you accept this default, a new `HOSTS .` file is created. Make sure that you properly define these hosts in the file. If you answer `Y`, the core configuration ends here.

1. The local loopback and the hostname you entered previously become the first entries in the `HOSTS .` file. Enter the next hostname at the prompt:

```
Next host name (<return> to end):
```

2. Enter the Internet address of the hostname.
3. Continue entering hostnames until you define all the hosts and their Internet addresses. Then press **Return** at the prompt:

```
Next host name (<return> to end):
```

Although hostnames are not case-sensitive, TCPware preserves their case as you enter them.

Below is an example of creating the `HOSTS .` file:

```
You can enter the host name and the corresponding internet address for the
hosts on the network.
```

```
The host definition file, TCPWARE_COMMON:[TCPWARE]HOSTS., contains the host
names and internet addresses for the hosts on the network. You may also edit
this file manually.
```

```
localhost LOOPBACK (127.0.0.1) added to host definition file.
MAIL.EXAMPLE.COM (192.168.1.56) added to host definition file.
```

```
Next host name (<return> to end): DAISY Return
```

```
Internet address for DAISY.EXAMPLE.COM: 192.168.1.57 Return
DAISY.EXAMPLE.COM (192.168.1.57) added to host definition file.
```

```
Next host name (<return> to end): Return
```

If you need to define additional hostnames later, or correct names already entered, edit the `TCPWARE:HOSTS .` file directly. The syntax of entries in the file is:

```
address hostname [alias [alias...]]
```

If you need to configure TCP/IP components, continue to the next chapter now.

4. Starting and Testing TCPware

Introduction

This chapter describes how to start and stop TCPware, and remove TCPware files. It is for the OpenVMS system manager, administrator, or operator responsible for system startup.

Prepare for Startup

Verify the Installation, Configuration, and Registration

Before you start TCPware for the first time, be sure you have:

- Installed your TCPware components.
- Correctly configured your TCPware components.
- Registered TCPware through your Product Authorization Key (PAK).

Running Other Products

If you run DECnet, DECwindows, HYPERchannel, or another vendor's TCP/IP product, there are a few things you need to keep in mind:

If you...	Then you must...
Run DECnet	Start DECnet before starting TCPware. If DECnet and TCPware use the same Ethernet controller, DECnet cannot start if TCPware is already running. (You do not have to run DECnet to use TCPware).

Run DECwindows	Set up the DECwindows transport interface. You can use the TCPware DECwindows transport interface only if your system runs VMS 5.5-2 or later, and if you enabled this feature during network configuration. To set up and use the TCPware DECwindows transport interface, see Chapter 28 in the <i>Management Guide</i> .
Use HYPERchannel support	Start and load the Network Systems Corporation H269 driver (as described in the H269 documentation) before starting TCPware.

System Parameters

You can use the `SYSGEN` utility in OpenVMS to examine the system parameters described in this section. Edit the `SYS$SYSTEM:MODPARAMS.DAT` file and use `AUTOGEN` to change the system parameters. System parameter settings need to be as follows:

- The TCPware shareable Socket Library, SMTP ONC RPC Run-Time Library and the TCPware DECwindows transport interface require a modest number of global pages and sections for the shareable images they install.
- `GBLPAGES` refers to the global page table entries. `GBLSECTIONS` refers to the number of global section descriptors. If an insufficient number of `GBLPAGES` or `GBLSECTIONS` are free, the shareable images might fail to install. If this happens, increase the number of each.
- The below table lists the minimum free requirements for global pages and sections required after installation but before starting TCPware.
- If you plan to use Serial Line IP (SLIP) lines, make sure you set the maximum buffer size (`MAXBUF`) and alternate type-ahead (`TTY_ALTYPAMD`) system parameters properly. Change the following parameters:
 - `MAXBUF` should be at least twice the maximum transmission unit (MTU) of the SLIP line plus 144. The default MTU for SLIP lines is 1006 bytes; therefore, `MAXBUF` must be at least 2156. Increase `MAXBUF` if necessary.
 - `MAXBUF` is dynamic. If you use `SYSGEN` to change it, you do not need to reboot the system for the change in value to take effect.
 - `TTY_ALTYPAMD` should be larger than its default value. This prevents characters from being lost. The greater the line speed, the higher you should set this parameter. For most applications, 1024 is appropriate.
 - `TTY_ALTYPAMD` is not dynamic. If you use `SYSGEN` to change this parameter, you must reboot the system for the change to take effect.

Account Privileges

Make sure each TCPware user account has TMPMBX and NETMBX privileges. These are the normal default privileges required to use TCPware. Use the OpenVMS AUTHORIZE utility to grant these privileges to the appropriate users.

Shareable Image	GBLPAGES	GBLSECTIONS
DECW_TRANSPORT_TCPWARE*	8	2
SMTP_MAILSHR	20	2
SMTP_MAILSHRP*	10	2
TCPWARE_RPCLIB_SHR	5	1
TCPWARE SOCKLIB_SHR	10	2

Automatic Startup Process

To automatically start TCPware each time you boot your system, add TCPware to your system startup file. Edit your system startup file and add these lines after the ones that start DECnet (note that they are valid only for the default TCPware installation common files location):

```
$ @SYS$SYSROOT:[TCPWARE]TCPWARE LOGICALS
$ @TCPWARE:STARTNET
```

Configuring the TCPware Commands

To configure the TCPware commands, edit your SYLOGIN.COM file to define all the TCPware commands. Add the following line to the "all accounts" definition section of the system-wide login file, SYS\$MANAGER:SYLOGIN.COM:

```
$ @TCPWARE:TCPWARE_COMMANDS
```

To prevent any errors in the SYLOGIN.COM file from causing a TCPware module to fail, you might want to include this line at the beginning of the file to disable error checking:

```
$ SET NOON
```

Note: If you chose to install TCPware common files in a location other than the default, you must redefine SYS\$SYSROOT to point to that location.

If your VMS version is...	Your startup file is...
OpenVMS VAX V6.x	SYS\$MANAGER:SYSTARTUP_VMS.COM
OpenVMS Alpha	SYS\$MANAGER:SYSTARTUP_VMS.COM
OpenVMS I64	SYS\$MANAGER:SYSTARTUP_VMS.COM
VMS V5.x	SYS\$MANAGER:SYSTARTUP_V5.COM

Configuration Menu Startup or Shutdown Process

You can start all components or selected components from the configuration menu system. At the DCL prompt enter:

```
$ @TCPWARE:CNFNET MENU
```

At the menu shown below, enter 1 if you want to start up TCPware's services.

```
TCPware(R) for OpenVMS Configuration Menu
Configuration Options:
  1 - Configure TCPware Services

  2 - Startup/Restart all TCPware Services
```

3 - Shutdown all TCPware Services

L - Display the software licensing information (PASSWORD)

E - Exit the configuration procedure (changes will be saved)

Enter configuration option: **1**

If you enter 1, another menu appears from which you can select to start or restart the entire service (4), or start or restart a particular component (6). In the latter case, a menu such as the one below appears.

Starting a Specific TCP/IP Component

Startup options:

- 1 - ACCOUNTING Startup the TCP/IP Services accounting facility
- 2 - CNFS Startup the NFS-OpenVMS Client
- 3 - DHCP4 Startup the Dynamic Host Configuration Protocol V4 Server
- 4 - DHCP Startup the Dynamic Host Configuration Protocol Server
- 5 - DNIP Startup DECnet over IP tunnels
- 6 - DNS Startup the Domain Name Server
- 7 - FTP Startup the FTP-OpenVMS Server
- 8 - GATED Startup the Gate Daemon
- 9 - IMAP Startup the Internet Message Access Protocol Server
- 10 - IPP Startup the Internet Printing Protocol Client
- 11 - IPS Startup the IPS subsystem
- 12 - KERBEROS Startup the Kerberos Services
- 13 - LPS Startup the Line Printer Services
- 14 - MISC Startup the Miscellaneous Services
- 15 - NFS Startup the NFS-OpenVMS Server
- 16 - NTP Startup the Network Time Protocol Daemon
- 17 - POP3 Startup the Post Office Protocol V3 Server
- 18 - PWIP Startup the PWIPDRIVER
- 19 - RCMD Startup the Berkeley R Commands
- 20 - SMTP Startup the Simple Mail Transfer Protocol Services
- 21 - SNMP Startup the Simple Network Management Protocol Agents
- 22 - SSH Startup the SSH-OpenVMS Server
- 23 - TALK Startup the TALK Server
- 24 - TELNET Startup the TELNET-OpenVMS Server
- 25 - TIMED Startup the TIMED Server
- 26 - XDM Startup the XDM Server

Enter menu option (E to exit):

CAUTION! Do not use the STOP PROCESS/ID command to stop TCPware or any of its components. Use the SHUTNET command as described on the following page.

Command Startup or Shutdown Process

You can also use the DCL command method to start TCPware or one of its components:

<pre>@TCPWARE:STARTNET [component]</pre>	<p>STARTNET by itself starts all TCPware. If you specify a component with the command, you start that component only (see Error! Reference source not found.the output listing above for the TCP/IP Services; note that your list of available components may be different). Start the TCP/IP Services components using</p> <pre>\$ @TCPWARE:STARTNET TCPWARE</pre> <p>Upon startup, TCPware checks for the logicals TCP, UDP, IP, INET, RMT, RCD, BG, and QX. If any of these logicals have been previously defined on your system, the following warning is generated:</p> <pre>%TCPWARE-W-BADLOGICAL</pre> <p>Redefine the conflicting logicals and restart TCPware.</p>
<pre>@TCPWARE:SHUTNET [component]</pre>	<p>SHUTNET by itself shuts down all TCPware. If you specify a component with the command, you shut down that component only (use one of the component names from the above output listing).</p>

Customizing Your Startup

If your network configuration has special requirements, you might need to create the file `TCPWARE:TCPWARE_STARTUP.COM` and call it from the OpenVMS system startup file. (See the comments in the `STARTNET.COM` file for more details about special requirements.)

To configure special requirements:

1. Copy the `TCPWARE:TCPWARE_STARTUP.TEMPLATE` template file to the `TCPWARE:TCPWARE_STARTUP.COM` file:

```
$ COPY TCPWARE_COMMON:[TCPWARE]TCPWARE_STARTUP.TEMPLATE -
_$ TCPWARE_COMMON:[TCPWARE]TCPWARE_STARTUP.COM
```

2. Edit the VMS system startup file.

a. Delete the following line or pair of lines, whichever the file contains:

```
$ @SYS$SYSROOT:[TCPIP]STARTNET
$ @SYS$SYSROOT:[TCPWARE]TCPWARE_LOGICALS
$ @TCPWARE:STARTNET
```

b. Add the following line to the VMS system startup file:

```
$ @TCPWARE_COMMON:[TCPWARE]TCPWARE_STARTUP.COM
```

3. Edit the `TCPWARE_STARTUP.COM` file as needed and as described in the rest of this section.

Note: Changes you make to network parameters using Network Control Utility (NETCU) commands are active until TCPware shuts down. Update the `TCPWARE_STARTUP.COM` file with these commands to make them permanent.

For example, you might want to do the following:

Step	Task	Action
1	Override the default TCP maximum segment size or window size	<p>See the description of the <code>START/TCP</code> command <code>/MSS</code> and <code>/MWS</code> qualifiers in the <i>NETCU Command Reference</i>, Chapter 2, <i>NETCU Commands</i>.</p> <p>If you use TCP over a satellite link with a line speed greater than 384 Kbits, configure TCPware on both sides with a window size greater than 63448 bytes. See the description of the <code>START TCP</code> command for details on using satellite links.</p>

2	Override the default UDP maximum datagram size	See the description of the <code>START/UDP</code> command <code>/MDS</code> qualifier.
3	Enable packet forwarding capability	See the description of the <code>ENABLE FORWARDING</code> command <code>/MDS</code> qualifier. You can also add the <code>ENABLE FORWARDING</code> command to the <code>TCPWARE_STARTUP.COM</code> file.
4	Join multicasting host group addresses	You may have applications that rely on multicasting yet do not want to change the application code to join the specific groups so that they can receive the multicast datagrams. Therefore, you can include <code>ADD MULTICAST_GROUP</code> commands to the <code>TCPWARE_STARTUP.COM</code> file to add the multicast IP addresses.

```
START/TCP/MWS=value/MSS=value /NOKEEPALIVE [1]
START/UDP/MDS=value [2]
ENABLE FORWARDING [3]
ADD MULTICAST_GROUP 224.0.0.2 /LINE=ISA-0 [4]
```

Starting User-Written Servers

If you want any user-written servers to start automatically when you start TCPware, edit the `SERVERS.COM` file. CNFNET creates a template of this file if none existed previously.

To start a user-written server automatically, do the following:

1. Edit the `TCPWARE:SERVERS.COM` file.
2. Enter the `ADD SERVICE` command in the file for each server you add.

For example, if you built `FINGERD` from the sources TCPware provides, you might add the command below to the end of the `SERVERS.COM` file.

The various quotas and parameters might be different for your system, or you might choose to take the defaults for most values.

See the description for the `ADD SERVICE` command in the *NETCU Command Reference*, Chapter 2, *NETCU Commands*.

```
ADD SERVICE FINGER TCP TCPWARE:FINGERD -
    /PROCESS_NAME = FINGERD -
    /NOACCOUNTING -
    /NOAUTHORIZE -
    /INPUT = NLA0: -
    /OUTPUT = NLA0: -|
    /ERROR = NLA0: -
    /UIC = [SYSTEM] -
    /AST_LIMIT = 10 -
    /BUFFER_LIMIT = 10240 -
    /ENQUEUE_LIMIT = 100 -
    /EXTENT = 500 -
    /FILE_LIMIT = 20 -
    /IO_BUFFERED = 6 -
    /IO_DIRECT = 6 -
    /MAXIMUM_WORKING_SET = 300 -
    /PAGE_FILE = 10000 -
    /PRIORITY = 4 -
    /PRIVILEGES = (NOSAME, SYSPRV, NETMBX, TMPMBX, WORLD) -
    /QUEUE_LIMIT = 8 -
    /WORKING_SET = 200 -
    /SUBPROCESS_LIMIT = 0
```

Installing and Configuring INGRES/Net

Action's INGRES/Net product can use TCPware as the TCP/IP network protocol. For supported versions of INGRES/NET, use TCPware's UCX Compatibility mode, which is the TCP_HP protocol at INGRES/Net startup.

Removing TCPware Components

You can remove any or all TCPware components:

- To remove a single component:

```
$ @TCPWARE:TCPWARE_REMOVE component
```

- To remove all TCPware components:

```
$ @TCPWARE:TCPWARE_REMOVE TCPware
```

CAUTION! This command deletes all relevant files in all TCPware-specific directories and the TCPWARE directory.

Register Your Product Authorization Key (PAK)

Registering this PAK allows you to start and run TCPware for all the products you install.

To register your PAK, do the following:

1. Copy down the string of digits representing your hardware ID. This is your Ethernet controller's hardware ID.
2. With your hardware ID number and product names and version information available, contact Process Software's Licensing Desk.
3. The Licensing Desk will ask you for the required information and provide you with the various values you must enter during the LMF procedure. Be sure to enter these values exactly as you see them, especially the Authorization Number.
4. Use the OpenVMS License Management Facility (LMF) in one of the two following ways, depending on your preference:

- `SY$UPDATE:VMSLICENSE` command: The menu- and prompt-driven method that takes you through each licensing step in detail. Enter:

```
$ @SY$UPDATE:VMSLICENSE
```

- `LICENSE REGISTER` command: The single command method where you can specify licensing information through qualifiers. Enter:

```
$ LICENSE REGISTER TCPWARE /qualifier /qualifier ...
```

See HP's *OpenVMS License Management Utility Manual* (or *A Practical Guide to OpenVMS Software License Management and Tools*) for details on the `VMSLICENSE` or `LICENSE REGISTER` procedures.

Sample Hardware ID Information

Provide your distributor or Process Software with the following information to obtain Product Authorization Key(s) for this system:

- * Hardware ID: "12-34-56".
- * The product name and version number for the product(s) you are installing on this system.

Refer to your product documentation for more information on obtaining Product Authorization Key(s).

Sample VMSLICENSE Command Procedure Menu

VMS License Management Utility Options:

1. REGISTER a Product Authorization Key
2. AMEND an existing Product Authorization Key
3. CANCEL an existing Product Authorization Key
4. LIST the Product Authorization Keys
5. MODIFY an existing Product Authorization Key
6. DISABLE an existing Product Authorization Key
7. DELETE an existing Product Authorization Key
8. COPY an existing Product Authorization Key
9. MOVE an existing Product Authorization Key
10. ENABLE an existing Product Authorization Key
11. SHOW the licenses loaded on this node
12. SHOW the unit requirements for this node

99. EXIT this procedure

Type '?' at any prompt for a description of the information requested.
Press Ctrl/Z at any prompt to exit this procedure.

Enter one of the above choices [1]

Sample VMS PAK Information

ISSUER:	PSC
AUTHORIZATION NUMBER:	9145685760
PRODUCT NAME:	TCPWARE-TCP
PRODUCER:	PSC
NUMBER OF UNITS:	200
VERSION:	
PRODUCT RELEASE DATE:	
KEY TERMINATION DATE:	

```
AVAILABILITY TABLE CODE:  F
ACTIVITY TABLE CODE:
KEY OPTIONS:                NO_SHARE
PRODUCT TOKEN:
HARDWARE I.D.:
CHECKSUM:                   4-ABCD-EFGH-IJKL-MNOP
```

Test TCPware

Use the following steps to test your TCPware connections after a startup:

1. Verify that the databases you need are properly updated by the startup. Among these are:

- TCPWARE:HOSTS.
- TCPWARE:HOSTS.EQUIV
- .RHOSTS
- ROUTING.COM

2. Log out of the system account - TCPware for OpenVMS is ready for general use.

3. Test TCPware - perform connectivity tests for each TCPware component you installed and configured. For example, use FTP to transfer some files.

If you uncover problems during testing, review the network configuration. If you need to reconfigure a component, stop TCPware first.

