VMS Software

VSI OpenVMS

VSI TCP/IP Services for OpenVMS Installation and Configuration

Document Number: DO-TCPINS-01A

Publication Date: September 2021

Revision Update Information: This is a new manual.

Operating System and Version: VSI OpenVMS Integrity Version 8.4-2
VSI OpenVMS Alpha Version 8.4-2L1

Software Version: VSI TCP/IP Services Version 5.7

VMS Software, Inc. (VSI)
Burlington, Massachusetts, USA

VSI TCP/IP Services for OpenVMS Installation and Configuration

Legal Notice

Preface

The VSI TCP/IP Services for OpenVMS product is the VSI implementation of the TCP/IP networking protocol suite and internet services for OpenVMS Alpha and I64 systems.

TCP/IP Services provides a comprehensive suite of functions and applications that support industry-standard protocols for heterogeneous network communications and resource sharing.

This manual explains how to install and configure the VSI TCP/IP Services for OpenVMS (TCP/IP Services) networking software on an OpenVMS system. This manual reflects the installation and configuration procedures for Version 5.6 of the TCP/IP Services product. For information about last-minute changes to these procedures, refer to the *VSI TCP/IP Services for OpenVMS Release Notes*.

1. About VSI

VMS Software, Inc. (VSI) is an independent software company licensed by Hewlett Packard Enterprise to develop and support the OpenVMS operating system.

VSI seeks to continue the legendary development prowess and customer-first priorities that are so closely associated with the OpenVMS operating system and its original author, Digital Equipment Corporation.

2. Intended Audience

This manual is for experienced OpenVMS and UNIX system managers and assumes a working knowledge of OpenVMS system management, TCP/IP networking, and TCP/IP terminology.

3. Document Structure

This manual contains three chapters and one appendix:

- Chapter 1 explains how to prepare for installing and configuring TCP/IP Services.
- Chapter 2 describes how to install TCP/IP Services on an OpenVMS system using the POLYCENTER Software Installation utility.
- Chapter 3 provides guidelines on how to configure the TCP/IP Services components after installation.
- Chapter 4 explains how to configure the IPv6 software.
- Appendix A provides a sample installation and configuration display as might appear on an OpenVMS system upon which TCP/IP Services has not been installed previously. The display examples in Chapter 3 show what might be seen when you upgrade TCP/IP Services software.

4. Related Documents

Table 1 lists the documents available with this version of TCP/IP Services.

Table 1. TCP/IP Services Documentation

Manual	Contents
VSI TCP/IP Services for OpenVMS Concepts and Planning	This manual provides conceptual information about TCP/IP networking on OpenVMS systems, including general planning issues to consider

Manual	Contents
	before configuring your system to use the TCP/IP Services software. This manual also describes the manuals in the TCP/IP Services documentation set and provides a glossary of terms and acronyms for the TCP/IP Services software product.
VSI TCP/IP Services for OpenVMS Installation and Configuration	This manual explains how to install and configure the TCP/IP Services product.
VSI TCP/IP Services for OpenVMS User's Guide	This manual describes how to use the applications available with TCP/IP Services such as remote file operations, email, TELNET, TN3270, and network printing.
VSI TCP/IP Services for OpenVMS Management	This manual describes how to configure and manage the TCP/IP Services product.
VSI TCP/IP Services for OpenVMS Management Command Reference	This manual describes the TCP/IP Services management commands.
VSI TCP/IP Services for OpenVMS ONC RPC Programming	This manual presents an overview of high-level programming using open network computing remote procedure calls (ONC RPCs). This manual also describes the RPC programming interface and how to use the RPCGEN protocol compiler to create applications.
VSI TCP/IP Services for OpenVMS Sockets API and System Services Programming	This manual describes how to use the Berkeley Sockets API and OpenVMS system services to develop network applications.
VSI TCP/IP Services for OpenVMS SNMP Programming and Reference	This manual describes the Simple Network Management Protocol (SNMP) and the SNMP application programming interface (eSNMP). It describes the subagents provided with TCP/IP Services, utilities provided for managing subagents, and how to build your own subagents.
VSI TCP/IP Services for OpenVMS Guide to IPv6	This manual describes the IPv6 environment, the roles of systems in this environment, the types and function of the different IPv6 addresses, and how to configure TCP/IP Services to access the IPv6 network. Note that the configuration information in *VSI TCP/IP Services for OpenVMS Guide to IPv6* is superseded by the IPv6 configuration information now provided in Chapter 4 of this guide.