5. Configuring the TCP/IP Services

Introduction

This chapter describes how to configure the components of TCPware. It is for the OpenVMS system manager or operator responsible for product configuration.

Proceed with this chapter after you install TCPware (Chapter 2) and configure the core environment (Chapter 3).

This chapter focuses on using the `CNFNET` menu-driven method (see Chapter 3) and the text and prompts that appear for a full configuration. Your configuration might differ, especially if you are changing specific component configurations.

For a basic configuration, accept the default values for each component, which appear in brackets after a prompt. This also helps you step through the process more quickly.

Each component configuration is described in its own section and in the order it occurs during the full configuration process. You can return to a specific component after you complete the full configuration procedure. Instructions to access the specific component configuration are given in each section.

Note: If you did not configure the core environment, the following message appears:

```
Please configure the core environment before configuring a specific
component
```

Return to Chapter 3, the *Start CNFNET* section.

Note: You do not need to reboot your system after the configuration.

A full configuration example appears in *Appendix B*.

Configure the TCPware Components

How you start to configure the TCPware components depends on how you chose to configure the core environment.

Basic Configuration Choice

If you invoked CNFNET in one of the following ways, you transition into the basic configuration after you complete the TCPware core configuration (in Chapter 3):

- @TCPWARE:CNFNET
- @TCPWARE:CNFNET TCPWARE
- @TCPWARE:CNFNET TCP
- @TCPWARE:CNFNET BASIC

After you complete the core environment configuration, you transition to the first prompt for the ACE/Client configuration, as shown below:

```
You can enter the host name and the corresponding internet address for the
hosts on the network.
```

```
The host definition file, TCPWARE_COMMON:[TCPWARE]HOSTS., contains the host
names and internet addresses for the hosts on the network. You may also edit
this file manually.
```

```
localhost LOOPBACK (127.0.0.1) added to host definition file.
NUNKI.EXAMPLE.COM (192.168.1.56) added to host definition file.
Next host name (<return> to end): DAISY
```

```
Internet address for DAISY.EXAMPLE.COM: 192.168.1.57
DAISY.EXAMPLE.COM (192.168.1.57) added to host definition file.
```

```
Next host name (<return> to end): Return
Do you want to use the TCPware ACE/Client to authenticate user login?[YES]
```

Full Configuration Choice

Use the full configuration choice when you want to configure all the TCPware components. You perform a full configuration when you invoke CNFNET using

```
$ @TCPWARE:CNFNET MENU
```

Enter **1** (Configure TCPware Services) at the Enter configuration option: prompt, and enter **2** (Configure all TCP/IP components) after you perform the TCP/IP core configuration and return to the TCPware Services Configuration Menu (see the example below).

You also perform a full configuration when you invoke CNFNET using:

```
$ @TCPWARE:CNFNET FULL
```

You usually perform a full configuration when you are familiar with each TCPware component and want to customize your settings. An example of invoking a full configuration:

```
TCPware Services Configuration Menu  
Configuration Options:
```

- 1 - Core environment for TCP/IP services
- 2 - Configure all TCP/IP components
- 3 - Configure a specific TCP/IP component

- 4 - Startup/Restart TCP/IP services
- 5 - Shutdown TCP/IP services
- 6 - Startup/Restart a specific TCP/IP component
- 7 - Shutdown a specific TCP/IP component

- E - Exit to previous menu

```
Enter configuration option: 2
```

Component Configuration Choice

The component configuration is most useful for fine tuning an individual component configuration. It is essentially a full configuration, but for a single component only. You start a component configuration when you invoke CNFNET using

```
$ @TCPWARE:CNFNET MENU
```

Complete the core configuration, return to the TCPware Component Configuration Menu, and enter **3** (Configure a specific TCP/IP component) at the prompt: Enter configuration option:.

You then access the Configuring a Specific TCP/IP Component menu. Enter the number next to the component listed at the prompt:

Enter menu option:

For example, to configure the NFS Client, enter **2**. (You can also enter the component name, such as **CNFS**.)

You can also perform a component configuration when you invoke CNFNET as follows:

```
$ @TCPWARE:CNFNET component
```

Substitute the component name abbreviation for *component* in the command. Use the abbreviations listed after the numbers in the below output.

```
Configuring a Specific TCP/IP Component
```

```
Configuration options:
```

- 1 - ACCOUNTING Configure the TCP/IP Services accounting facility
- 2 - ACECLIENT Configure the ACE/Client Service
- 3 - CNFS Configure the NFS-OpenVMS Client
- 4 - DHCP4 Configure the Dynamic Host Configuration Protocol V4 Server
- 5 - DHCP Configure the Dynamic Host Configuration Protocol Server
- 6 - DNIP Configure DECnet over IP tunnels
- 7 - DNS Configure the Domain Name Server
- 8 - FTP Configure the FTP-OpenVMS Server
- 9 - GATED Configure the Gate Daemon
- 10 - IMAP Configure the Internet Message Access Protocol Server
- 11 - IPP Configure the Internet Printer Protocol
- 12 - IPS Configure the IPS subsystem
- 13 - KERBEROS Configure the Kerberos Services
- 14 - LPS Configure the Line Printer Services
- 15 - MISC Configure the Miscellaneous Services
- 16 - NFS Configure the NFS-OpenVMS Server
- 17 - NTP Configure the Network Time Protocol Daemon
- 18 - POP3 Configure the Post Office Protocol V3 Server
- 19 - PWIP Configure the PWIPDRIVER
- 20 - RCMD Configure the Berkeley R Commands
- 21 - SMTP Configure the Simple Mail Transfer Protocol Services
- 22 - SNMP Configure the Simple Network Management Protocol Agents
- 23 - SSH Configure the SSH-OpenVMS Server
- 24 - TALK Configure the TALK server
- 25 - TELNET Configure the TELNET-OpenVMS Server
- 26 - TIMED Configure the TIMED Server
- 27 - XDM Configure the XDM Server

```
Enter menu option (E to exit):
```

For example, to configure the NFS client, enter

```
$ @TCPWARE:CNFNET CNFS
```

Configure the NFS Client

Because you need to install, configure, and start TCPware before you can set up the NFS client, you might want to enter **N** at the prompt:

```
Do you want the NFS Client [YES]
```

This lets you continue with CNFNET. You can always go back later to invoke the NFS client component configuration using

```
$ @TCPWARE:CNFNET CNFS
```

You need to first use the Network Control Utility (NETCU) to define entries for the PROXY and GROUP databases to enforce file system protection across the network.

Prepare

Before you add users to the PROXY and GROUP databases, you need to:

- Be sure the network is up and running.
- Identify which OpenVMS client users need to access NFS served files on the network.
- Match the OpenVMS users with valid accounts on the host running the NFS server software. In some cases, you might need to create new usernames to accommodate these accounts.

```
$ NETCU
NETCU>SHOW PROXY
%TCPWARE_NETCU-I-NOENTRIES, no PROXY entries found

NETCU>ADD PROXY SMITH /UID=1127 /GID=15 /CLIENT/SERVER
NETCU>SHOW PROXY
NFS PROXY Database V6.1 Copyright (c) Process Software

Username      UID      GID      Host(s)
-----      ---      ---      -
SMITH         1127     15
NETCU>RELOAD PROXY SMITH
```

Add GROUP Users

To add users to the client GROUP database:

1. Access the UNIX server and issue the `cat /etc/group` command at the UNIX system prompt. The format of each entry in the `/etc/group` file is:

```
unix-group:encrypted-password:GID:user-list
```

2. Select the file record with the `unix-group` that you want to associate with the OpenVMS user, and record the GID number. For example, select the following `accounting` group:

```
accounting:x:30:smith,jones
```

Then record the GID as the number 30.

3. Log out of the UNIX NFS server system.

4. Set the default to `SYS$SYSTEM` on the OpenVMS system and run `AUTHORIZE`.

5. Enter the `SHOW/IDENT` command and check the list of authorized rights identifiers.

6. Enter the `ADD /IDENTIFIER` command along with an OpenVMS rights identifier that corresponds to your chosen entry on the UNIX server.

7. Grant the `ACCOUNTING` identifier to all client users you want to have group access to the server file. These users should correspond to the `user-list` entries for the entry in the `/etc/group` file. Use the `GRANT /IDENTIFIER` command for each user.

8. Exit `AUTHORIZE`.

```
>cat /etc/group
wheel:x:0:
nogroup:x:65534:
daemon:x:1:
kmem:x:2:
bin:x:3:
tty:x:4:
operator:x:5:
news:x:6:
uucp:x:8:
audit:x:9:
login:x:15:joe2
staff:x:10:peters,henry
other:x:20:
accounting:x:30:smith,jones|
>exit
logout
$ SET DEF SYS$SYSTEM
$ RUN AUTHORIZE
```

```

UAF>SHOW/IDENT *
Name          Value          Attributes
BART          [001000,000127]
DECNET        [000376,000376]
DIALUP        %X80000002
FAL$SERVER    [000376,000373]
INTERACTIVE   %X80000003
LOCAL         %X80000004
SYSTEM        [000001,000004]
USER          [000200,000200]
UAF>ADD/IDENTIFIER ACCOUNTING
%UAF-I-RDBADDMMSG, identifier ACCOUNTING value: %X80010006 added to rights
data base
UAF>GRANT/ID ACCOUNTING SMITH
%UAF-I-GRANTMSG, identifier ACCOUNTING granted to SMITH
UAF>GRANT/ID ACCOUNTING SMITH
%UAF-I-GRANTMSG, identifier ACCOUNTING granted to SMITH
UAF>EXIT
%UAF-I-NOMODS, no modifications made to system authorization file
%UAF-I-NAFNOMODS, no modifications made to network proxy data base
%UAF-I-RDBDONEMSG, rights data base modified

```

Add GROUP Groups

To add a group to the GROUP database:

1. Run NETCU.
2. Enter an ADD GROUP command for the new group. Use the format:

```
NETCU> ADD GROUP nfs-group identifier
```

nfs-group is the same number as the group in the `/etc/group` file on the server; for example, 30 in the `accounting:x:30:smith,jones` entry.

identifier is the rights identifier you previously defined with the ADD /IDENTIFIER command; for example, ACCOUNTING.

3. Enter the SHOW GROUP command in NETCU to confirm that the GROUP database contains the correct information. The value can be either hexadecimal (as shown in the below example) or in UIC format (such as `[1000,1000]`).
4. Enter the RELOAD GROUP command if you added a group to an existing GROUP database. This command ensures that new entries take effect by reloading the database on the client.
5. Exit NETCU.

6. Repeat the process for each new group definition; for example, group 10 in the below example (the `staff:x:10:peters,henry` entry in the `/etc/group` file on the server).

```
$ NETCU
NETCU>ADD GROUP 30 ACCOUNTING
NETCU>SHOW GROUP
NFS GROUP Database V6.1 Copyright (c) Process Software
Group   Name           Value             Host(s)
-----  ----
30      ACCOUNTING        %X80010006
NETCU>RELOAD GROUP
NETCU>EXIT
$ RUN AUTHORIZE
UAF>ADD /ID STAFF
%UAF-I-RDBADDMMSGU, identifier STAFF added
UAF>GRANT /ID STAFF PETERS
%UAF-I-GRANTMSG, identifier STAFF granted to PETERS
UAF>GRANT /ID STAFF HENRY
%UAF-I-GRANTMSG, identifier STAFF granted to HENRY
$ NETCU
NETCU>ADD GROUP 10 STAFF
```

See the *TCPware Management Guide*, Chapter 13, *Managing the NFS Client*.

Configure the DHCP Client

Note: Versions of TCPware prior to 6.1 provided both DHCP V4 and a legacy DHCP V3 implementation. DHCP V3 has been deprecated since TCPware 5.9, and is no longer provided. If you're still running the legacy DHCP V3 server, an easy and automated upgrade path is available. See Chapter 4, *DHCP/BOOTP Server*, in the *TCPware Management Guide*.

If this is your first time using a DHCP client on the host, you need to create a configuration file for it (`TCPWARE:DHCLIENT.CONF`). There is a template configuration file available in the TCPware common directory.

To create a configuration file from the template:

```
$ COPY TCPWARE:DHCLIENT4_CONF.TEMPLATE TCPWARE:DHCLIENT.CONF
```

The DHCP client configuration file should now be edited to specify the name of your host. Talk to your network administrator: the administrator may want to assign you a host name.

To specify a host name, edit the configuration file to replace this line:

```
#send host-name "testing";
```

with this line:

```
send host-name "any hostname you want";
```

To configure your local host to use the DHCP client, run the TCPware configuration utility CNFNET.

```
$ @TCPWARE:CNFNET DHCLIENT4
```

After you configure the local host to use a DHCP client, you can run STARTNET to start TCPware:

```
$ @TCPWARE:STARTNET
```

Here are two examples:

Using CNFNET:

```
$ @TCPWARE:CNFNET
```

```
TCPware (R) for OpenVMS Version 6.1-0 Network Configuration procedure for:  
TCP/IP Services:
```

```
    FTP-OpenVMS  
    NFS-OpenVMS Client  
    NFS-OpenVMS Server  
    SMTP-OpenVMS  
    TELNET-OpenVMS  
    Kerberos Services  
    SSH-OpenVMS Server
```

This procedure helps you define the parameters needed to get TCPware (R) for OpenVMS running on this system.

This procedure creates the configuration data file, TCPWARE_SPECIFIC:[TCPWARE]TCPWARE_CONFIGURE.COM, to reflect your system's configuration.

Type Return to continue... **Return**

```
... ..  
... ..
```

You need to supply the following information for each line:

- The internet address for the line
- The name for the line (same as the host name if single line host, fully qualified domain name if using DNS)
- The subnet mask for the line
- The line specific information (depends on the line)

If there is a DHCP server running on the network and this is a single line

host, you may get the information from DHCP server automatically. To do so, please select 2.

1. Configure Internet address and related items manually.
2. Configure Internet address and related items automatically

Continue with selection [1]:2 Return

Configure line SVA-0:

Set DHCP client Host Name

You can press Enter to let the system choose a host name. Or you can specify a name you would like to use for the host. However, the final name for the host will be up to the DHCP server to decide, it may not be the name you specify.

Host Name (Return to end) []:**Return**

You need to specify local time zone information. Time zone maybe specified as fixed value which must be manually set for the daylight savings time change, or you can use NTP (Network Time Protocol) Daemon to change the system clock and time offset automatically.

Do you want to have NTP set the time and time offset automatically [NO]?

... ..

... ..

Using CNFNET DHCLIENT:

```
$ @TCPWARE:CNFNET DHCLIENT
```

TCPware(R) for OpenVMS Version 6.1-0 Network Configuration procedure for:

TCP/IP Services:

- FTP-OpenVMS
- NFS-OpenVMS Client
- NFS-OpenVMS Server
- SMTP-OpenVMS
- TELNET-OpenVMS
- Kerberos Services
- SSH-OpenVMS Server

This procedure helps you define the parameters needed to get TCPware(R) for OpenVMS running on this system.

This procedure creates the configuration data file, TCPWARE_SPECIFIC:[TCPWARE]TCPWARE_CONFIGURE.COM, to reflect your system's configuration.

```
Type Return to continue... RETURN
```

```
Configuring the Dynamic Host Configuration Protocol (DHCP) Client:  
Do you want to use the DHCP Client [YES]: RETURN
```

```
The DHCP Client can perform error logging and debug message logging to  
OPCOM.
```

```
You can choose whether to log debug messages to OPCOM (errors are always  
logged to OPCOM).
```

```
Log error/debug messages to OPCOM [NO]: RETURN
```

```
Set DHCP client Host Name :
```

```
You can press Enter to let the system choose a host name. Or you can specify  
a name you would like to use for the host. However, final name for the host  
will be up to the DHCP server to decide, it may not be the name you specify.
```

```
Host Name (Return to end) []:
```

```
Do you want to restart DHCLIENT [NO]: RETURN  
$
```

Configure the DHCP Server

Note: Versions of TCPware prior to 6.1 provided both DHCP V4 and a legacy DHCP V3 implementation. DHCP V3 has been deprecated since TCPware 5.9, and is no longer provided. If you're still running the legacy DHCP V3 server, an easy and automated upgrade path is available. See Chapter 4, *DHCP/BOOTP Server*, in the *TCPware Management Guide*.

The Dynamic Host Configuration Protocol (DHCP) server supports the DHCP protocol and the BOOTP (bootstrap) protocol. Both protocols allow you to supply IP addresses and network configuration data to remote client systems.

CNFNET Steps

You can configure the DHCP server as part of the general CNFNET configuration or specifically using `@TCPWARE:CNFNET DHCP4:`

1. At the prompt, enter **Y** if you want to run the server, or press **Return** or enter **N** if you do not want to run the server.
2. If you responded **Y** in step 1, you must also specify what kind of error logging and debug logging you want and where you want the logging to go.
 - a. Specify the debug logging level you want, or press **Return** to accept the default, which is to log severe errors and warnings.
 - b. Specify the name of the debug log file you want, or press **Return** to accept the default (`TCPWARE:DHCPDEBUG.LOG`). Enter **NL:** to have no log file.
 - c. At the prompt, enter **Y** if you want the date included in each log file entry (the time is always included), or press **Return** or enter **N** if you do not want the date included.
 - d. At the prompt, enter **Y** if you want debug messages logged to OPCOM, or press **Return** or enter **N** if you do not.

For more information on DHCP, see the *TCPware Management Guide*, Chapter 4, *DHCP/BOOTP Server*.

```
Configuring the Dynamic Host Configuration Protocol (DHCP) Server:
Do you want to enable the Dynamic Host Configuration/Bootstrap Protocol
Server (DHCPD) [YES]: Y
```

```
The DHCP server can perform error logging and debug message logging to OPCOM
or a file or both. You can set the error/debug logging level, the name of
the file to log to (if any), whether to include the date on each entry in
the log file, and whether to log debug messages to OPCOM (errors are always
logged to OPCOM). The logging level value is a decimal integer that is a
bitmask of levels of increasing severity. The levels are (in decimal):
```

```
1  Severe Errors
3  Warnings
7  Informationals
15 Debug Messages
31 Dump Packets (Formatted)
63 Dump Packets (Hex)
```

```
It is recommended that the value be set to log at least severe errors and
warnings.
```

```
Error/Debug logging level [3]: Return
```

```
Debug file name (use _NL: for none) [TCPWARE:DHCPDEBUG.LOG]: Return
```

Include date on each log entry [NO]: **Return**

Log debug messages to OPCOM [NO]: **Return**

Configure DECnet over IP Tunnels

The next step is to configure DECnet over IP tunnels. Tunneling DECnet over IP allows you to configure a DECnet line and circuit between two OpenVMS systems running TCPware.

Prepare

To configure DECnet over IP tunneling, you need:

- The Internet address of the remote host that establishes the tunnel.
- The port number for this tunnel on the remote host (the default port number is 64215).

CNFNET Steps

You can configure TCPware's DECnet over IP tunnels as part of the general CNFNET configuration or specifically as @TCPWARE:CNFNET DNIP (see the below example).

1. Respond to the prompt Do you want to configure DECnet over IP tunnels [NO] : with **Y**.
2. Specify the DECnet line name for the first DECnet over IP tunnel. If this is the first DECnet over IP tunnel, enter DNIP-0-0.
3. Enter the IP address of the remote host.
4. Enter the port number for this tunnel on the remote host. To accept the default port number [64215], press **Return**.
5. Enter the port number for this tunnel on the local host. If the one given is correct, press **Return**.
6. Enter **Y** if you want to configure another DECnet over IP tunnel. If you answer **Y**, return to step 2 and configure the next DECnet over IP tunnel.
7. To end configuring tunnels, enter **N** or press **Return** when the Do you want to configure another tunnel prompt reappears.
8. If the DNIP configuration is correct, enter **END** or **E** at the What would you like to do (ADD, CHANGE, DELETE, or END) : prompt.

Configuring DECnet over IP tunnels:

DECnet over IP tunneling allows you to establish DECnet lines and circuits over a TCP/IP network.

Do you want to configure DECnet over IP tunnels [NO]: **Y**

Specify DECnet line name for the tunnel [DNIP-0-0]: **Return**

You need to specify the internet address of the remote host with which you want to establish the tunnel.

Specify remote host internet address: **192.168.2.10**

You need to specify the TCP port number for the tunnel on both the local and remote hosts. Normally you should use the default port number (64215, an unassigned port that is unlikely to be used on your systems). If for any reason you need a different port number, specify it here.

The local port number and remote port number do not have to be the same.

You can use the same port number for more than one tunnel.

Specify port number for this tunnel on remote host 192.168.2.10 [64215]:
Return

Specify port number for this tunnel on this host [64215]: **Return**

Do you want to configure another tunnel [NO]: **Y**

Specify DECnet line name for the tunnel [DNIP-0-1]: **Return**

Specify remote host internet address: **192.168.2.65**

Specify port number for this tunnel on remote host 192.168.2.65 [64215]:**Return**

Specify port number for this tunnel on this host [64215]:**Return**

Do you want to configure another tunnel [NO]: **Return**

The currently configured tunnels are:

DECnet Line	Remote Host	Local Port	Remote Port
DNIP-0-0	192.168.2.10	64215	64215
DNIP-0-1	192.168.2.65	64215	64215

You may enter:

ADD	To add a new tunnel or tunnels
CHANGE	To change an existing tunnel or tunnels
DELETE	To delete an existing tunnel or tunnels
END	To end configuring the DECnet over IP tunneling

What would you like to do (ADD, CHANGE, DELETE, or END): **END**

Configure DNS

If you entered a domain-style hostname when you defined your local hostname during the core configuration, CNFNET asks additional questions about the Domain Name Services.

You can configure the Domain Name Services as part of the general CNFNET configuration or specifically as

```
$ @TCPWARE:CNFNET DNS
```

If this is not a first-time installation, CNFNET asks if you want to change the existing configuration. Press **Return** for YES, or enter **N** for NO.

Enabling the DNS server creates a default caching server if there was no previous configuration.

If you intend to run a server other than the default caching server, you must edit the DNS configuration. See the *Editing Database Files* section in Chapter 3 of the *TCPware Management Guide*.

```
Configuring the Domain Name Services (DNS):
```

```
Do you want to change the DNS configuration [YES]: Return
```

```
Do you want to enable the DNS Server [NO]: Y
```

```
Cluster Load balancing is used to order a list of IP addresses based on their perceived system load. This server must be authoritative for any cluster names that are to use cluster load balancing, and the server must know what those cluster names are. If you would like to use cluster load balancing, enter yes to be prompted to enter cluster names. Use spaces to separate cluster names
```

```
Do you want to configure a list of cluster names [NO]: Y
```

```
Enter the cluster name(s) []: cluster.example.com
```

```
Do you want to enable DNS client support [YES]: Return
```

```
The client needs to obtain information from an DNS server.
```

```
Provide the internet address(es) of up to three DNS servers. Use spaces to separate multiple addresses.
```

```
Note: If the local host is configured as a server, you can enter the loopback internet address or the local host's internet address to make use of that server.
```

```
Enter the internet address of the server(s) [192.168.1.1]: Return
```

```
By default, the client appends the local domain name to local queries, and queries that fail resolving as fully qualified names. If you would like
```

other domains appended, provide the name(s) of up to six domains to append. If you do not want to append a domain other than your default domain, answer no to skip to the next section. Use spaces to separate multiple domains.

Do you want to configure a list of domains [NO]: **Y**

Enter the name(s) of the domains in search list []: **example.com com**

By default, the client resolves host names with 1 or more dots absolutely before appending your domain name. If you would like host names with 1 or more dots to be resolved with your domain name first, or you would like host names with no dots to be resolved absolutely, you want to change the number of dots.

Do you want to configure number of dots [NO]: **Y**

Enter the minimum number of dots to be resolved absolutely [1]: **2**

This is how your DNS client is configured:

```
Domain Name:      example.com
Name Server(s):   192.168.1.1
Domain List:      example.com com
Number of Dots:   2
```

Is this configuration correct [YES]: **Return**

Configure the FTP Server

CNFNET Steps

You can configure the FTP server as part of the general CNFNET configuration or specifically as

```
$ @TCPWARE:CNFNET FTP
```

Note: It is advisable, if you want automatic startup of this component, to include the \$ SET NOON line in your SYLOGIN.COM file to prevent the component from failing should there be an error in the file.

Configuring FTP:

Do you want to enable the FTP server [YES]: **Return**

```
Do you want to enable the FTP client [YES]: Return
Do you want to enable FTP accounting [NO]: Y
Name of host that will run accounting collection program [localhost]:
Return
Port number that accounting collection program listens on []: Return
```

CNFNET then continues with the resolver configuration, as in the previous section.

Configure the Gateway Routing Daemon

The Gateway Routing Daemon (GateD) manages multiple routing protocols, including the Routing Information Protocol (RIP), Local Network Protocol (HELLO), Open Shortest Path First (OSPF), Exterior Gateway Protocol (EGP), Border Gateway Protocol (BGP), and ICMP Router Discovery.

GateD allows you to control the flow of routing information by means of a configuration language. Once you start GateD, it makes routing decisions based on the data gathered by the routing protocols.

CNFNET Steps

You can configure GateD as part of the general CNFNET configuration or specifically as

```
$ @TCPWARE : CNFNET GATED
```

Press **Return** for YES or enter **N** for NO at the prompt (see the below example).

```
Configuring the GateDaemon (GateD):
```

```
GateD is a routing process that automatically exchanges routing information with other hosts using a variety of protocols. The supported protocols are: RIP Version 1, RIP Version 2, DCN HELLO, OSPF Version 2, EGP Version 2, BGP Versions 2 through 4, and Router Discovery.
```

```
Please follow the procedure described in the TCPware for OpenVMS Installation & Configuration Guide to configure GateD.
```

```
Do you want to use the TCPware GateDaemon [YES]: Return
```

CAUTION! If using GateD, do not also have route settings in the ROUTING.COM file, since these routes can conflict.

Create the GATED.CONF File

Create the `TCPWARE:GATED.CONF` configuration file. For example, the statements in the `GATED.CONF` file shown below address a situation where the gateway announces a default route to the backbone and announces all the subnet routes to the outside world.

```
# enable RIP:
#
rip yes;
# using RIP, announce all local subnets via interface 192.168.12.3:
#
export proto rip interface 192.168.12.3 metric 3
{
    proto rip interface 192.168.1.5
    {
        all;
    };
};
#
# Using RIP, announce default via interface 192.168.1.5:
#
export proto rip interface 192.168.3.1
{
    proto rip interface 192.168.1.5
    {
        default;
    };
};
};
```

See the *TCPware Management Guide*, Chapter 8, *Routing and GateD*.

Configure the IMAP Server

The Internet Message Access Protocol (IMAP) server lets remote PC systems retrieve mail from your system's mailboxes. TCPware's implementation is IMAP Version 4 revision1.

CNFNET Steps

You can configure the IMAP server as part of the general CNFNET configuration or specifically as `@TCPWARE:CNFNET IMAP` (see the below example):

1. Enter **Y** or **Return** at the prompt asking if you want to enable the TCPware IMAP server. If you do not want IMAP, enter **N**.
2. If you entered **Y**, enter the user (account) the IMAPD (daemon) process should execute as. The default is SYSTEM. Whatever user you choose must have SYSNAM, TMPMBX, NETMBX, and SYSPRV or BYPASS privileges.
3. Determine if you want to enable message caching.

By default, the IMAP server caches only the text of the last accessed message and the attributes of all messages in the currently selected folder. Enabling message caching causes the server to cache the text of all messages once seen and until the folder is closed. Message caching can increase server performance, but requires considerably more memory.

4. Determine the debug logging level for the connection. Select:
 - NONE if you do not want debug logging (default)
 - ERROR if you want to log errors only
 - INFO if you want to log informational messages and errors
 - DEBUG if you want complete debug logging

You can enter just the first letter of your choice at the prompt.

5. CNFNET displays the IMAP configuration parameters you set. Respond whether this is correct by pressing **Return** for YES, or entering **N** for NO. If NO, return to step 2 to reenter the parameters.
6. If you previously configured the IMAP server, a prompt comes up asking if you want to restart it based on the changes you made.

For more information on IMAP, see the *TCPware Management Guide*, Chapter 17, *Managing Mail Services*, in the *IMAP Server* section.

```
Configuring the Internet Message Access Protocol V4 (IMAP) Server:
```

```
For detailed information on the following parameters, refer to the TCPware  
for OpenVMS Management Guide.
```

```
Do you want to enable the IMAP server [YES]: Return
```

```
Specify the username the IMAPD process should execute as. The account  
requires SYSNAM, TMPMBX, NETMBX, and SYSPRV or BYPASS privileges.
```

```
Enter the username [SYSTEM]: Return
```

```
The server can be configured to cache all messages in a folder while it is  
in use. This may increase performance in some cases, but requires
```

substantially more memory per process. By default, only the most recently accessed message is cached.

Do you want to enable full message caching [NO]: **Y**

Determine the logging level, Options are:

```
NONE    - No logging
ERROR   - Errors only
INFO    - Information messages and Errors
DEBUG   - Complete Debug logging
```

You may enter the first character of your choice.

Enter your choice (None, Error, Info, Debug) [INFO]: **NONE**

The IMAP server is configured as follows:

```
Username           : SYSTEM
Message caching enabled : YES
log level          : NONE
```

Is this correct [YES]: **Return**

Do you want to restart the Internet Message Access Protocol Server [NO]: **Y**

Shutting down the Internet Message Access Protocol Server ...
Starting the Internet Message Access Protocol Server ...

Configure IPP with CNFNET

CNFNET Steps

You can configure IPP as part of the general CNFNET configuration, or specifically as

@TCPWARE: CNFNET IPP (see the below example).

```
$ @TCPWARE:CNFNET IPP
```

TCPware(R) for OpenVMS Version 6.1-0 Network Configuration procedure for:

```
TCP/IP Services:
  FTP-OpenVMS
  NFS-OpenVMS Client
  NFS-OpenVMS Server
  SMTP-OpenVMS
  TELNET-OpenVMS
```

Kerberos Services
SSH-OpenVMS Server

This procedure helps you define the parameters needed to get TCPware(R) for OpenVMS running on this system.

This procedure creates the configuration data file, TCPWARE_SPECIFIC:[TCPWARE]TCPWARE_CONFIGURE.COM, to reflect your system's configuration.

Type <return> to continue... **RETURN**

Configuring IPP Symbiont (IPP):

IPP Symbiont is an Internet Printing Protocol Client that enables printing using IPP to IPP-capable printers and servers over a TCP/IP network. The supported version of the IPP protocol is 1.0.

Please follow the procedure described in the TCPware for OpenVMS Installation and Configuration Guide to configure IPP print queues.

Do you want to use the TCPware for OpenVMS IPP Symbiont [YES]: **YES**

Configuring the default document format for the IPP symbiont.

IPP allows the specification of the document format using MIME media types, such as "text/plain", "application/postscript" or others. The default document format entered here will become the default used by all IPP queues that do not specify a different default in their own configurations. Individual jobs may specify other values as needed. To force the default to be whatever format the individual printers have set as a default, specify "****printer_default****".

What is the default document format [text/plain]: **RETURN**

Configuring Job retry Delay for the IPP symbiont.

When there is a problem with a job that appears to be temporary in nature, the job will be requeued and tried again after a delay. The Job Retry Delay specifies the default value for how long a job will be requeued for. Individual queues may specify a different value. Specify this time as a standard OpenVMS delta time.

What is the job retry delay time [0 00:10:00.00]: **RETURN**

Configuring Max Log Bytes for the IPP symbiont.

When logging data in DETAILED_TRACE mode, the actual data being sent and received is written to the log file in hexadecimal and in ASCII. The default behavior of the symbiont is to log all data. This setting will change that default for all IPP queues to the value entered. Individual

queues may be configured to use different values than the default. The value is specified in bytes.

What is the MAX_LOG_BYTES value [-1]: **RETURN**

Configuring Max Stream Count for the IPP symbiont.

Each IPP symbiont process can handle data for up to 16 different IPP queues. Each queue handled by a given symbiont process is referred to as a "stream". This setting determines how many streams each queue will handle. When more than this number of IPP queues are started, additional symbiont processes will be created, each handling no more than MAX_STREAMS streams.

What is the maximum number of streams per symbiont process [16]: **15**

Configuring Log Level for the IPP symbiont.

There are a number of different detail levels for logging symbiont progress and problem messages. The most detailed level, "DETAILED_TRACE", can generate significant amounts of data, and should be reserved for situations where a problem is being investigated. It is not recommended for normal use.

This value specifies the default level to be used by all queues that do not specify a different value explicitly in their configurations. See the IPP documentation for a list of legal values for this parameter.

What is the default logging level [JOB_TRACE]: **FILE TRACE**

Configuring Opcom Log Level for the IPP symbiont.

There are a number of different detail levels for sending symbiont progress and problem messages to OPCOM. The most detailed level, "DETAILED_TRACE", can generate significant amounts of data, and should probably not be used for this setting.

This value specifies the default level to be used by all queues that do not specify a different value explicitly in their configurations. See the IPP documentation for a list of legal values for this parameter.

What is the default OPCOM logging level [INFO]: **RETURN**

Configuring Opcom Terminal for the IPP symbiont.

There are several OPCOM "terminals" to which OPCOM messages can be directed. This value specifies the default OPCOM terminal to be used by all queues that do not specify a different value explicitly in their configurations. See the IPP documentation for a list of legal values for this parameter.

Which OPCOM terminal should logging messages be sent to [PRINTER]: **RETURN**

Configuring Autostart for the IPP symbiont.

When TCPware is started, or CNFNET is used to start the IPP component in particular, it can automatically issue a START/QUEUE command for all of the queues on the system that use the IPP print symbiont.

Do you want to auto-start the IPP queues [NO]: **YES**

Configuring Autostop for the IPP symbiont.

When TCPware is shutdown, or CNFNET is used to shutdown the IPP component in particular, it can automatically issue a STOP/QUEUE/RESET command for each of the queues on the system that use the IPP print symbiont.

Do you want to auto-stop the IPP queues [NO]: **YES**

Do you want to restart the IPP client [NO]: **YES**

Shutting down the IPP client ...
All TCPWARE_IPP_SYMB queues stopped.
Starting the IPP client ...
Starting queue TW_IPP...
All TCPWARE_IPP_SYMB queues started.

Configure IPS with CNFNET

CNFNET Steps

You can configure IPP as part of the general CNFNET configuration, or specifically as @TCPWARE: CNFNET IPP (see the below example).

```
$ @TCPWARE:CNFNET IPS
TCPware(R) for OpenVMS Version 6.1-0 Network Configuration procedure for:

      TCP/IP Services:
          FTP-OpenVMS
          NFS-OpenVMS Client
          NFS-OpenVMS Server
          SMTP-OpenVMS
          TELNET-OpenVMS
          Kerberos Services
          SSH-OpenVMS Server
```

This procedure helps you define the parameters needed to get TCPware(R) for OpenVMS running on this system.

This procedure creates the configuration data file, TCPWARE_SPECIFIC:[TCPWARE]TCPWARE_CONFIGURE.COM, to reflect your system's configuration.

Type <return> to continue... **RETURN**

TCPware IPS (Intrusion Prevention System) is a highly-configurable subsystem for detecting attacks on components such as SSH, telnet and ftp, and responding to these attacks by putting packet filters on interfaces to block those attacks in real-time.

For detailed information on TCPware IPS, refer to the TCPware for OpenVMS Management Guide.

Do you want to enable TCPware IPS [YES]? **RETURN**

TCPware IPS uses a mailbox to deliver event information from instrumented components to the FILTER_SERVER process. The mailbox must be sized to accommodate the anticipated number of simultaneous event messages from all components. Failure to do this could result in events being lost.

The number may range from 50 to a maximum of 1000, with a default value of 400.