For a comprehensive overview of the TCP/IP protocol suite, refer to the book *Internet working with TCP/IP: Principles, Protocols, and Architecture*, by Douglas Comer.

5. VSI Encourages Your Comments

You may send comments or suggestions regarding this manual or any VSI document by sending electronic mail to the following Internet address: <docinfo@vmssoftware.com>. Users who have

OpenVMS support contracts through VSI can contact <support@vmssoftware.com> for help with this product.

6. Conventions

The following conventions may be used in this manual:

Convention	Meaning
Ctrl/ *x*	A sequence such as **Ctrl/** *x* indicates that you must hold down the key labeled Ctrl while you press another key or a pointing device button.
PF1 *x*	A sequence such as PF1 *x* indicates that you must first press and release the key labeled PF1 and then press and release another key or a pointing device button.
Return	In examples, a key name enclosed in a box indicates that you press a key on the keyboard. (In text, a key name is not enclosed in a box.)
. . .	A horizontal ellipsis in examples indicates one of the following possibilities: • Additional optional arguments in a statement have been omitted. • The preceding item or items can be repeated one or more times. • Additional parameters, values, or other information can be entered.
. . .	A vertical ellipsis indicates the omission of items from a code example or command format; the items are omitted because they are not important to the topic being discussed.
( )	In command format descriptions, parentheses indicate that you must enclose the options in parentheses if you choose more than one.
[ ]	In command format descriptions, brackets indicate optional choices. You can choose one or more items or no items. Do not type the brackets on the command line. However, you must include the brackets in the syntax for OpenVMS directory specifications and for a substring specification in an assignment statement.
[|]	In command format descriptions, vertical bars separate choices within brackets or braces. Within brackets, the choices are options; within braces, at least one choice is required. Do not type the vertical bars on the command line.
{ }	In command format descriptions, braces indicate required choices; you must choose at least one of the items listed. Do not type the braces on the command line.
bold text	This typeface represents the introduction of a new term. It also represents the name of an argument, an attribute, or a reason.
italic text	Italic text indicates important information, complete titles of manuals, or variables. Variables include information that varies in system output (Internal error *number*), in command lines (/PRODUCER= *name*), and in command parameters in text (where *dd* represents the predefined code for the device type).
UPPERCASE TEXT	Uppercase text indicates a command, the name of a routine, the name of a file, or the abbreviation for a system privilege.
`Monospace type`	Monospace type indicates code examples and interactive screen displays. In the C programming language, monospace type in text identifies the following elements: keywords, the names of independently compiled external functions and

Convention	Meaning
	files, syntax summaries, and references to variables or identifiers introduced in an example.
-	A hyphen at the end of a command format description, command line, or code line indicates that the command or statement continues on the following line.
numbers	All numbers in text are assumed to be decimal unless otherwise noted. Nondecimal radixes—binary, octal, or hexadecimal—are explicitly indicated.

Other conventions are:

- All numbers are decimal unless otherwise noted.
- All Ethernet addresses are hexadecimal.

Chapter 1. Preparing to Install and Configure TCP/IP Services

This chapter explains how to prepare for installing and configuring VSI TCP/IP Services for OpenVMS software.

1.1. Understanding the Major Tasks

Installing the TCP/IP Services software takes just a few minutes to complete. You can install the software during the OpenVMS operating system installation procedure or as a layered product.

After you install TCP/IP Services, you need to enable the services and verify the configuration through the menu-driven TCPIP$CONFIG configuration procedure. This step may take about 15 minutes to complete.

Table 1.1 lists the major tasks involved in installing and configuring TCP/IP Services and the sections that describe these tasks.

Table 1.1. Major Tasks: Installing and Configuring

Step	Task to perform...	Described in...
1	Prepare for installation and configuration.	Sections 1.2 and 1.3
2	Shut down any previous versions of TCP/IP Services running on the system.	Section 2.1
3	Install TCP/IP Services.	Chapter 2
4	Configure TCP/IP Services according to your network needs.	Chapter 3
5	Start TCP/IP Services.	Section 3.6
6	Verify the configuration.	Section 3.9
7	Complete additional configuration and setup tasks, as appropriate.	Section 3.10
8	Configure the system as an IPv6 host or IPv6 router.	Chapter 4

1.2. Preinstallation Tasks

Table 1.2 lists the tasks you should complete before you install TCP/IP Services on your system, and the sections that describe these tasks.

Table 1.2. Preinstallation Tasks

Step	Task to perform...	Described in...
1	Inspect the distribution kit.	Section 1.2.1
2	Extract and read the TCP/IP Services release notes.	Section 1.2.2

Step	Task to perform...	Described in...
3	Back up the system disk.	Section 1.2.3
4	Perform an OpenVMS operating system upgrade, if applicable.	Section 1.2.3
5	Register the TCP/IP Services license PAK.	Section 1.2.4
6	Check the disk space, memory, and system parameters.	Sections 1.2.5 through 1.2.7
7	Assign a user identification code (UIC), if necessary.	Section 1.2.8
8	Assemble information for configuration.	Section 1.3
9	Remove any Version 5.0 IPv6 and Version 5.3 SSH or failSAFE Early Adopters Kits (EAKs).	Section 1.2.9

1.2.1. Inspecting the Distribution Kit

Make sure you have a complete software distribution kit. If you have the OpenVMS consolidated distribution CD kit, also known as the Software Products Library (SPL), check the CD master index for the location of the TCP/IP Services for OpenVMS kit. If you have an individual CD, supply the device name (such as DKA *n*) for the media when you issue the command to install TCP/IP Services.

Check that the kit contains everything listed on the Bill of Materials (BOM). If anything is missing or damaged, contact your VSI representative.

1.2.2. Extracting the Release Notes

The *VSI TCP/IP Services for OpenVMS Release Notes* document contains important information you should know before you install the product.

You can have the POLYCENTER Software Installation utility extract the release notes as either a text file or a PostScript file. To extract the release notes as a text file, enter the following POLYCENTER Software Installation utility command:

```
$ PRODUCT EXTRACT FILE TCPIP/SELECT=TCPIP055.RELEASE_NOTES
```

To extract the release notes as a PostScript file, enter the following:

```
$ PRODUCT EXTRACT FILE TCPIP/SELECT=TCPIP055_RELEASE_NOTES.PS
```

1.2.3. Backing Up the System Disk and Upgrading OpenVMS

Before you install TCP/IP Services, VSI recommends that you back up the system disk using the backup procedures established at your site. After the backup operation is complete, you should upgrade the OpenVMS operating system, if applicable.

For information about backing up a system disk, refer to the *VSI OpenVMS System Manager's Manual, Volume 1: Essentials*.

For information about how to upgrade OpenVMS, refer to the appropriate OpenVMS upgrade and installation manual.

1.2.4. Registering the License Product Authorization Key

Before you install TCP/IP Services on a newly licensed node or cluster, you must register a License Product Authorization Key (PAK) using the OpenVMS License Management Facility (LMF). Without a PAK, you can use only DECwindows TCP/IP Transport software.

On OpenVMS I64 systems, an OpenVMS Operating Environment (OE) PAK must be installed. The license for TCP/IP Services for OpenVMS is contained within each of the OE licenses.

If you are upgrading TCP/IP Services on a node or cluster that is licensed for this software, you have already completed the License PAK registration requirements.

If you ordered the license and the media together, the PAK is included with your distribution kit. Otherwise, the PAK is shipped separately to the location specified on the license order.

If you are also installing prerequisite or optional software, review the PAK status and install the PAKs for any prerequisite or optional software before you install TCP/IP Services.

To register a license, log in to the SYSTEM account and do one of the following:

- Run the SYS$UPDATE:VMSLICENSE.COM file and enter the data from your License PAK.
- At the DCL prompt, enter the LICENSE REGISTER command and the appropriate qualifiers.

You must register a license for each node in an OpenVMS Cluster.

For complete information about LMF, refer to the *VSI OpenVMS License Management Utility Guide*.

1.2.5. Checking the Disk Space

Make sure your system has at least 150,000 blocks of disk space available. The actual disk space needed varies depending on the system environment, configuration, and software options.