NOTE: If the size of the mailbox is changed, a system reboot must be performed to recreate the mailbox with the desired size.

Enter the max # of simultaneous event messages in the mailbox [400]: **RETURN**

Some process quotas for the FILTER_SERVER process must be set up to avoid issues with the FILTER_SERVER process hanging in MUTEX state.

The specific quotas, TQELM and ASTLM, should be determined based on receiving events per source addresses per rule per component. A good rule of thumb is to allocate TQELM's as follows:

- 1 for automated hourly reporting
- 1 for automated 24-hour maintenance
- 1 for each source address per rule per component for which an event has been received. These timers are used to clean up internal address structures after 24 hours of inactivity from the address.
- 1 for each non-empty event queue per source address per rule per component. These timers are used to delete aged events from the event queue.

Form ASTLM, this tends to be used at a slightly higher rate

than TQELM, so plan accordingly.

For both TQELM and ASTLM, the default values are 500.

```
Enter the value for TQELM for the FILTER_SERVER process [500]: RETURN
```

```
Enter the value for ASTLM for the FILTER_SERVER process [500]: RETURN
```

```
Do you want to restart the IPS subsystem [NO]: Y
```

```
Shutting down the IPS subsystem ...
```

```
Starting the IPS subsystem ...
```

```
$
```

Configure the Line Printer Services

The Line Printer Services (LPS) include some of TCPware's remote printing features. LPS supports an LPS client and a Line Printer Daemon (LPD) server. LPS lets you use the LPR, LPQ, and LPRM commands to print local files on remote hosts, display status information for remote print queues, and remove jobs from remote print queues. LPS also lets you use the OpenVMS PRINT command to print files remotely. For LPS, you need to configure:

- The default remote printer for the LPS commands (LPR, LPQ, and LPRM)
- The OpenVMS print queue for the PRINT command
- Possible batch startup
- The LPD server

CNFNET Steps

You can configure the Line Printer Services (LPS) as part of the general CNFNET configuration or specifically as

```
$ @TCPWARE:CNFNET LPS
```

Begin with the following steps:

1. Enter **Y** at the prompt asking if you want to enable the Line Printer Services.
2. Enter **Y** at the prompt asking if you want to configure LPS now.
3. Configure the spool directory for LPS. LPS uses a spool directory to temporarily store the files to be printed. You can use the default location or specify a different location as an OpenVMS directory specification. The default is `TCPWARE_SPECIFIC:[TCPWARE.LPS_SPOOL]`.

Note: It might be necessary to configure the remote LPD server to accept print jobs from the client host. See your UNIX system administrator or documentation for information.

Configuring the Line Printer Services (LPS):

Line Printer Services consists of the client and the server. The client lets users on this OpenVMS host print files on printers attached to remote hosts. The server accepts files from remote hosts to be printed on printers attached to this OpenVMS host. LPS configuration consists of configuring:

- Default remote printer for LPS Client commands (LPR, LPQ, LPRM)
- OpenVMS Print Queue
- LPD Server

Do you want to enable the Line Printer Services (LPS) [NO]: **Y**

Do you want to configure LPS now [YES]: **Return**

Configuring the spool directory for Line Printer Services.

LPS uses a spool directory to temporarily store the files to be printed. You may use the default location or specify a different location as an OpenVMS directory specification.

Enter the spool directory specification
[TCPWARE_SPECIFIC:[TCPWARE.LPS_SPOOL]]:

Configure the Default Remote Printer for LPS

You can configure the default remote printer to be able to use the UNIX-style LPR, LPQ, and LPRM commands in the Line Printer Services (LPS).

Prepare

To configure LPS on the client so that users can use the UNIX-style LPR, LPRM, and LPQ commands, you need the name of the:

- Local spool directory (TCPWARE_SPECIFIC:[TCPWARE.LPS_SPOOL] by default)

- Remote host serving the print queue
- Print queue on the remote print server

If the print server is a UNIX or Linux system, get the host name by using the `hostname` command:

```
$ hostname
alpha.example.com
```

And locate the print queue name by using the `lpstat` command:

```
$ lpstat -p
```

If the print queue or hostname information needs editing, get your UNIX system manager to make changes.

CNFNET Steps

To configure the default remote printer (see the below example):

1. Decide if you want to define the default remote printer at this time.
2. Enter the hostname for the remote printer. If you are not planning to use the LPR, LPRM, and LPQ commands, enter an asterisk (*).
3. Enter the default remote printer on the remote host; for example

```
ALPHA: SYS$PRINT.
```

4. If the default remote printer configuration is correct, enter `END` at the prompt `What would you like to do (CHANGE, DELETE, or END):`.

```
Configuring the default remote printer for LPS client commands.
```

```
If you plan to use the LPR, LPQ and LPRM commands, you may define a default
remote printer. LPS uses this printer if users do not specify a remote
printer in the LPR, LPQ, or LPRM command.
```

```
Currently there is no default remote printer defined.
```

```
Do you want to define the default remote printer [YES]: 
```

```
Enter the host name for the remote printer []: ALPHA
```

```
Enter the remote printer on alpha []: SYS$PRINT
```

```
The current configuration for default remote printer is:
```

```
What would you like to do (CHANGE, DELETE, or END): END
```

Configure the LPS Client OpenVMS Print Queues

LPS lets you use the OpenVMS `PRINT` command to print on a remote printer. You can configure local LPS OpenVMS queues to send print jobs to remote printers attached to a remote host running LPD.

CNFNET Steps

To configure LPS client print queues (see the below example):

1. For a first-time configuration, this message will appear:

```
Currently there is no print queue configured
```

However, if CNFNET recognizes a `PRINTCAP` file on the system, the message `A printcap file has been found on this system` appears. You have the option to use information in this file at the prompt

```
Do you want to base the symbiont configuration on printcap [YES]:
```

See Chapter 15 in the *Management Guide, Managing Print Services*, for details on the `PRINTCAP` database.

2. If you are not using the `PRINTCAP` database, enter **Y** at the prompt asking if you want to configure print queues.

3. Enter the local LPS queue name; for example: `DOC$PRINT`.

4. Enter the remote hostname you want associated with the queue; for example: `SIGMA`.

5. Enter the remote printer name associated with the remote host; for example: `DOC__PRINTER`.

6. Enter **Y** or **N** at the prompt asking if users can override the remote printer specification.

7. Respond to the prompt asking you to select the formatting options;

- Enter `LPD` (the default) to enable the LPS OpenVMS print queue to send files to the remote LPD server for formatting.
- Enter `vms` to enable the LPS OpenVMS queue to support the `/FORM` qualifier and formatting on the local print queue.

8. Responding to the additional qualifiers prompt is optional. Additional qualifiers refer only to qualifiers available with the OpenVMS `INITIALIZE/QUEUE` command.

For example, to implement OpenVMS device control, enter:

```
/LIBRARY=LN03DEVCTL
```

This qualifier specifies the device control modules within the device control library. Depending on your formatting configuration, this means the LPS OpenVMS queue either applies the device control information to the local device or to the remote device.

9. Enter **Y** or **N** at the prompt asking if you want to configure another print queue.

10. Respond to the prompt asking if you would like to ADD, CHANGE, DELETE, or START a queue, or END configuring the print queues; for example: END.

Use the START option only if LPS is already running. This is useful for restarting a single queue when changing its configuration or starting the newly created queue without stopping any existing ones.

Configuring LPS OpenVMS Print Queue

You can configure an LPS OpenVMS print queue to print files on a printer attached to a remote host running LPD. Use the OpenVMS PRINT command to send print jobs to this queue.

You must name one or more local OpenVMS print queues for LPS to use. For each local OpenVMS print queue, you must also specify the:

- Associated remote host name
- Name of the printer attached to the remote host

You can also specify additional qualifiers used when LPS initializes the print queue. Please refer to the OpenVMS documentation on the INITIALIZE/QUEUE command for the qualifiers you can use.

Currently there is no print queue configured.

Would you like to configure print queues [NO]: **Y**

Specify the OpenVMS print queue name for LPS: **DOC\$PRINT**

Specify the remote host name: **SIGMA**

Specify the remote printer on sigma: **DOC PRINTER**

May users override the remote printer specification [NO]: **Return**

Select formatting option (VMS/LPD) [LPD]: **Return**

Specify additional qualifier []: **Return**

Do you want to configure another queue [NO]: **Return**

The currently configured queues are:

OpenVMS Print Queue	Remote Host	Remote Printer	OvR	Fmt
-----	-----	-----	---	---

```
DOC$PRINT          sigma          doc_printer      NO    LPD
```

You may enter:

```
ADD      To add a new print queue(s)
CHANGE   To change an existing print queue(s)
DELETE   To delete an existing print queue(s)
START    To (re)start print queue(s)
END      To end configuring the print queue(s)
```

```
What would you like to do (ADD, CHANGE, DELETE, START or END): END
```

Configure LPS for Batch Startup

You can select to start LPS on a batch queue, which greatly reduces the time of TCPware startup if there are many LPS print queues defined.

To start LPS as a batch job (see the below example):

1. Enter **Y** at the prompt asking if you want to start LPS on a batch queue. The default is NO.
2. Enter the batch queue name. The default is SYS\$BATCH.

STARTNET now submits the LPS portion of TCPware startup to the specified batch queue. The LPS startup log file, TCPWARE:LPSSTART.LOG, retains the LPS batch startup information.

Go to the next section to configure the LPD Server.

```
Do you want to start LPS on a batch queue [NO]: Y
Enter the batch queue name for the LPS startup [SYS$BATCH]: Return
```

When this selection is made, STARTNET will submit LPS portion of startup to the specified batch queue. Log of the startup will remain in TCPWARE:LPSSTART.LOG.

Configure the LPD Server

If you configure the Line Printer Services (LPS), you may also want to configure the LPS server (LPD). LPD allows remote users to send files to print queues on your OpenVMS host. To configure the LPD server (see the below example):

1. Enter **Y** at the prompt asking if you want this host to support the LPD server. If you accept the default NO, go to the next section.

2. Enter **Return** or **N** at the prompt if you do not want the LPD server to use batch queues. If you want to use batch queues, enter **Y**.

Note that:

- LPD places the jobs it receives into ordinary OpenVMS print queues. You must define these queues on your local host before anyone can use LPD. TCPware does not set up these queues and you cannot define them in CNFNET. Instead, see your OpenVMS documentation for instructions.
- The local LPD works properly only if the system manager on the remote client with which it communicates properly configured it to send print jobs.

Users at remote clients need to specify names of OpenVMS print queues as printers. On many UNIX systems, the `/etc/printcap` file defines this information. See your client documentation for details.

Note: STARTNET does not define the `TCPWARE_LPD_qname_PARAMETER`, `TCPWARE_LPD_qname_FORM`, and `TCPWARE_LPD_qname_QUEUE` logicals. You should define these system logicals in the system startup file.

Configuring the LPD Server

Do you want this host to support the LPD server [NO]: **Y**

Do you want the LPD server to allow batch queues to be used [NO]: **Return**

Build the LPD Server Access File

The LPD access file determines which remote hosts can use the LPD server and maps remote users to OpenVMS usernames.

Prepare

To build the LPD access file, you need the name of the:

- Remote host allowed access to the print server.
- Remote user on the remote host that you want to be allowed access.
- Local user for the remote user on the print server.

- Default local user for the remote users whose hosts are defined in the LPD access file but whose remote usernames are not mapped to a specific OpenVMS username.

CNFNET Steps

The LPD server requires an LPD access file. You can build this file now or later (see the example below):

1. Enter **Y** at the prompt asking you if you want to build the LPD access file now. If you enter **N** or press **Return**, continue with the next section.
2. Enter the name of the remote host allowed access; for example: ALPHA.
3. Enter the remote user on the remote host allowed access. For example, the remote user on ALPHA: KOENIG. Use upper- or lowercase letters according to how the remote host defines the name.
4. Enter the local username for the remote user at the remote host. For example, KOENIG at ALPHA: LUNA. The system converts this username to uppercase, regardless of how you enter it.
5. Repeat steps 3 and 4 for each remote user permitted to print files on printers attached to your OpenVMS host. After you enter all usernames for a remote host, press **Return**.
6. Press **Return** at the remote host prompt to stop entering information.
7. Enter a default OpenVMS username; for example, LPD_USER.

Remote users whose hosts are defined in the LPD access file but whose remote usernames are not mapped to a specific OpenVMS username use this default.

The LPD Server requires an LPD Access File, specifying:

- Which remote hosts are permitted to print files on this system.
- Remote-to-local OpenVMS username mappings.

Do you want to build the LPD Access File now [YES]: **Return**

Press return at the remote host prompt to stop entering information.

Enter the name of the remote host allowed access: **alpha**

When you have entered all users from alpha to be allowed local access, press return to specify the next remote host.

NOTE: Enter * to map all remote users to a local username.

Enter the remote user on alpha allowed access: **koenig**

Enter the local username for koenig at alpha: **luna**

Enter the remote user on alpha allowed access: **Return**

Enter the name of the remote host allowed access: **Return**

You need to define a default OpenVMS username for remote users whose hosts are defined in the LPD Access File, but whose remote usernames are not mapped to a local OpenVMS username.

Enter the default OpenVMS username: **lpd_user**

Note: Be careful when defining the default OpenVMS username. Remote users can submit batch jobs to your local OpenVMS host by printing to a batch queue (if enabled). To prevent unauthorized users from submitting batch jobs, avoid defining a username belonging to a privileged account (such as `SYSTEM`). Instead, create a special user account and use the `AUTHORIZE` utility to restrict access.

Configure the Miscellaneous Services

The miscellaneous services include the following:

TFTPD	Trivial File Transfer Protocol Server
CHARGEND	Character Generator Protocol Server
DAYTIMED	Daytime Protocol Server
DISCARDD	Discard Protocol Server
ECHOD	Echo Protocol Server
QUOTED	Quote-of-the-Day Server

IDENT	Identification Server (formerly Authentication Server)
TIME	Time Protocol

All these services can be enabled or disabled. They also have some options that can be configured.

CNFNET Steps

You can configure the Miscellaneous Services as part of the general CNFNET configuration or specifically as `@TCPWARE:CNFNET MISC` (see the below example):

1. At the prompt, enter **Y** if you want TFTP, or press **Return** or enter **N** if you do not want TFTP.
2. If you entered **Y** in step 1, you must also enter the TFTP root working directory. Enter a directory name or press **Return** to accept the default (`TCPWARE_ROOT: [TCPWARE.TFTP_WORK]`). (See the following subsection.)
3. For all other services, at the prompt, enter **Y** if you want to enable, or press **Return** or enter **N** if you want to disable service.

See the *Management Guide* for more information on the TFTP and other miscellaneous servers.

TFTP File Access

The TFTP protocol does not provide user authentication. Therefore, TFTP allows access only to files in the `TCPWARE_TFTP_ROOT` directory and its subdirectories. You usually define this system logical as `TCPWARE_ROOT: [TCPWARE.TFTP_WORK]`, but you can define it otherwise.

TFTP allows you to read, create, and write files in this directory. It creates files transferred in "netascii" mode as `STREAM_LF` formatted files, and files transferred in "binary" mode as fixed-length 512-byte record files.

Configuring the Miscellaneous Services:

Do you want the Trivial File Transfer Server (TFTP) [NO]: **Y**

You must specify the root working directory for TFTP.

Remote TFTP users have access only to the files within this directory (and its subdirectories).

NOTE: The TFTP protocol does not provide user authorization. Any remote users can access the files in this directory and its subdirectories. You may want to write protect this directory, if remote users will not need to create new files.

```
Enter the root working directory for
TFTPD [TCPWARE_ROOT:[TCPWARE.TFTP-WORK]]: Return

Do you want the CHARGEN Server (CHARGEND) [NO]: Return
Do you want the DAYTIME Server (DAYTIMED) [NO]: Return
Do you want the DISCARD Server (DISCARDD) [NO]: Return
Do you want the ECHO Server (ECHOD) [NO]: Return
Do you want the QUOTE Server (QUOTED) [NO]: Return
Do you want the AUTH Server (Identification) [NO]: Return
Do you want the TIME Service [NO]: Return

Do you want to restart the miscellaneous servers [NO]: Return
```

Configure the NFS Server

Because you need to install, configure, and start TCPware before you can set up the NFS server, you might want to enter **N** at the Do you want the NFS Server [YES] prompt. This lets you continue with CNFNET. You can always go back later to invoke the NFS server component configuration using

```
$ @TCPWARE:CNFNET NFS
```

Prepare to Set Up the Server

Before you set up the server:

1. Identify the NFS users on the network that should have access to the OpenVMS server.

Obtain the User ID (UID) and Group ID (GID) numbers for each NFS user. For UNIX system users, obtain the UIDs and GIDs from the `/etc/passwd` file (the below example). For PC users, assign any UIDs and GIDs that do not conflict with existing users.

For an OpenVMS user, assign a UID and GID that does not conflict with UNIX users. You can take the UIDs and GIDs from the user UIC [*gid, uic*]. Any method is acceptable if it generates unique UID/GID pairs for each user.

2. Identify which OpenVMS directories and files the NFS users need to access. You should export only the necessary directories and files.
3. Match the NFS users with the valid usernames of OpenVMS accounts that can use the required directories and files.

In some cases, you need to create new OpenVMS accounts to accommodate the NFS users. You must update your `SYSUAF.DAT` file. (See your OpenVMS documentation.)

Set Up the Server

Setting up the NFS server consists of the following:

1. Add users to the PROXY database.
2. Add directories to the EXPORT database.
3. If necessary, create a spool directory.
4. Restart and test the server.

Add Users to the Server PROXY Database

To add users to the server PROXY database (see the example below):

1. Be sure the network is running.
2. Start TCPware.
3. Invoke NETCU by entering at the DCL prompt:

```
$ NETCU
```

Enter an `ADD PROXY` command for each NFS user and superuser. Use the format:

```
NETCU> ADD PROXY vms-username /UID=uid /GID=gid [/HOST=host]
```

The `vms-username` is the OpenVMS account to which you want to register an NFS user. Enter this name exactly as it is entered in the OpenVMS user authorization file (UAF).