To find out how many free blocks exist on the system disk, enter:

```
$ SHOW DEVICE SYS$SYSDEVICE
```

1.2.6. Checking the Physical Memory

The minimum physical memory required for TCP/IP Services for OpenVMS is the same as that required for the OpenVMS operating system. For OpenVMS physical memory requirements, refer to the Software Product Description for the OpenVMS operating system (SPD 82.35.xx).

To check the memory on your system, enter:

```
$ SHOW MEMORY/FULL
```

1.2.7. Checking the System Parameters

Most systems have adequate system resources readily available to include the TCP/IP Services software. However, you should check the system parameters outlined in the following sections. Make any necessary changes to the MODPARAMS.DAT file, then run AUTOGEN, and reboot your system.

Note

Booting OpenVMS with MIN, INST, or UPGRADE is not supported. The product configuration and startup command procedures (TCPIP$CONFIG.COM and TCPIP$STARTUP.COM) fail if you perform any kind of boot other than a full boot.

The following recommendations apply to minimal configurations. Requirements will increase as you add services and inbound or outbound connections.

1.2.7.1. Global Pagelets and Global Sections

The TCP/IP Services software requires at least 160 global sections and 12,000 global pagelets be available. The minimum requirement is affected by the number of services you enable.

To check the number of available global pagelets and global sections, enter WRITE commands with the F$GETSYI lexical functions. The following is an example from an OpenVMS Alpha system:

```
$ WRITE SYS$OUTPUT F$GETSYI("FREE_GBLPAGES")
143576
$ WRITE SYS$OUTPUT F$GETSYI("FREE_GBLSECTS")
249
```

To increase the global pagelets and global sections, add statements to the SYS $SYSTEM:MODPARAMS.DAT file that increase the values of the system parameters GBLPAGES and GBLSECTIONS, as in the following example:

```
ADD_GBLPAGES = 7500
ADD_GBLSECTIONS = 75
```

1.2.7.2. Nonpaged Dynamic Pool

Add at least 500,000 bytes of available nonpaged dynamic pool for the software, as follows:

1. Log in to the SYSTEM account.
2. Identify the amount of additional nonpaged pool your system requires. Use the estimated value of 500,000 bytes, and then increase the value depending on the maximum amount of sockets you have. For each socket, allow a value of 2,000 bytes.

Note

On a system that uses FDDI, the default sizes for the TCP/IP socket buffer quotas are increased automatically. This increases throughput across the FDDI for local TCP connections.

3. Refer to the following example, and then edit MODPARAMS.DAT to reflect the appropriate value for the NPAGEDYN and NPAGEVIR parameters:

   ```
   ! Add nonpaged pool for HP TCP/IP Services for OpenVMS.
   !
   ADD_NPAGEDYN=500000
   ADD_NPAGEVIR=500000
   ```

For more information about nonpaged dynamic pool, refer to the *VSI OpenVMS System Manager's Manual, Volume 1: Essentials*.

1.2.8. Assigning a User Identification Code

An OpenVMS user or group of users is identified by a unique, assigned user identification code (UIC) in the format [*group,member*], where *group* and *member* are numeric, alphanumeric, or alphabetic characters. For example, a UIC can be either [306,210], [GROUP1, JONES], or simply JONES. The UIC is linked to a system-defined rights database that determines user and group privileges.

The TCPIP$CONFIG configuration procedure uses a group UIC to create accounts for services. If a user-specified UIC is not in place from a previous configuration, the procedure creates the following UIC group numbers:

Default UIC Group Number	Description
3655	The default UIC group number for service accounts. If this is an initial product configuration but the procedure detects that number 3655 is in use, TCPIP$CONFIG prompts you for a new UIC group number.
3375	The default UIC group number for the TCPIP $NOBODY user account.
3376	The default UIC group number for the ANONYMOUS account.

Before you assign a new group UIC, check that the number you chose is not already in use by entering the following commands:

```
$ RUN SYS$SYSTEM:AUTHORIZE
UAF> SHOW /BRIEF [your-group-number,*]
UAF> SHOW /IDENTIFIER /VALUE=UIC:[your-group-number,*]
```

To force TCPIP$CONFIG to allow you to specify a new UIC group number, assign the value TRUE to the logical name TCPIP$ASK_GROUP_UIC, as in the following example. When you configure TCP/IP Services, TCPIP$CONFIG prompts you for the group UIC.

```
$ DEFINE TCPIP$ASK_GROUP_UIC TRUE
```

1.2.9. Remove Early Adopters Kits (EAKs)

If you have installed one or more of the following EAKs, you must use the PCSI REMOVE command to remove the EAKs before you install TCP/IP Services Version 5.5:

- Version 5.0 IPv6 EAK

Note

After you remove the Version 5.0 IPv6 EAK, you must do the following:

1. Run the TCPIP$IP6_SETUP.COM command procedure. For more information, see Chapter 4.
2. After you install the current version of TCP/IP Services, recompile and relink your applications.

- Version 5.3 SSH for OpenVMS EAK
- Version 5.3 failSAFE IP EAK

1.3. Assembling Configuration Information

Use the worksheet in Table 1.3 to assemble configuration information.

If you are configuring TCP/IP Services on the system for the first time, the TCPIP$CONFIG configuration procedure prompts you for the information listed in Table 1.3. If you are reconfiguring after a product upgrade, the procedure uses the previous configuration information as the default for the new configuration.

For information to help you answer the questions on the configuration worksheet, refer to the appropriate chapters in the *VSI TCP/IP Services for OpenVMS Management* manual.

Table 1.3. Configuration Planning Worksheet

	When the configuration procedure asks...	**Your answer will be...**
What is the system's host name (for example, MYNODE)?		_____
What is the system's Internet domain name (for example, widgets.com)?		_____
Do you plan to have your IP interface under control of the DHCP client? If so, the next items on this worksheet (the system's addresses and masks, and the system's network interface), might be configured automatically by the DHCP server, in which case you do not need to specify them. Ask your network manager for details.		_____
What are the system's addresses and masks? [1]		
*	IP address (for example, 19.112.139.14)	_____
*	Subnet (network mask) address (for example, 255.0.0.0)	_____
*	Broadcast address (for example, 19.255.255.255)	_____
What is the system's network interface (for example, WE0)? [1]		_____
		_____
		_____
For failSAFE IP, what are the interfaces that will be used for the IP address's standby?		_____
		_____
		_____
What is the UIC group number for TCP/IP Services (see Section 1.2.8)? For example, 3655.		_____
Which type of routing is appropriate for the network, Static or Dynamic?		_____
	Static — For simple networks where routes do not change If static, enter the default gateway's host name and address	

	When the configuration procedure asks...	Your answer will be...
	(for example, GATWY1; 19.112.0.65).	
	Dynamic — For complex networks where flexibility is required If dynamic, you must specify either ROUTED or GATED routing.	
Do you plan to enable the BIND resolver? If so:		
*	What is the name of the BIND server you want the resolver to use (for example, MAINSV)?	_____
*	What is the IP address of the BIND server (for example, 19.112.139.10)?	_____
*	What is the domain name (for example, mainsv.widgets.com)?	_____
Do you plan to enable SNMP? If yes:		
*	Do you want to allow SNMP management clients to modify the MIBs by issuing `set` requests?	_____
*	Do you want to enable authentication traps when the master agent receives an SNMP request that specifies an unauthorized community string?	_____
*	What is the name of the system's contact person? Specify text as in the following example: Sam Spade.	_____
*	What is the location of the system? Specify one or two fields of text as in the following three examples:	_____
	- Falcon Building, Los Angeles - Boston, MA - Northwest	
*	Do you want to allow any network manager to remotely monitor your system? If so, you need to specify a public community name. The default is	_____

	When the configuration procedure asks...	Your answer will be...
	public. Specify a string consisting of alphanumeric characters only. Do not enclose the string in quotes; the case is preserved as entered. Example: Rw2.	
*	Do you want to provide additional community names and addresses (for implementing traps and allowing access beyond the default read-only provided by the “public” community)?	_____

[1]If the IP interface runs under control of the DHCP client, this information might be configured automatically. Check with your network manager. For more information, refer to the DHCP client documentation.

Chapter 2. Installing TCP/IP Services

This chapter explains how to install the VSI TCP/IP Services for OpenVMS software as a layered product using the POLYCENTER Software Installation utility. The instructions are appropriate for an initial installation or an upgrade.

For information about how to install the product directly from the OpenVMS operating system CD/DVD menu, refer to the *VSI OpenVMS Upgrade and Installation Manual*.

For information about the POLYCENTER Software Installation utility, refer to the *VSI OpenVMS System Manager's Manual, Volume 1: Essentials*.