If the username is not in the UAF, use the `AUTHORIZE` utility and add the user to the UAF. Do this before you add the username to the PROXY database.

Obtain the `uid` and `gid` values from client's `/etc/passwd` file (see the below example). Enter `UID=0 AND GID=1` for a superuser.

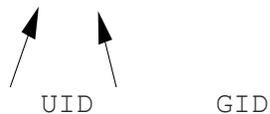
For PC users, assign any UIDs and give the same GIDs to users that need to have group access to files. Do not use wildcards.

Using the added `/HOST` qualifier with a host name value means that only the specified user on the specified host can use the server account.

4. Enter the `SHOW PROXY` command to confirm that you entered the information correctly.
5. Enter the `RELOAD PROXY` command if you added users to an existing `PROXY` database. This command ensures that new entries take effect by reloading the database on the server.

Obtaining UID and GID From UNIX `/etc/passwd`

```
> cat /etc/passwd
gimli:fmE3CZNyjKZt2:1000:15:Frodo Gimli:/usr/users/user:/bin/csh
pippin:TZ7u8CuAJRs5g:1134:15:Merry Pippin:/usr/users/pippin:/bin/csh
```



Adding Users to the Server `PROXY` Database

```
(Iota) $ RUN TCPWARE:STARTNET
(Iota) $ NETCU
NETCU>ADD PROXY SYSTEM /UID=0 /GID=1/HOST=SIGMA
NETCU>ADD PROXY GIMLI/UID=1000 /GID=15
NETCU>ADD PROXY PIPPIN /UID=1134 /GID=15
NETCU>SHOW PROXY
NFS PROXY Database V6.1 Copyright (c) Process Software

Username      UID      GID      Host(s)
-----
SYSTEM        0        1        SIGMA
GIMLI         1000     15
PIPPIN        1134     15

NETCU>RELOAD PROXY
NETCU>EXIT
```

Add Directories to the Server `EXPORT` Database

To add an entry to the NFS `EXPORT` database:

1. Be sure the network is up and running.
2. Enter an `ADD EXPORT` command at the `NETCU` prompt for each OpenVMS directory you want exported. Use the format:

```
ADD EXPORT "pathname" vms-directory
```

The *pathname* is the name the NFS client uses for the exported directory. Enclose the pathname in quotation marks (" "). The pathname is generally a UNIX-style name similar to an OpenVMS directory name.

Note: The case of the pathname is preserved so you must use the same case when using the NFS MOUNT command.

The *vms-directory* is the device and directory on the local OpenVMS system that you want to export.

When adding an EXPORT entry for the NFS client, export that entry using the /NOCONVERT qualifier to the NFSMOUNT command.

3. Enter an ADD EXPORT command for the spool directory if you use PCNFSD for printing.

If the spool directory is a subdirectory of a directory already listed in the EXPORT database, you do not need to create a separate entry.

Do not append the PC client host name to the end of the directory specification.

It is recommended that you enter the PC spool directory entry in the EXPORT database as follows:

```
ADD EXPORT "/spool" device:[directory] /NOCONVERT /RFM=UNDEFINED
```

4. Enter the SHOW EXPORT command to confirm your entries.

Note: You can also set additional export parameters, including specifying particular hosts, using ADD EXPORT qualifiers. See the ADD EXPORT command description in Chapter 2 of the *NETCU Command Reference, NETCU Commands*, for details on these parameters.

Create a Spool Directory

Complete this step only if you have PCs and plan to use the PC NFS protocol (PCNFS) for printing. Otherwise, proceed to the next section.

To create a spool directory:

1. Enter the `CREATE/DIRECTORY` command and create a spool directory on the server that the PCNFS server program (PCNFSD) can use for printing.
2. Create a subdirectory within the spool directory for each client allowed to use PCNFS for printing. The subdirectory name is the client's host name. You can skip this step if you choose to create subdirectories automatically (see *CNFNET Steps, Part 2*).

Note: You need to export the spool directory only. When you create the `EXPORT` database, be sure to include the spool directory. Do not include any subdirectories within the spool directory.

Adding an Entry to the Server EXPORT Database

```
NETCU>ADD EXPORT "/mnt/iota" DUA0:[000000]
%TCPWARE_NETCU-I-ADDPATH, added path /mnt/iota

NETCU>ADD EXPORT "/pcreports/spool" DUA0:[PCREPORTS.SPOOL] -
_NETCU>/NOCONVERT /RFM=UNDEFINED
%TCPWARE_NETCU-I-ADDPATH, added path /pcreports/spool

NETCU>SHOW EXPORT
NFS EXPORT Database V6.1 Copyright (c) Process Software

Path                Directory                Host(s)
----                -
/mnt/iota            DUA0:[000000]
/pcreports/spool    DUA0:[PCREPORTS.SPOOL]

NETCU>EXIT
```

Creating a Spool Directory and Spool Subdirectories

```
$ CREATE/DIRECTORY DUA0:[PCREPORTS.SPOOL]
$ CREATE/DIRECTORY DUA0:[PCREPORTS.SPOOL.DAISY]
$ CREATE/DIRECTORY DUA0:[PCREPORTS.SPOOL.ROSE]
```

CNFNET Steps, Part 1

To configure the NFS server in CNFNET:

1. Enter **Y** or **Return** at the prompt asking if you would like the NFS v3 server on this machine. To use the NFS v2 server, enter **N** to get to the NFS v2 prompt.
2. Press **Return** to accept the default access identifier.

Accepting the default of [] (null) means that you do not want to add any further access restrictions to the server than already exist. Entering a value further restricts access to the server.

3. Press **Return** to accept the default security mask value, or enter a new value.

Accepting the default of [] means that you do not want to add any security mask values. You should normally specify these options on a filesystem basis using appropriate `NETCU ADD EXPORT` command qualifiers. However, if you want these options on a system-wide basis, add their individual bit mask values and enter the result at the prompt. The options and their matching `ADD EXPORT` qualifiers are:

- Superuser mount - Only the superuser can mount filesystems
(/SUPERUSER_MOUNT)
- Explicit - Only filesystems explicitly exported can be mounted (/EXPLICIT_MOUNT)
- Mount proxy check - The UID/GID used in mount requests must exist in the PROXY database
(/PROXY_CHECK)
- Privileged port checks - All incoming NFS requests must originate from privileged ports
(/PRIVILEGED_PORT).
- Report all access allowed for files to the client (the server does all access checks)
(/SERVER_ACCESS)
- Allow PCNFS batch queue printing (no corresponding qualifier)
- Disable PCNFSD use of the intrusion database (no corresponding qualifier)
- Disable PCNFSD deletion of printed files (no corresponding qualifier)

Configuring NFS Server:

```
Do you want the NFS v3 Server (NFSDV3) [YES]: Return
```

For detailed information on NFS-OpenVMS Server parameters, refer to the TCPware for OpenVMS(R) Installation & Configuration Guide.

The access identifier parameter, `NFS_ACCESS_IDENTIFIER`, specifies the name of the rights identifier to be granted to all NFS users. This parameter is optional.

To remove a previously entered identifier, enter `*`.

Enter the access identifier []: **Return**

The security mask parameter, `NFS_SECURITY`, controls access to the OpenVMS system. Note that these options should normally be specified on a file system basis (rather than a global basis) using the appropriate `NETCU ADD EXPORT` command qualifiers (as indicated below) if applicable.

Bit Mask	Meaning when set
1	Superuser mount. Only the superuser is allowed to mount file systems (<code>/SUPERUSER_MOUNT</code>).
2	Explicit mount. Only file systems explicitly exported can be mounted (<code>/EXPLICIT_MOUNT</code>).
4	Mount proxy check. The UID/GID used in mount requests must exist in the PROXY database (<code>/PROXY_CHECK</code>).
8	Privileged port check. All incoming NFS requests must originate from privileged ports (<code>/PRIVILEGED_PORT</code>).
16	Report all access allowed for files to client (server does all access checks) (<code>/SERVER_ACCESS</code>).
32	Allow PCNFS batch queue printing.
64	Disable PCNFSD use of the intrusion database.
128	Disable PCNFSD deletion of printed files.

To specify the security mask, add up all the bit mask values for the types of security you want provided.

Enter the security mask []: **68**

CNFNET Steps, Part 2

During the second part of this NFS server configuration, you need to respond to the logging class and configuration prompts.

If you are configuring the NFS server for the first time, use the default values to get the server up and running quickly. You can change the parameter values later.

Enter **Y** or **Return** to accept the default logging class mask value or enter a new value.

2. After CNFNET displays the current value of each parameter, enter Y or Return if the configuration is correct.

If you enter **N**, CNFNET repeats the prompts for each parameter.

The logging class mask parameter, `NFS_LOG_CLASS`, controls the types of information written to the log file.

Bit Mask	Meaning when set	Comments
1	Warnings	Error recovery messages
2	Mount Requests	Mount call messages
4	General	General operation messages
8	Security	Security violation messages
16	NFS Errors	NFSERR_IO messages

To specify the logging class mask, add up all the bit mask values for the types of information you want logged. The value -1 logs all classes.

Enter the logging class mask [-1]: **Return**

Automatically create subdirectories for each client [NO]: **Y**

These are the NFS-OpenVMS Server configuration parameters you selected:

```
Type:                Network File System Server
Access Identifier:   (none)
Security Mask:      68 = Proxy, Disable Intrusion
Logging Class Mask: -1 = Warnings, Mounts, General, Security, Errors
PCNFSD enable:     1 (YES)
Spool directory:    /pcreports/spool(autocreate subdirectories)
```

Is this configuration correct [YES]: **Return**

Start and Restart the NFS Server

To start the NFS server:

1. Enter @TCPWARE: STARTNET NFS at the DCL prompt.
2. Enter @TCPWARE: SHUTNET NFS at the DCL prompt, if the server is running.
3. Enter @TCPWARE: STARTNET NFS at the DCL prompt.

```
$ @TCPWARE: STARTNET NFS
Starting NFS -OpenVMS Server...
%RUN-S-PROC_ID, identification of created process is 00000060
%RUN-S-PROC_ID, identification of created process is 00000061
.
.
.
$
```

Test the NFS Server

To test the server:

1. Access an NFS client authorized to use this server.
2. On the NFS client, enter a mount command for one of the exported directories. Refer to the directory by the pathname assigned in the EXPORT database.
3. For a UNIX client, enter the `cd` command and change the directory to the one you specified in the mount command, for example: `cd /iota`
4. For a UNIX client, issue the `ls` command to show the contents of this directory. The NFS server is installed and configured properly if this command does not cause the system to display an error message.

See below for sample output of the `ls` command.

5. Check the log file to make sure the NFS server is running and that status messages do not indicate problems.

```
$ TYPE TCPWARE:NFSERVER.LOG
```

If problems arise, see the *Troubleshooting* section in Chapter 14, *Managing NFS Server*, of the *Management Guide* for possible solutions.

If you need to modify the PROXY or EXPORT database, use the commands available through NETCU.

Note: The server updates the PROXY database dynamically only if you use the `/SERVER` qualifier with the `ADD PROXY` command or use the `RELOAD PROXY` command in NETCU. Also use the `RELOAD PROXY` command in to reload the database every time you modify the system authorization file (SYSUAF).

```
$ TELNET SIGMA
.
.
.
sigma.example.com# mount iota:/mnt/iota /iota
sigma.example.com# cd /iota
sigma.example.com# ls
backup.sys      contin.sys      lpsCLIENT      sqlsrvSERVER    syslost
```

```
badblk.sys      corimg.sys      notesSERVER    sys0            sysmaint
badlog.sys      engineering     nsc            sys293          user
bitmap.sys      indexf.sys      rdmRUJ         syscommon       vmsCOMMON
clipart         lci            root           sysexec         volset.sys

sigma.example.com#
```

Note: NFS v3 server - Testing the asynchronous write functionality has revealed a problem with some v3 clients not recognizing failed asynchronous write requests. The writes may fail due to a full UDP buffer on the server. Process Software recommends increasing the UDP buffer size on the server if you are using a v3 client. We have tested successfully with a buffer size of 25:

```
NETCU> START/UDP/UNSOLICITED_RECEIVE_LIMIT=25
```

Configure the Network Time Protocol

The Network Time Protocol (NTP) synchronizes timekeeping among a set of distributed time servers and clients.

CNFNET Steps

You can configure NTP as part of the general CNFNET configuration or specifically as
@TCPWARE:CNFNET NTP

Enter **Y** or **Return** at the prompt asking you if you want to use the TCPware NTP daemon. This creates the NTP server. (If you do not want NTP, enter **N**.)

Configuration File

To use NTP, you must create the NTP configuration file, TCPWARE:NTP.CONF. To create the most basic version of this file:

1. Determine one, or preferably two or more, NTP time servers on your network.
2. Identify NTP-supporting hosts with which you regularly exchange data where accurate time coordination is an issue.

3. Configure each NTP time server as a `server` and each participating client host as a `peer` in the `NTP.CONF` file.

If your time servers were 192.168.67.1, 192.168.67.2, and 192.168.67.3, you could include the entries shown below in host 192.168.67.100's `NTP.CONF` file:

```
server 192.168.67.1
server 192.168.67.2
server 192.168.67.3
peer   192.168.67.101
peer   192.168.67.102 ...
```

You can also designate master clocks and local masters for more advanced configuration.

For details, see the *Management Guide, Chapter 10, Network Time Protocol (NTP)*.

Configuring the Network Time Protocol (NTP) Daemon:

Kerberos is installed on this system. For Kerberos to work correctly, use the Network Time Protocol (NTP) Daemon to synchronize the clock on this system with the other systems that are also using Kerberos.

Do you want to use the TCPware for OpenVMS NTP Daemon [YES]: **Return**

You may set the parameter `WAYTOOBIG`, which defines the number of seconds difference between the system clock and the reference clock past which no clock adjustment will be performed by the NTP daemon.

While you may set this to any numeric value you wish, you should realize that setting it to lower than 4000 may interfere with NTP attempting to automatically adjust your system clock for Daylight Savings Time (if your timezone rule calls for that).

Enter value for `WAYTOOBIG` [289985]: **4000**

Do you want to restart the Network Time Protocol Daemon [NO]: **Y**

Configure POP3

The Post Office Protocol Version 3 (POP3) server lets remote PC systems retrieve mail in your system's inbound mailbox.

CNFNET Steps

You can configure the POP3 server as part of the general CNFNET configuration or specifically as @TCPWARE:CNFNET POP3 (see the below example):

1. Enter **Y** or **Return** at the prompt asking if you want to enable the TCPware POP3 server. If you do not want POP3, enter **N**.
2. If you enter **Y**, enter the maximum number of new mail messages to return per connection to the remote PC. The default is 32. Either accept the default by pressing **Return** or enter another number.
3. Determine the debug logging level for the connection:
 - Select ERROR if you want to log errors only
 - Select INFO if you want to log informational messages and errors
 - Select THREAD if you want detailed thread logging, informational messages, and errors
 - Select DEBUG if you want complete debug logging

You can enter just the first letter of your choice at the prompt. The default is **I**.

4. If you want to execute a MAIL PURGE /RECLAIM operation, enter **Y**.
5. CNFNET displays the POP3 configuration parameters you set. Respond whether this is correct by pressing **Return** for YES, or entering **N** for NO. If NO, return to step 2 to reenter the parameters.

For more information on POP3, see the *Management Guide*, Chapter 17, *Managing Mail Services*, the *POP3 Server* section.

```
Configuring The Post Office Protocol V3 (POP3) Server:
```

```
For detailed information on the following parameters, refer to the TCPware  
for OpenVMS Management Guide.
```

```
Do you want to enable the POP3 server [YES]: Return
```

```
Enter Maximum number of new mail messages to return per connect [32]:  
Return
```

```
Determine the logging level, Options are:
```

```
ERROR - Errors only  
INFO - Information messages and Errors  
THREAD - Detailed Thread logging, information messages and Errors  
DEBUG - Complete Debug logging
```

```
You may enter the first character of your choice.
```

```
Enter your choice (Error, Info, Thread, Debug) [INFO]: Return
```

```
Do you want to execute a MAIL PURGE/RECLAIM operation after use [YES]:
```

```
Return
```

```
The POP3 server is configured as follows:
```

```
Maximum number of new mail messages to return : 32  
Logging Level : INFO  
Do a MAIL PURGE/RECLAIM : YES  
Is this correct [YES]: Return
```

Configure the PWIPDRIVER

CNFNET Steps

You can enable the PWIPDRIVER for PATHWORKS and DECnet/OSI as part of the general CNFNET configuration or specifically as @TCPWARE:CNFNET PWIP:

Press **Return** or enter **N** at the prompt asking if you want to enable the PWIPDRIVER. The default is YES.

If you do not want the PWIPDRIVER, enter **N**.

```
Configuring the PWIPDRIVER:
```

```
The PWIPDRIVER is *required* by Pathworks and DECnet/OSI over TCP/IP.
```

```
Do you want to enable the PWIPDRIVER [YES]: Return
```

Configure the Berkeley R Commands

The Berkeley R commands consist of:

- Three R services (login, shell, and exec)
- Three clients (RLOGIN, RSH, and RMT)

CAUTION! Make sure that you are familiar with the R commands and authorization methods before starting the R services. Failure to do so may inadvertently expose you to a security risk. (See the *Management Guide*, Chapter 16, *Managing R Commands*.)

Configure the R Services

You can enable the Berkeley R commands as part of the general CNFNET configuration or specifically as

```
$ @TCPWARE:CNFNET RCMD
```

First, determine the type of R Service you want to enable: login, shell, or exec

Read the explanations for each on the CNFNET screen.

Proceed directly to the next section to configure the R commands clients.

Configuring the Berkeley R Commands:

The Berkeley R Commands have 2 parts: services and clients.

login service allows remote users to log in to this system using the BSD RLOGIN protocol. Authorization is done using equivalence files alone, or with both equivalence files and the user having to enter a password.

shell and exec services both allow remote users to execute a single command on this system. The difference is in the authorization method used. shell uses equivalence files while exec uses explicit username/password strings.