2.1. Invoking the Installation Procedure

When you have completed the recommended preinstallation tasks outlined in Chapter 1 and have read the release notes (Section 1.2.2), you are ready to upgrade or install TCP/IP Services.

During a product upgrade, existing configuration files are preserved in case you want to use them when you configure this version of the software.

To install the TCP/IP Services software on an OpenVMS Alpha or I64 system, proceed as follows:

1. Log in to the SYSTEM account.
2. Check to make sure that other users are not logged in to the system.
3. Edit the SYS$STARTUP:SYSTARTUP_VMS.COM file and check to see if the command @SYS$STARTUP:UCX$STARTUP is defined. If this command is defined, edit the line, replacing the command definition with @SYS$STARTUP:TCPIP$STARTUP so that the current version of the product starts automatically when the system starts up.
4. If a previous version of the TCP/IP Services software is installed on the system, shut it down by using the appropriate command:

If the software version is...	Use this command...
Version 4. *x*	`@SYS$MANAGER:UCX$SHUTDOWN.COM`
Version 5. *x*	`@SYS$STARTUP:TCPIP$SHUTDOWN.COM`

5. VSI recommends that you log the installation procedure. If you have DECnet configured on your system, you can create a log of the installation procedure by entering the following command and then log in to the system account again:

   ```
   $ SET HOST 0/LOG=file-specification
   ```

   In this command, *file-specification* is the name of the file to which you want the log written. The log file is written to the current directory.

   If you do not have DECnet but have the LAT protocol (Version 5.0 or later), you can use the following command:

   ```
   $ SET HOST /LAT /LOG=file-specification
   ```

6. Start the POLYCENTER Software Installation utility by entering the PRODUCT INSTALL command with the directory path appropriate for your system. For example:

```
$ PRODUCT INSTALL TCPIP /SOURCE=directory-path
```

In this command, *directory-path* specifies the disk and directory name for the source drive that holds the TCP/IP Services kit. For example, /SOURCE=DKA400:[TCPIPAXP055].

If you do not specify the source qualifier, the POLYCENTER Software Installation utility searches the location defined by the logical name PCSI$SOURCE. If not defined, the utility searches the current default directory.

2.2. Stepping Through the Installation Procedure

After you invoke the installation procedure, you are prompted for information. Example 2.1 shows a sample installation on an OpenVMS Alpha system that has an earlier version of TCP/IP Services installed on it. Additional explanatory information follows each portion of the installation procedure. For a sample installation on a system on which the product has never been installed, see Appendix A.

The actual installation output that is displayed on your system might vary, depending on your current configuration and the operating system (Alpha or I64).

Note

To stop the installation at any time, press Ctrl/Y. The installation procedure deletes any files that were created, then exits.

The symbols *xx* in the following example and elsewhere in this document represent the product's two-digit update version number.

The following example shows an installation on an OpenVMS Alpha system. Output for installations on OpenVMS I64 systems are similar. One difference is the TCP/IP Services product name: on OpenVMS I64 systems it is I64VMS TCPIP, while on OpenVMS Alpha systems it is DEC AXPVMS TCPIP, as shown in Example 2.1.

Example 2.1. TCP/IP Services Installation: Sample POLYCENTER Software Installation Utility Procedure

```
   1 - DEC AXPVMS TCPIP V5.5-xx            Layered Product
   2 - DEC AXPVMS TCPIP V5.1-15            Layered Product
   3 - DEC AXPVMS TCPIP V5.0-11            Layered Product
   4 - All products listed above
   5 - Exit

Choose one or more items from the menu separated by commas: 1 Return
```

The initial menu that is displayed includes the latest TCP/IP Services product and any versions of the product that are in place on the system. Install the latest version (option 1).

```
The following product has been selected:
    DEC AXPVMS TCPIP V5.5-xx                 Layered Product

Do you want to continue? [YES] Return
```

Pressing Return allows the procedure to continue.

```
Configuration phase starting ...

You will be asked to choose options, if any, for each selected product and
 for
any products that may be installed to satisfy software dependency
 requirements.

DEC AXPVMS TCPIP V5.5-
xx: HP TCP/IP Services for OpenVMS.

    Copyright 1976, 2004 Hewlett-Packard Development Company, L.P.

    Hewlett-Packard Development Company, L.P.
    HP TCP/IP Services for OpenVMS offers several license options.

Do you want the defaults for all options? [YES] Return
```

Press Return (or enter YES) to choose the POLYCENTER Software Installation utility defaults for the options, or enter NO to choose other options.

```
Do you want to review the options? [NO] Return
```

Enter YES to review the POLYCENTER Software Installation utility options. Press Return (or enter NO) to continue with the final phase of the installation.