All services can, optionally, use Service Access Lists to further restrict remote access.

There are 3 clients: RLOGIN, RSH, and RMT.

You have the option of making the services available. You should be familiar with the R Commands and the authorization methods before starting the services to insure that you do not inadvertently expose your system to a security risk.

Configure RLOGIN, RSH, and RMT

The R commands include an RLOGIN client, RSH client, and RMT client. To continue configuring the R commands:

1. Press **Return** if you want to activate the login service, or enter **N** if you do not.

2. Specify the type of login authorization you want. The selections are NORMAL or SECURE. Press **Return** if you want to accept NORMAL, the default value. Enter SECURE if you want SECURE login authorization. SECURE login authorization requires a .RHOSTS file entry on the system.

See the *Host Equivalence Files* section of Chapter 16, *Managing R Commands*, in the *Management Guide* for details.

The login service allows remote users to log in using the BSD RLOGIN protocol.

3. Press **Return** if you want to activate the shell service, or enter **N** if you do not. (The Remote Copy Program (RCP) requires this service.)
4. Press **Return** if you want to activate the exec service, or enter **N** if you do not. (The RCP command also requires this service.)
5. Press **Return** if you want to install the RLOGIN image, or enter **N** if you do not.
6. Press **Return** if you want to install the RSH image, or enter **N** if you do not.
7. Press **Return** if you want to install the RMTSETUP image for RMT, or enter **N** if you do not.

Host Equivalence File

Determine the method you want to use for host equivalence. Once you start TCPware, remote users cannot access the R services until you set up the host equivalence data in the HOSTS.EQUIV or .RHOSTS file:

- The HOSTS.EQUIV file defines which remote hosts or users can access the server host. The HOSTS.EQUIV file is in the TCPWARE directory and is analogous to the /etc/hosts.equiv file in UNIX.

Place the HOSTS.EQUIV file in either the TCPWARE_COMMON: [TCPWARE] or TCPWARE_SPECIFIC: [TCPWARE] directory, depending on your needs.

- The .RHOSTS file lets users have remote access to accounts beyond what the HOSTS.EQUIV file specifies. The .RHOSTS file is in the user's login directory and is analogous to the UNIX ~/.rhosts file.

To create a .RHOSTS file, use a text editor on the TCPware host to create a SYS\$LOGIN: .RHOSTS file in your login directory.

```
Do you want to activate login service [YES]: Return
```

```
There are 2 methods of authorization available for login service.
```

NORMAL: Uses equivalence files to authorize remote users, and allows remote user to try a username/password if there isn't an equivalence file match.

SECURE: Uses equivalence files, and if there is a match, requires the remote user to enter the account's password correctly. If there is no equivalence file match, access is denied.

Which type of login authorization (NORMAL, SECURE) [NORMAL]: **Return**

Do you want to activate shell service [YES]: **Return**

Do you want to activate exec service [YES]: **Return**

The RLOGIN, RSH, and RMTSETUP (without the /PASSWORD qualifier) commands require SYSPRV privilege to bind to reserved TCP ports which are needed for them to work correctly. In a BASIC configuration, the executable images are INSTALLED with SYSPRV privilege to allow all users on your system to make use of them. In this FULL configuration, you have the option of restricting the use of these 3 commands.

Answering "NO" to the following questions restricts use of the indicated command to users with either SYSPRV or BYPASS privilege only.

Answering "YES" allows general use of the command.

Do you want to INSTALL the RLOGIN image [YES]: **Return**

Do you want to INSTALL the RSH image [YES]: **Return**

Do you want to INSTALL the RMTSETUP image [YES]: **Return**

Note: It is advisable, if you want automatic startup of this component, to include the \$ SET NOON line in your SYLOGIN.COM file to prevent the component from failing should there be an error in the file.

Configure SMTP

Follow these steps to configure SMTP. Refer to the *TCPware Management Guide*, Chapter 17, and the *TCPware Network Control Utility (NETCU) Command Reference*, Chapter 1, for information on the TCPWARE CONFIGURE /MAIL command.

CNFNET Steps

You can configure SMTP as part of the general CNFNET configuration or specifically as

```
$ @TCPWARE:CNFNET SMTP
```

1. Enter whether you want to use the SMTP Mail Transfer Agent. The default is NO.
2. Enter the username of the local postmaster. Press **Return** to accept the default ([SYSTEM]).

One user on this system must act as the local postmaster. This person receives mail sent to the postmaster. The person's username must always be valid while SMTP operates.

Configuring SMTP-OpenVMS:

For detailed information on the following parameters, refer to the TCPware for OpenVMS Management Guide.

Do you want to use the SMTP Mail Transfer Agent? [YES]: **Return**

One user on this system must act as the local postmaster. This person will receive mail sent to the postmaster. The person's username must always be valid while SMTP-OpenVMS is operating.

Enter the username of the local postmaster [SYSTEM]: **Return**

Do you want to enable the SMTP RFC2789 MIB [Yes]? **Return**

Do you want to enable SMTP accounting [Yes]? **Return**

Name of the host that will run the accounting collection program
[localhost]: **Return**

Port number that accounting collection program listens on []: **Return**

For further configuration options, please see the procedure described in the TCPware for OpenVMS Installation & Configuration Guide to configure SMTP-OpenVMS

Configure SNMP Services

SNMP is the Simple Network Management Protocol. Activate the SNMP agent only if your network has an SNMP client (network management station).

CNFNET Steps

You can configure the SNMP services as part of the general CNFNET configuration or specifically as `@TCPWARE:CNFNET SNMP:`

1. Enter **Y** if you want to activate the SNMP agent on your host.
2. You might want to configure the SNMP Multiplexing (SMUX) Service. If so, activate it on the host by typing **Y** at the prompt. Also, include the relevant peer names in the `SNMPD.CONF` file (see *Configuration File*) using the given syntax.

Note: Enabling SMUX when there are no SMUX subagents to use it can interfere with walking of the SNMP management base due to the SMUX MIB returning `NoSuchName` when no subagents exist. SMUX is a historical protocol, and should not be enabled unless there are subagents that will be using it. Specific items in the SNMP management base that appear after the SMUX MIB can still be queried when they are accessed from the start of their management base.

3. You might want to configure the SNMP Agent X Service. If so, activate it on the host by typing **Y** at the prompt. Also, include the relevant peer names in the `SNMPD.CONF` file (see *Configuration File*) using the given syntax. You need Agent X for SMTP and FTP Statistics as well as for using HP's Insight Manager's subagents.

4. You might want to configure an SNMP subagent on your host. A subagent serves private Management Information Bases (MIBs) available through an application programming interface (API).

External users wanting to have their private MIBs served by TCPware's SNMP agent should develop a shareable image that exports the APIs in the private MIBs in addition to the routines needed to access the MIB variables.

Enter **Y** if you want to configure SNMP subagents on your host.

The subagent must be an installed shareable image and export the routines `SnmExtensionInit`, `SnmExtensionQuery`, and `SnmExtensionTrap` as universal symbols. If you have more than one subagent, enter each name when prompted.

While entering the name, do not enter the `.EXE` extension. For example, if you built and installed a shareable image called `PRIVATE_MIB.EXE` for a subagent, enter `PRIVATE_MIB` as the name of the shareable image when prompted.

Enter **Return** by itself to end the subagent configuration.

See the *Programmer's Guide*, Chapter 10, *SNMP Extendible Agent API Routines*.

Configuration File

TCPware normally uses default values for SNMP Services. To customize the configuration (such as by adding SMUX or AgentX peers), edit the `TCPWARE_COMMON:SNMPD.CONF` configuration file.

See the *Management Guide*, Chapter 7, *Managing SNMP Services*, for information on the `SNMPD.CONF` file.

After editing the SNMP configuration file, you need to stop and restart the agent so the changes can take effect. Follow these steps:

1. Log in as the system manager.
2. Stop the SNMP agent process by entering:

```
$ @TCPWARE:SHUTNET SNMP
```

3. Start the SNMP agent process by entering:

```
$ @TCPWARE:STARTNET SNMP
```

Configuring the SNMP Agent:

```
SNMP is the Simple Network Management Protocol. If you activate the SNMP agent on this host, the agent will start up when you start up the network and will respond to queries. Answer YES to the next prompt only if your network has an SNMP client (network management station).
```

```
Do you want to activate the SNMP agent on this host [NO]: Y
```

Configuring the SNMP SMUX Service:

```
You have the option of enabling the SNMP server's SMUX Service. SMUX (RFC 1227) is an SNMP subagent protocol.
```

```
Warning: If you enable SMUX support, the SNMP server will only accept SMUX connections from hosts explicitly listed in the SNMPD.CONF file. Make sure to configure this file appropriately. Refer to the TCPware Management Guide, the Managing SNMP Services chapter.
```

```
Do you want to activate the SNMP SMUX service on this host [NO]: Return
```

Configuring the SNMP AgentX Service:

You have the option of enabling the SNMP server's AgentX Service. AgentX (RFC 2741) is an SNMP subagent protocol.

Warning: If you enable AgentX support, the SNMP server will only accept AgentX connections from hosts explicitly listed in the SNMPD.CONF file. Make sure to configure this file appropriately. Refer to the TCPware Management Guide, the Managing SNMP Services chapter.

Do you want to activate the SNMP AgentX service on this host [NO]: **Return**

Configuring an SNMP subagent(s):

An SNMP subagent is a shareable image that serves a private MIB. If the master SNMP agent receives a query for a variable in the private MIB, it will hand that query to the subagent for resolution.

Each subagent must be a shareable image, and conform to the SNMP Extendible Agent API Routines interface defined in the TCPware Programmer's Guide.

Answer YES to the next prompt only if this installation has SNMP subagents.

Do you want to configure subagent(s) on this host [NO]: **Y**

Please enter the name of one subagent per prompt, until finished. When finished press <Return> at the prompt to signify the end. Please do not enter the ".EXE" extension.

Enter the name of the shareable image without .EXE: **SNMP_AGENT1_SHR**

Enter the name of the shareable image without .EXE: **SNMP_AGENT2_SHR**

Enter the name of the shareable image without .EXE: **Return**

Configure the SSH Utility

SSH is the Secure Shell protocol. TCPware provides support for both SSH Version 1 protocol and SSH Version 2 protocol.

Please note that in addition to the configuration performed via CNFNET as described below, there are configuration files for both the SSH1/SSH2 servers and SSH client which must be modified as appropriate to meet the security requirements of your organization. Refer to chapters 25 and 26 of the *TCPware Management Guide* for details on the configuration files.

CNFNET Steps

You can enable TCPware's SSH utility as shown below.

```
$ @TCPWARE:CNFNET SSH
```

Configuring SSH-OpenVMS

For detailed information on the following parameters, refer to the TCPware for OpenVMS Management Guide.

TCPware supports both SSH1 and SSH2 servers. You may configure TCPware to support either SSH1 servers or SSH2 servers, or both. Note that the choice of TCPware servers has no impact on the TCPware SSH client, which supports both SSH1 and SSH2 remote servers.

Do you want to enable the SSH1 server[NO]? **YES**

Do you want to enable the SSH2 server[NO]? **YES**

For SSH1, you must specify the number of bits in the RSA key. The range is 512 to 32768 bits, but keys longer than 1024 are generally not much safer, and they significantly increase the amount of CPU time consumed by key generation when the SSHD_MASTER process is starting.

Enter the number of bits in the RSA key[768]: **Return**

You may specify an alternate configuration file for the SSH1 server. If you have already specified an alternate config file, enter a single space and hit RETURN at the prompt to reset it to the default file name.

Enter an alternate SSH1 configuration filename[: **Return**

You may specify an alternate configuration file for the SSH2 server. If you have already specified an alternate config file, enter a single space and hit RETURN at the prompt to reset it to the default file name.

Enter an alternate SSH2 configuration filename[: **Return**

Specify the level of debug for the SSH1 and SSH2 servers.

For SSH1, any non-zero value will turn on debug, but there is no "degree of debug."

For SSH2, this is a value from 0 to 50, where zero is no debug and 50 is the maximum level of debug. Note that at levels exceeding debug level 8, there may be a substantial impact on SSH2 server (and possibly, the system, too) performance due to the amount of information logged.

Enter the debug level[0 50, 0]: **Return**

For SSH1, you may enter the name of an alternate RSA host key file. If you have already specified an alternate host key file, enter a single space and hit RETURN at the prompt to reset it to the default file name.

Enter an alternate SSH1 public server host key file []: **Return**

Specify the time in seconds after which the server private key is generated. This is only done for SSH1 sessions.

Enter the key regeneration time [3600]: **Return**

You may specify the number of seconds a user has to enter a password during user authentication (default = "dval" = 600). In addition, you may allow this to default to the value used by OpenVMS when a user is logging into a non-SSH session. To specify an infinite wait time, enter 0 for the timeout value.

Do you want to change the default login grace time [NO]? **Return**

Specify the port for the SSH server to listen on, if you wish to use a port other than the default port of 22.

Enter port to use[22]: **Return**

You may disable listening for server connections on an IPV4 socket or on an IPV6 socket. The default is to listen on both IPV4 and IPV6 sockets.

NOTE: you must have either IPV4 or IPV6 (or both) listen sockets enabled.

Do you want to disable listening on an IPV4 socket [NO]? **Return**

Do you want to disable listening on an IPV6 socket [NO]? **y**

Do you want any messages logged by the SSH server at all [YES]? **Return**

Do you want verbose logging by the SSH server [NO]? **Return**

You may specify the maximum number of concurrent SSH sessions to be allowed on the server. This is the total of both SSH1 and SSH2 sessions. The default is 1000 sessions.

Enter maximum number of concurrent SSH sessions [1-1000, 100]: **Return**

You may permit the server to log a brief informational message when a user is allowed or denied access to a system.

- For SSH1 connections, an ACCEPT or REJECT event will be simply dependent upon if a user could connect based on the ALLOWGROUP/DENYGROUP settings in the configuration file SSH_DIR:SSHD_CONFIG. The message will be of the form:

```
<date><time> SSH1 (accepted) from [192.168.0.1,111] (my.server.com)
```

- For SSH2 sessions, an ACCEPT or REJECT event will be logged when the user is either successfully authenticated or fails authentication. The message will be of the form:

<date><time> SSH2 (accepted) from user "foo" at [192.168.0.1,111]
(my.server.com)

You may specify the name and location of the log file to record accepted and/or rejected connections. If you simply hit RETURN, this information will be logged to OPCOM as opposed to a disk file.

By default, this file will be in the SSH_DIR: directory. You may override this by specifying a complete filename, including the directory specification; or by specifying a logical name that translates to a full filename specification.

Do you want to log accepted sessions [NO] **Return**
Do you want to log rejected sessions [NO] **Return**

In OpenVMS, users with passwords that have expired because the SYSUAF PWDLIFETIME value has been exceeded are allowed to log into the system, and are then forced to change their password. The SSH1 protocol does not allow for that condition. Answer "YES" to the following question if you wish to allow users with expired passwords to still log into the system. They WILL NOT be forced to change their password.

Note that the SSH2 protocol is not restricted as the SSH1 protocol is; changing of expired passwords, save for pre-generated passwords, is performed by many SSH2 clients (including the TCPware client).

Do you want to allow users with preexpired passwords to log in [YES]?
Return

The SSH1 protocol does not permit the display of the contents of SYS\$ANNOUNCE logical or file prior to a user logging in. Answering "Y" to the next question will cause the TCPware SSH1 client to display the contents of SYS\$ANNOUNCE after user authentication is completed but before the contents of SYS\$WELCOME are displayed.

Do you want to display SYS\$ANNOUNCE [YES]? **Return**

When generating user keys, a passphrase may be used to further protect the key. No limit is normally enforced for the length of the passphrase. However, you may specify a minimum length the passphrase may be.

What you want the minimum passphrase length to be for SS1 [0-1024, 0]? 10

What you want the minimum passphrase length to be for SSH2 [0-1024, 0]? 10

Do you want to restart the SSH-OpenVMS Server [NO]: **YES**

Shutting down the SSH-OpenVMS Server ...

Starting the SSH-OpenVMS Server ...

```
%RUN-S-PROC_ID, identification of created process is 20800104
$
```

Configure the TALK Utility

The TALK utility allows you to exchange messages you type at your terminal window with another local or remote user.

CNFNET Steps

You can enable TCPware's TALK as part of the general CNFNET configuration or specifically as @TCPWARE:CNFNET TALK.

```
$ @TCPWARE:CNFNET TALK
```

Configuring TALK Utility:

The TALK client/server operates with other "NTALK" clients and servers. The "NTALK" protocol was introduced in BSD V4.3; the version of TALK shipped with TCPware is not compatible with TALK utilities based on earlier versions of BSD.

In order for users to use TALK, the TALKD server must also be enabled.

Do you want to enable the TALKD server [Y]: **Return**

Configure TELNET

CNFNET Steps

You can configure TELNET as part of the general CNFNET configuration or specifically as @TCPWARE:CNFNET TELNET (see the below example).

Specify at the prompt how many TELNET listeners you want on this system. Set this number to **1** unless you expect a lot of incoming TELNET activity. This number does not limit the number of incoming TELNET sessions. The number of sessions is limited only by the available system resources (such as the maximum number of processes).

Configuring TELNET-OpenVMS:

Determine how many Server-TELNET listeners you want on this system. Set this number to 1 unless you expect a lot of incoming TELNET activity. This number does not limit the number of incoming TELNET sessions. The number of sessions is limited only by the available system resources (such as the maximum number of processes).
Enter the number of Server-TELNET listeners [1]: **Return**

Note: It is advisable, if you want automatic startup of this component, to include the \$
SET NOON line in your SYLOGIN.COM file to prevent the component from failing should there be an error in the file.

Configure TIMED

The Time Synchronization Protocol (TIMED) synchronizes the clocks of the various hosts in a LAN.

CNFNET Steps

You can configure TCPware's TIMED as part of the general CNFNET configuration or specifically as @TCPWARE:CNFNET TIMED (see the below example):

1. Specify if you want to use the TIMED daemon at the prompt

```
Do you want to use the TCPware TIMED Daemon [YES]:.
```

2. TIMED operates in one of three modes:

- SLAVE - The secondary daemon adjusts time in response to a master daemon. A slave daemon can never become a master.
- MASTER - The master candidate daemon operates as a master if there are no other masters already running in the network, runs as a secondary if there is already a master, and may be promoted to a master in case the master terminates (there can be multiple masters).
- FIXED_MASTER - Operates as a master in fixed mode and adjusts the secondary daemon to its own node instead of calculating the network average time, and adjusts the clocks on all the nodes, including its own (only one fixed master can be in the network and there should be no other master or secondary candidate in the network).

If you do not want to accept the default (MASTER), reply with **Y** at the prompt:

Do you want to change the TIMED mode [NO]:

and indicate a different mode at the Select TIMED mode (SLAVE/MASTER/FIXED_MASTER) [MASTER] : prompt.

3. Decide which networks you want included or excluded in TIMED synchronization. By default, TIMED tries to communicate to other servers through all the available networks on each host:

- INCLUDE specifies the list of networks to include in the time synchronization
- EXCLUDE specifies the list of networks to exclude from the time synchronization

Your current configuration (DEFAULT) appears. You are then prompted whether you want to change it at the prompt

Do you want to change the TIMED network configuration?

NO is the default response.

To change the configuration, enter **y** and then enter INCLUDE or EXCLUDE at the prompt

Select TIMED network configuration (DEFAULT/INCLUDE/EXCLUDE) [DEFAULT]:

Then, at the next prompt, enter the network or list of networks (separated by commas) to include or exclude.

Your current configuration appears.

Decide if you want to restart TIMED. The default is NO.

Configuring the TIMED Daemon:

Do you want to use the TCPware for OpenVMS TIMED Daemon [YES]: **Return**

Each TIMED daemon in this network can operate in the following 3 different modes:

SLAVE	Slave daemon which adjust time in response to a master daemon. Never promoted to a master.
MASTER	Master candidate daemon which operates as a master if there are no other masters already running in the network. It will run as slave if there is already a master, and may promote to master in case the master terminates. There can be multiple daemons run in this mode.
FIXED_MASTER	This daemon will operate as a master in fixed mode. In fixed mode, the master adjusts the slave daemon to its own node instead of calculating the network average time, and adjusts the clocks on all the nodes, including its own. Only one fixed master is allowed in the network and there should be no other master or master

```
candidate in the network.
```

```
Current configuration is: MASTER
```

```
Do you want to change the TIMED mode [NO]: Return
```

By default, TIMED will try to communicate to other daemons through all the available networks on this host. If the host is connected to more than one network, you can optionally limit the networks to which TIMED will synchronize the time. You can either:

- INCLUDE to specify the list of networks to include in the time synchronization

Or

- EXCLUDE to specify the list of networks to exclude from time synchronization

```
Current configuration is:  
DEFAULT
```

```
Do you want to change the TIMED network configuration [NO]: Return
```

Configure X Display Manager

CNFNET Steps

You can configure the X Display Manager as part of the general CNFNET configuration or specifically as @TCPWARE:CNFNET XDM (see the below example).

Determine if you want to use the XDM Server. The default is NO.

If you enable XDM, you can manage remote X displays (X terminals). When started, remote X displays communicate with XDM through the UDP-based X Display Manager Control Protocol (XDMCP). The XDM Server creates a DECwindows login process that prompts users on the remote X display to log in and create a DECwindows session.

```
Configuring the X Display Manager (XDM) Server:
```

```
Do you want to use the TCPware for OpenVMS XDM Server [NO]: Return
```

Appendix A. Sample Installation

This appendix provides a sample TCPware new installation.

The system manager's responses are in **bold** type. Note that your responses might not necessarily be the same as those given in the example.

```
$ @SYS$UPDATE:VMSINSTAL TCPWARE061
```

```
OpenVMS VAX Software Product Installation Procedure V7.3
```

```
It is 1-JUN-2023 at 07:50.
```

```
Enter a question mark (?) at any time for help.
```

```
The following products will be processed:
```

```
TCPWARE V6.1
```

```
Beginning installation of TCPWARE V6.1 at 07:50
```

```
%VMSINSTAL-I-RESTORE, Restoring product save set A ...
```

```
%VMSINSTAL-I-RELMOVED, Product's release notes have been moved to SYS$HELP.
```

```
TCPware(R) for OpenVMS Version 6.1-0
```

```
Copyright (c) by Process Software
```

```
Refer to the "Installing TCPware" chapter of the TCPware(R) for OpenVMS  
Installation & Configuration Guide.
```

```
You can specify the directory where you want the TCPware common files  
installed. The default location for the TCPware common files is  
SYS$COMMON. A [.TCPWARE] subdirectory will be created in the  
directory you specify.
```

```
* Where do you want to install the TCPware common files [SYS$COMMON]:
```

```
RETURN
```

```
You can specify the directory where you want node specific files
```

installed. This directory must not be used by any other nodes in a cluster. The default location is SYS\$SPECIFIC:[TCPWARE]. A [.TCPWARE] subdirectory will be created in the directory you specify.

* Where do you want to install the TCPware node specific files [SYS\$SPECIFIC]: **RETURN**

TCPware 6.1-0 will be installed.

This concludes the question and answer portion of the installation.

Your system will now be updated to include TCPware for OpenVMS. This will take a short while.

%VMSINSTAL-I-RESTORE, Restoring product save set B ...

```
+-----+
|           Installing TCP-OpenVMS           |
+-----+
```

%VMSINSTAL-I-SYSDIR, This product creates system disk directory TCPWARE_COMMON:[TCPWARE].

If you intend to use TCPware on other nodes in this VMScluster, and you have the appropriate software licenses, you must run the network configuration procedure on each node.

%VMSINSTAL-I-SYSDIR, This product creates system disk directory TCPWARE_COMMON:[TCPWARE.EXAMPLES].

%VMSINSTAL-I-SYSDIR, This product creates system disk directory TCPWARE_COMMON:[TCPWARE.INCLUDE].

%VMSINSTAL-I-SYSDIR, This product creates system disk directory TCPWARE_COMMON:[TCPWARE.NAMED].

%VMSINSTAL-I-RESTORE, Restoring product save set C ...

```
+-----+
|           Installing ONC RPC Services           |
+-----+
```

%VMSINSTAL-I-SYSDIR, This product creates system disk directory TCPWARE_COMMON:[TCPWARE.INCLUDE.RPCOLD].

%VMSINSTAL-I-SYSDIR, This product creates system disk directory TCPWARE_COMMON:[TCPWARE.INCLUDE.RPCXDR].

%VMSINSTAL-I-SYSDIR, This product creates system disk directory TCPWARE_COMMON:[TCPWARE.EXAMPLES.RPC].

%VMSINSTAL-I-RESTORE, Restoring product save set D ...

```
+-----+
|           Installing FTP-OpenVMS           |
+-----+
```

%VMSINSTAL-I-SYSDIR, This product creates system disk directory
TCPWARE_SPECIFIC:[TCPWARE.FTPS].

```
+-----+
|           Installing service ACCOUNTING component           |
+-----+
```

%VMSINSTAL-I-RESTORE, Restoring product save set E ...

```
+-----+
|           Installing NFS-OpenVMS Client                       |
+-----+
```

%VMSINSTAL-I-RESTORE, Restoring product save set F ...

```
+-----+
|           Installing NFS-OpenVMS Server                       |
+-----+
```

%VMSINSTAL-I-RESTORE, Restoring product save set G ...

```
+-----+
|           Installing SMTP-OpenVMS                           |
+-----+
```

```
+-----+
|           Installing POP3 Server                             |
+-----+
```

```
+-----+
|           Installing IMAP Server                             |
+-----+
```

%VMSINSTAL-I-RESTORE, Restoring product save set H ...

```
+-----+
|           Installing TELNET-OpenVMS                          |
+-----+
```

```
+-----+
|           Installing SSH for OpenVMS                         |
+-----+
```

%VMSINSTAL-I-SYSDIR, This product creates system disk directory
TCPWARE_SPECIFIC:[TCPWARE.SSH].

%VMSINSTAL-I-SYSDIR, This product creates system disk directory
TCPWARE_SPECIFIC:[TCPWARE.SSH2].

%VMSINSTAL-I-SYSDIR, This product creates system disk directory
TCPWARE_SPECIFIC:[TCPWARE.SSH2.HOSTKEYS].

%VMSINSTAL-I-SYSDIR, This product creates system disk directory
TCPWARE_SPECIFIC:[TCPWARE.SSH2.KNOWNHOSTS].

%VMSINSTAL-I-RESTORE, Restoring product save set I ...

```
+-----+  
|           Installing Kerberos V4 Services           |  
+-----+
```

To complete the installation, follow the steps described in the
"Configuring TCPware" and "Starting Up TCPware" chapters of the
TCPware for OpenVMS Installation & Configuration Guide.

%VMSINSTAL-I-MOVEFILES, Files will now be moved to their target
directories...

Installation of TCPWARE V6.1 completed at 08:02

Adding history entry in VMI\$ROOT:[SYSUPD]VMSINSTAL.HISTORY

VMSINSTAL procedure done at 08:02

Appendix B. Sample Configuration

This appendix provides a sample full TCPware configuration.

The system manager's responses are in **bold type**. Note that your responses might not necessarily be the same as those given in the example.

```
$ @TCPWARE:CNFNET MENU
```

```
TCPware(R) for OpenVMS Version 6.1-0 Network Configuration procedure for:
```

```
TCP/IP Services:
  FTP-OpenVMS
  NFS-OpenVMS Client
  NFS-OpenVMS Server
  SMTP-OpenVMS
  TELNET-OpenVMS
  Kerberos Services
  SSH-OpenVMS Server
```

This procedure helps you define the parameters needed to get TCPware(R) for OpenVMS running on this system.

This procedure creates the configuration data file, TCPWARE_SPECIFIC:[TCPWARE]TCPWARE_CONFIGURE.COM, to reflect your system's configuration.

Type <return> to continue...**Return**

```
TCPware(R) for OpenVMS Configuration Menu
```

```
Configuration Options:
```

- 1 - Configure TCPware Services
- 2 - Startup/Restart all TCPware services
- 3 - Shutdown all TCPware services

- L - Display the software licensing information (PASSWORD)
- E - Exit the configuration procedure (changes will be saved)

```
Enter configuration option: 1
```

TCPware Services Configuration Menu

Configuration Options:

- 1 - Core environment for TCP/IP services
- 2 - Configure all TCP/IP components
- 3 - Configure a specific TCP/IP component
- 4 - Startup/Restart TCP/IP services
- 5 - Shutdown TCP/IP services
- 6 - Startup/Restart a specific TCP/IP component
- 7 - Shutdown a specific TCP/IP component

E - Exit to previous menu

Enter configuration option: **1**

Configuring the core TCP/IP environment....

Please enter your Process Software Maintenance Agreement (MAS) number if you have one and have it available. This number can be found on the top of your Software Maintenance and Support Acknowledgement form.

If you do not have this number, press <RETURN> at the prompt. If you would like to enter this information later, you can set it using the command:

```
$ @TCPWARE:CNFNET MAS
```

Enter your Maintenance Agreement (MAS) number []: **12345**

Please wait ... determining default lines.

You need to enter the line identifications for the available network devices. The following is a partial list of the network devices that are supported:

Line Id	Network Device
-----	-----
QNA-n	for Digital's DELQA, DESQA, or DEQNA (XQDRIVER)
UNA-n	for Digital's DELUA or DEUNA (XEDRIVER)
BNA-n	for Digital's DEBNI, DEBNA, or DEBNT (ETDRIVER)
SVA-n	for Digital's DESVA (ESDRIVER)
MNA-n	for Digital's DEMNA (EXDRIVER)
ISA-n	for Digital's VAX 4000 (EZDRIVER)
MFA-n	for Digital's DEMFA FDDIcontroller 400 (FXDRIVER)
FZA-n	for Digital's DEFZA FDDIcontroller 700 (FCDRIVER)
PRO-n	for Proteon's proNET (PNDRIVER)
HYP-n	for NSC's HYPERchannel (NxDRIVER)
SLIP-n	for (static) Serial Line IP (any terminal device)
DECNET-	for IP over DECnet (requires DECnet)

```

DSB-n          for Digital's DSB32 (SLDRIVER)
DST-n          for Digital's DST32 (ZSDRIVER)
DSV-n          for Digital's DSV11 (SJDRIVER)
X25-n          for VAX P.S.I. (IP over X.25)
LPB-0          for local loopback (no device driver)

```

Unless your system has more than one controller, n is 0.
Enter the line identifications [LPB-0,EWA-0]: **Return**

You need to supply the following information for each line:

- The internet address for the line
- The name for the line (same as the host name if single line host, fully qualified domain name if using DNS)
- The subnet mask for the line
- The line specific information (depends on line)

If there is a DHCP server running on the network and this is a single line host, you may get the information from DHCP server automatically. To do so, please select 2.

1. Configure Internet address and related items manually.
2. Configure Internet address and related items automatically

Continue with selection [1]: **Return**

If a network is not subnetted, press Return at the subnet mask prompt. Otherwise, enter the subnet mask for the network as an internet address. These are the default subnet masks for each network class:

Network Class	Default Subnet Mask
-----	-----
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Using LOOPBACK (127.0.0.1) as name for line LPB-0.

What is the local host's INTERNET ADDRESS for line EWA-0: **192.168.2.56**

What is the NAME for line EWA-0: **LILAC.EXAMPLE.COM**

What is the SUBNET MASK for line EWA-0 [255.255.255.0]: **Return**

Do you want to enable TRAILER packet support for line EWA-0 [NO]: **Return**

Do you want to enable RARP (Reverse ARP) support for line EWA-0 [YES]:
Return

The network devices are configured as follows:

Line	Address	Name	Options
----	-----	----	-----
LPB-0	127.0.0.1	LOOPBACK	
EWA-0	192.168.2.56	LILAC.EXAMPLE.COM	/MASK=255.255.255.0 /FLAGS=(NOTRAILERS)

Is this configuration correct [YES]: **Return**

If your network is connected to other networks, you may wish to enter the internet address of a default gateway. If your network has more than one gateway, enter the gateway "closest" to the networks that you will be connecting to most frequently. The (sub)network portion of the internet address for the gateway MUST match that of a locally connected (sub)network.

Enter 0.0.0.0 if you need to remove a previously defined default gateway or your network does not have any gateways.

Your routing requirements might be more complex if your network has several gateways. Handle this by adding the appropriate NETCU commands (such as ADD ROUTE) to the TCPWARE_COMMON:[TCPWARE]ROUTING.COM command procedure.

For more information on routing, refer to the TCPware for OpenVMS(R) documentation.

Enter the internet address of the default gateway [0.0.0.0]: **192.168.2.126**

You need to specify local time zone information. Time zone may be specified as fixed value which must be manually set for the daylight savings time change, or you can use NTP (Network Time Protocol) Daemon to change the system clock and time offset automatically.

Do you want to have NTP set the time and time offset automatically [NO]?

Return

You need to provide the offset from universal time (UT) or local timezone name. It is recommended that you specify an offset from UT instead of entering a time zone name.

Offset from universal time

in hours and minutes:	+HHMM (east) or -HHMM (west)
Universal time zone:	UT, UTC, GMT
North American time zone:	EST, EDT, CST, CDT, MST, MDT, PST, PDT
Military time zone:	Any single letter A through Z except J

You may enter a non-standard time zone name, although the internet discourages their use. If you use a non-standard name, you will be prompted to enter the offset from universal time as well.

Enter the offset from UT or the local time zone name [UT]: **EDT**

You need to enter the official name of this host as it is known locally and by other hosts on the network. Default is the name you specified for the first network device.

If your system will use Domain Name Services, you must enter the full domain name of the host.

Enter the official host-domain name for this host [lilac.example.com]:

Return

You can enter the host name and the corresponding internet address for the hosts on the network.

The host definition file, TCPWARE_COMMON:[TCPWARE]HOSTS., contains the host names and internet addresses for the hosts on the network. You may also edit this file manually.

Names you defined for each network devices are automatically added:

localhost LOOPBACK (127.0.0.1) added to host definition file.
lilac.example.com (192.168.2.56) added to host definition file.

You may add definitions for the other hosts if you are not going to use DNS. If you use DNS, enter <return> at the next prompt:

Next host name (<return> to end): **Return**

TCPware Services Configuration Menu

Configuration Options:

- 1 - Core environment for TCP/IP services
- 2 - Configure all TCP/IP components
- 3 - Configure a specific TCP/IP component

- 4 - Startup/Restart TCP/IP services
- 5 - Shutdown TCP/IP services
- 6 - Startup/Restart a specific TCP/IP component
- 7 - Shutdown a specific TCP/IP component

E - Exit to previous menu

Enter configuration option: **2**

Configuring all of the TCP/IP components....

Type <return> to continue... **RETURN**

Configuring the Accounting listener:

TCPware accounting consists of two components: The accounting record logger, which this procedure configures and controls, and the services that can use the accounting process.

This procedure controls the startup of the accounting record logger. The details such as the name of the accounting file, the port that the accounting record logger listens on, and the list of IP addresses that can use the accounting logger are controlled by TCPWARE:ACCOUNTING.CONF

Do you want to activate the Accounting listener on this host [NO]: **Return**

Configuring NFS-OpenVMS Client:

Do you want the NFS Client [YES]: **Return**

Configuring the Dynamic Host Configuration Protocol (DHCP) Server:

Do you want to enable the Dynamic Host Configuration/Bootstrap Protocol Server (DHCPD) [NO]: **Return**

Configuring DECnet over IP tunnels:

DECnet over IP tunneling allows you to establish DECnet lines and circuits over a TCP/IP network.

Do you want to configure DECnet over IP tunnels [NO]: **Return**

Configuring the Domain Name Services (DNS):

The Domain Name Services (DNS) for this host were previously configured to operate as a server.

Do you want to change the current configuration [YES]: **Return**

Do you want to enable the DNS Server [YES]: **Return**

%DNS-I-CONVERT, Setting up default Nameserver Config File

Cluster Load balancing is used to order a list of IP addresses based on their perceived system load. This server must be authoritative for any cluster names that are to use cluster load balancing, and the server must know what those cluster names are. If you would like to use cluster load balancing, enter yes to be prompted to enter cluster names. Use spaces to separate cluster names.

Do you want to configure a list of cluster names [NO]: **Return**

Do you want to enable DNS client support [YES]: **Return**

The client needs to obtain information from a DNS server.

Provide the internet address(es) of up to three DNS servers. Use spaces to separate multiple addresses.

Note: If the local host is configured as a server, you can enter the loopback internet address or the local host's internet address to make use of that server.

Enter the internet address of the server(s) [127.0.0.1]: **Return**

By default, the client appends the local domain name to local queries, and queries that fail resolving as fully qualified names. If you would like other domains appended, provide the name(s) of up to six domains to append.

If you do not want to append a domain other than your default domain, answer no to skip to the next section. Use spaces to separate multiple domains.

Do you want to configure a list of domains [NO]: **Return**

By default, the client resolves host names with 1 or more dots absolutely before appending your domain name. If you would like host names with 1 or more dots to be resolved with your domain name first, or you would like host names with no dots to be resolved absolutely, you want to change the number of dots.

Do you want to configure number of dots [NO]: **Return**

By default, the client will retry translation requests up to 4 times, with an initial wait for a reply of 5 seconds. The wait time doubles with each retransmission of the request until an answer is received, or all retries are exhausted. If you have more than one nameserver in your list of nameservers, the actual wait time allowed for each server is divided in an attempt to keep the total retry wait time the same as with a single server. This results in a total timeout of approximately 75 seconds per request if a nameserver does not answer.

Do you want to configure the number of retries or the initial retransmission delay [NO]: **Return**

This is how your DNS client is configured:

```
Domain Name:                example.com
Name Server(s):             127.0.0.1
```

Is this configuration correct [YES]: **Return**

Configuring FTP-OpenVMS:

Do you want to enable the FTP server [NO]: **Return**

Configuring GateDaemon (GateD):

GateD is a routing process that automatically exchanges routing information with other hosts using a variety of protocols. The supported protocols are: RIP Version 1, RIP Version 2, DCN HELLO, OSPF Version 2, EGP Version 2, BGP Versions 2 through 4, and Router Discovery.

Please follow the procedure described in the TCPware for OpenVMS Installation and Configuration Guide to configure GateD.

Do you want to use the TCPware for OpenVMS GateDaemon [NO]: **Return**

Configuring The Internet Message Access Protocol V4 (IMAP) Server:

For detailed information on the following parameters, refer to the TCPware for OpenVMS Management Guide.

Do you want to enable the IMAP server [NO]: **Return**

Configuring IPP Symbiont (IPP):

IPP Symbiont is an Internet Printing Protocol Client that enables printing using IPP to IPP-capable printers and servers over a TCP/IP network. The supported version of the IPP protocol is 1.0.

Please follow the procedure described in the TCPware for OpenVMS Installation and Configuration Guide to configure IPP print queues.

Do you want to use the TCPware for OpenVMS IPP Symbiont [NO]: **YES**

Configuring the default document format for the IPP symbiont.

IPP allows the specification of the document format using MIME media types, such as "text/plain", "application/postscript" or others. The default document format entered here will become the default used by all IPP queues that do not specify a different default in their own configurations. Individual jobs may specify other values as needed. To force the default to be whatever format the individual printers have set as a default, specify "***printer_default***".

What is the default document format [text/plain]: **Return**

Configuring Job retry Delay for the IPP symbiont.

When there is a problem with a job that appears to be temporary in nature, the job will be requeued and tried again after a delay. The Job Retry Delay specifies the default value for how long a job will be requeued for. Individual queues may specify a different value. Specify this time as a standard OpenVMS delta time.

What is the job retry delay time [0 00:10:00.00]: **Return**

Configuring Max Log Bytes for the IPP symbiont.

When logging data in DETAILED_TRACE mode, the actual data being sent and received is written to the log file in hexadecimal and in ASCII. The default behavior of the symbiont is to log all data. This setting will change that default for all IPP queues to the value entered. Individual

queues may be configured to use different values than the default. The value is specified in bytes.

What is the MAX_LOG_BYTES value [-1]: **Return**

Configuring Max Stream Count for the IPP symbiont.

Each IPP symbiont process can handle data for up to 16 different IPP queues. Each queue handled by a given symbiont process is referred to as a "stream". This setting determines how many streams each queue will handle. When more than this number of IPP queues are started, additional symbiont processes will be created, each handling no more than MAX_STREAMS streams.

What is the maximum number of streams per symbiont process [16]: **Return**

Configuring Log Level for the IPP symbiont.

There are a number of different detail levels for logging symbiont progress and problem messages. The most detailed level, "DETAILED_TRACE", can generate significant amounts of data, and should be reserved for situations where a problem is being investigated. It is not recommended for normal use.

This value specifies the default level to be used by all queues that do not specify a different value explicitly in their configurations. See the IPP documentation for a list of legal values for this parameter.

What is the default logging level [JOB_TRACE]: **Return**

Configuring Opcom Log Level for the IPP symbiont.

There are a number of different detail levels for sending symbiont progress and problem messages to OPCOM. The most detailed level, "DETAILED_TRACE", can generate significant amounts of data, and should probably not be used for this setting.

This value specifies the default level to be used by all queues that do not specify a different value explicitly in their configurations. See the IPP documentation for a list of legal values for this parameter.

What is the default OPCOM logging level [INFO]: **Return**

Configuring Opcom Terminal for the IPP symbiont.

There are several OPCOM "terminals" to which OPCOM messages can be directed. This value specifies the default OPCOM terminal to be used by all queues that do not specify a different value explicitly in their configurations. See the IPP documentation for a list of legal values for this parameter.

Which OPCOM terminal should logging messages be sent to [PRINTER]: **Return**

Configuring Autostart for the IPP symbiont.

When TCPware is started, or CNFNET is used to start the IPP component in particular, it can automatically issue a START/QUEUE command for all of the queues on the system that use the IPP print symbiont.

Do you want to auto-start the IPP queues [NO]: **Return**

Configuring Autostop for the IPP symbiont.

When TCPware is shutdown, or CNFNET is used to shutdown the IPP component in particular, it can automatically issue a STOP/QUEUE/RESET command for each of the queues on the system that use the IPP print symbiont. If you do not enable Autostop for the IPP symbiont you will need to make sure that you have stopped all IPP queues by some other means before you shutdown or restart TCPware. Shutting down the kernel while leaving network print symbionts running could result in aborted print jobs.

Do you want to auto-stop the IPP queues [NO]: **Return**

TCPware IPS (Intrusion Prevention System) is a highly-configurable subsystem for detecting attacks on components such as SSH, telnet and ftp, and responding to these attacks by putting packet filters on interfaces to block those attacks in real-time.

For detailed information on TCPware IPS, refer to the TCPware for OpenVMS Management Guide.

Do you want to enable TCPware IPS [YES]? **RETURN**

TCPware IPS uses a mailbox to deliver event information from instrumented components to the FILTER_SERVER process. The mailbox must be sized to accommodate the anticipated number of simultaneous event messages from all components. Failure to do this could result in events being lost.

The number may range from 50 to a maximum of 1000, with a default value of 400.

NOTE: If the size of the mailbox is changed, a system reboot must be performed to recreate the mailbox with the desired size.

Enter the max # of simultaneous event messages in the mailbox [400]: **Return**

Some process quotas for the FILTER_SERVER process must be set up to avoid issues with the FILTER_SERVER process hanging in MUTEX state.

The specific quotas, TQELM and ASTLM, should be determined based on receiving events per source addresses per rule per component. A

good rule of thumb is to allocate TQELM's as follows:

1 for automated hourly reporting
1 for automated 24-hour maintenance
1 for each source address per rule per component for which an event has been received. These timers are used to clean up internal address structures after 24 hours of inactivity from the address.
1 for each non-empty event queue per source address per rule per component. These timers are used to delete aged events from the event queue.

For ASTLM, this tends to be used at a slightly higher rate than TQELM, so plan accordingly.

For both TQELM and ASTLM, the default values are 500.

Enter the value for TQELM for the FILTER_SERVER process [500]: **Return**
Enter the value for ASTLM for the FILTER_SERVER process [500]: **Return**

Configuring Kerberos (Version 4) Services:

Kerberos allows you to control user access to network services.

Do you want the Kerberos Services [NO]: **Return**

Configuring the Line Printer Services (LPS):

Line Printer Services consists of the client and the server. The client lets users on this OpenVMS host print files on printers attached to remote hosts. The server accepts files from remote hosts to be printed on printers attached to this OpenVMS host. LPS configuration consists of configuring:

- Default remote printer for LPS Client commands (LPR,LPQ,LPRM)
- OpenVMS Print Queue
- LPD Server

Do you want to enable the Line Printer Services (LPS) [NO]: **Return**

Configuring the Miscellaneous Services:

Do you want the Trivial File Transfer Server (TFTPD) [NO]: **Return**

Do you want the CHARGEN Server (CHARGEND) [NO]: **Return**

Do you want the DAYTIME Server (DAYTIMED) [NO]: **Return**

Do you want the DISCARD Server (DISCARD) [NO]: **Return**

Do you want the ECHO Server (ECHOD) [NO]: **Return**

Do you want the QUOTE Server (QUOTED) [NO]: **Return**

Do you want the AUTH (Ident Service) [NO]: **Return**

Do you want the TIME Service [NO]: **Return**

Configuring NFS-OpenVMS Server:

Do you want the NFS V3 Server (NFSDV3) [YES]: **Return**

For detailed information on NFS-OpenVMS Server parameters, refer to the TCPware(R) for OpenVMS Installation & Configuration Guide.

Type <return> to continue... **Return**

The access identifier parameter, NFS_ACCESS_IDENTIFIER, specifies the name of the rights identifier to be granted to all NFS users. This parameter is optional.

To remove a previously entered identifier, enter *.

Enter the access identifier []: **MARKETING**

The security mask parameter, NFS_SECURITY, controls access to the OpenVMS system. Note that these options should normally be specified on a file system basis (rather than a global basis) using the appropriate NETCU ADD EXPORT command qualifiers (as indicated below), if applicable.

Bit Mask	Meaning when set
-----	-----
1	Superuser mount. Only the superuser is allowed to mount file systems (/SUPERUSER_MOUNT).
2	Explicit mount. Only file systems explicitly exported can be mounted (/EXPLICIT_MOUNT).
4	Mount proxy check. The UID/GID used in mount requests must exist in the PROXY database (/PROXY_CHECK).
8	Privileged port check. All incoming NFS requests must originate from privileged ports (/PRIVILEGED_PORT).
16	Report all access allowed for files to client (server does all access checks) (/SERVER_ACCESS).
32	Allow PCNFSD batch queue printing.
64	Disable PCNFSD use of the intrusion database.
128	Disable PCNFSD deletion of printed files.

To specify the security mask, add up all the bit mask values for the types of security you want provided.

Enter the security mask [0]: **16**

The logging class mask parameter, NFS_LOG_CLASS, controls the types of information written to the log file.

Bit Mask	Meaning when set	Comments
-----	-----	-----

1	Warnings	Error recovery messages
2	Mount Requests	Mount call messages
4	General	General operation messages
8	Security	Security violation messages
16	NFS Errors	NFSERR_IO messages

To specify the logging class mask, add up all the bit mask values for the types of information you want logged. The value -1 logs all classes.

Enter the logging class mask [-1]: **Return**

The PCNFSD enable parameter, NFS_PCNFSD_ENABLE, enables or disables the PCNFSD protocol.

You may enter YES (to enable PCNFSD), NO (to disable PCNFSD), or PRINTING-ONLY (to enable PCNFSD for printing only - authentication requests are ignored).

Do you want PCNFSD enabled [YES]: **Return**

The spool directory parameter, NFS_PCNFSD_SPOOL, defines the spool directory used for printing files with PCNFSD. If this parameter is undefined, the printing capability of PCNFSD is disabled. The spool directory name is case sensitive.

To remove a previously entered spool directory, enter *.

Enter the PC-NFS Client spool directory []: **/NFS/EXPORTED/SPOOL**

These are the NFS-OpenVMS Server configuration parameters you selected:

```

Access Identifier:  MARKETING
Security Mask:     16 = All Access
Logging Class Mask: -1 = Warnings, Mounts, General, Security, Errors
PCNFSD enable:    1 (YES)
Spool directory:   /NFS/EXPORTED/SPOOL

```

Is this configuration correct [YES]: **Return**

Configuring the Network Time Protocol (NTP) Daemon:

Kerberos is installed on this system. For Kerberos to work correctly, use the Network Time Protocol (NTP) Daemon to synchronize the clock on this system with the other systems that are also using Kerberos.

Do you want to use the TCPware for OpenVMS NTP Daemon [YES]: **Return**

You may set the parameter WAYTOOBIG, which defines the number of seconds difference between the system clock and the reference clock past which no clock adjustment will be performed by the NTP daemon.

While you may set this to any numeric value you wish, you should realize that setting it to lower than 4000 may interfere with NTP attempting to automatically adjust your system clock for Daylight Savings Time (if your timezone rule calls for that).

Enter value for WAYTOOBIG [4000]: **Return**

Configuring The Post Office Protocol V3 (POP3) Server:

For detailed information on the following parameters, refer to the TCPware for OpenVMS Management Guide.

Do you want to enable the POP3 server [NO]: **Return**

Configuring the PWIPDRIVER:

The PWIPDRIVER is **required** by Pathworks and DECnet/OSI over TCP/IP.

Do you want to enable the PWIPDRIVER [YES]: **Return**

Configuring the Berkeley R Commands:

The Berkeley R Commands have 2 parts: services and clients. There are 3 R services: login, shell, and exec. login service allows remote users to log in to this system using the BSD RLOGIN protocol. Authorization is done using equivalence files alone, or with both equivalence files and the user having to enter a password.

shell and exec services both allow remote users to execute a single command on this system. The difference is in the authorization method used. shell uses equivalence files while exec uses explicit username/password strings.

All services can, optionally, use Service Access Lists to further restrict remote access.

There are 3 clients: RLOGIN, RSH, and RMT.

You have the option of making the services available. You should be familiar with the R Commands and the authorization methods before starting the services to insure that you do not inadvertently expose your system to a security risk.

Do you want to activate login service [YES]: **Return**

There are 2 methods of authorization available for login service.

NORMAL: Uses equivalence files to authorize remote users, and allows remote user to try a username/password if there isn't an equivalence file match.

SECURE: Uses equivalence files, and if there is a match, requires the remote user to enter the account's password correctly. If there is no equivalence file match, access is denied.

Which type of login authorization (NORMAL, SECURE) [SECURE]: **Return**

Do you want to activate shell service [YES]: **Return**

Do you want to activate exec service [YES]: **Return**

The RLOGIN, RSH, and RMTSETUP (without the /PASSWORD qualifier) commands require SYSPRV privilege to bind to reserved TCP ports which are needed for them to work correctly. In a BASIC configuration, the executable images are INSTALLED with SYSPRV privilege to allow all users on your system to make use of them. In this FULL configuration, you have the option of restricting the use of these 3 commands.

Answering "NO" to the following questions restricts use of the indicated command to users with either SYSPRV or BYPASS privilege only.

Answering "YES" allows general use of the command.

Do you want to INSTALL the RLOGIN image [YES]: **Return**

Do you want to INSTALL the RSH image [YES]: **Return**

Do you want to INSTALL the RMTSETUP image [NO]: **Return**

Configuring SMTP-OpenVMS:

For detailed information on the following parameters, refer to the TCPware for OpenVMS Management Guide.

Do you want to use the SMTP Mail Transfer Agent? [NO]: **Return**

Configuring the SNMP Agent:

SNMP is the Simple Network Management Protocol. If you activate the SNMP agent on this host, the agent will start up when you start up the network and will respond to queries. Answer YES to the next prompt only if your network has an SNMP client (network management station).

Do you want to activate the SNMP agent on this host [NO]: **Return**

Configuring SSH-OpenVMS:

For detailed information on the following parameters, refer to the TCPware for OpenVMS Management Guide.

TCPware supports both SSH1 and SSH2 servers. You may configure TCPware to support either SSH1 servers or SSH2 servers, or both. Note that the choice of TCPware servers has no impact on the TCPware SSH client, which supports both SSH1 and SSH2 remote servers.

Do you want to enable the SSH1 server [NO]? **Return**

Do you want to enable the SSH2 server [NO]? **Return**

Configuring TALK Utility

The TALK client/server operates with other "NTALK" clients and servers. The "NTALK" protocol was introduced in BSD V4.3; the version of TALK shipped with TCPware is not compatible with TALK utilities based on earlier versions of BSD.

In order for users to use TALK, the TALKD server must also be enabled.

Do you want to enable the TALKD server [NO]: **Return**

Configuring TELNET-OpenVMS:

Determine how many Server-TELNET listeners you want on this system. Set this number to 1 unless you expect a lot of incoming TELNET activity.

This number does not limit the number of incoming TELNET sessions. The number of sessions is limited only by the available system resources (such as the maximum number of processes).

Enter the number of Server-TELNET listeners [1]: **Return**

Configuring the TIMED Daemon:

Do you want to use the TCPware for OpenVMS TIMED Daemon [NO]: **Return**

Configuring the X Display Manager (XDM) Server:

Do you want to use the TCPware for OpenVMS XDM Server [NO]: **Return**

TCPware Services Configuration Menu

Configuration Options:

- 1 - Core environment for TCP/IP services
- 2 - Configure all TCP/IP components
- 3 - Configure a specific TCP/IP component

- 4 - Startup/Restart TCP/IP services
- 5 - Shutdown TCP/IP services

- 6 - Startup/Restart a specific TCP/IP component
- 7 - Shutdown a specific TCP/IP component

Enter configuration option: **E**