In this example, the options are not reviewed. If you enter YES to review the options, the procedure displays the options and asks whether you are satisfied with the options. To accept the options as listed, press Return. To change the options, enter NO.

```
Execution phase starting ...
The following product will be installed to destination:
    DEC AXPVMS TCPIP V5.5-xx             DISK$ALPHASYS:[VMS$COMMON.]
The following product will be removed from destination:
    DEC AXPVMS TCPIP V5.1-15             DISK$ALPHASYS:[VMS$COMMON.]
Portion done: 0%...10%...20%...30%...40%...50%...60%...70%...80%...90%
```

The following message appears only if an earlier version of TCP/IP Services was configured on your system. A similar message, verifying the product name and version, appears if you are installing for the first time.

```
%PCSI-I-PRCOUTPUT, output from subprocess follows ...
% TCPIP-W-PCSI_INSTALL
% - BG device exists.
%   To use the version of HP TCP/IP Services that was just installed,
%   system must be rebooted.
%
Portion done: 100%
The following product has been installed:
    DEC AXPVMS TCPIP V5.5-xx              Layered Product
The following product has been removed:
    DEC AXPVMS TCPIP V5.1-15              Layered Product
DEC AXPVMS TCPIP V5.5-xx: HP TCP/IP Services for OpenVMS.
    Check the release notes for current status of the product.
```

2.3. Postinstallation Tasks

After the installation completes, perform the following steps:

1. Optionally, you can:

   - Read the *VSI TCP/IP Services for OpenVMS Release Notes* on line or print the file from SYS $HELP:TCPIP056_RELEASE_NOTES.PS or SYS$HELP:TCPIP056.RELEASE_NOTES.

   - Display a list of the TCP/IP Services files that were installed. Enter the following command:

     ```
     $ PRODUCT LIST TCPIP /SOURCE=directory-path
     ```

     In this command, *directory-path* specifies the disk and directory name for the source drive that holds the TCP/IP Services kit (for example, /SOURCE=DKA400:[TCPIPAXP055]). If you do not specify the source qualifier, the POLYCENTER Software Installation utility searches the location defined by the logical name PCSI$SOURCE. If not defined, the utility searches the current default directory.

2. If you had a previous version of TCP/IP Services configured on your system and the software was previously started, reboot your system for the new TCP/IP Services software to take effect.

Important

Do not delete any files that remain from the previous version of the product. Many of these files are used by TCPIP$CONFIG for converting your existing configuration to the new configuration (described in Chapter 3).

When rebooting OpenVMS, perform only a full boot. Any other kind of boot causes the product configuration and startup command procedures (TCPIP$CONFIG.COM and TCPIP$STARTUP.COM) to fail.

3. Proceed to Chapter 3 to configure TCP/IP Services.

Note

With previous versions of TCP/IP Services, you were required to log out of the SYSTEM account and then log back in to the SYSTEM account to establish the TCPIP command environment. Starting with Version 5.4 of TCP/IP Services, this is no longer required.

Chapter 3. Configuring TCP/IP Services

After you install VSI TCP/IP Services for OpenVMS, you need to enable the components and characteristics you require for your particular system using the menu-driven TCPIP$CONFIG configuration procedure.

This chapter explains the TCPIP$CONFIG menus, provides sample installation output, and summarizes additional configuration and setup tasks.

Note

Before configuring TCP/IP services for OpenVMS, make sure you do the following:

- Create a System Authorization File (SYSUAF) database and a RIGHTSLIST database. The TCPIP $CONFIG.COM configuration procedure fails on systems that do not have these databases.
- Create and start the queue manager. The queue manager must be running. This is important especially if you plan to enable services that use queues, such as SMTP and LPD.

  The queue manager is normally enabled by default. To determine whether it is running, enter the following command at the OpenVMS DCL prompt, as shown: `$ SHOW QUEUE/MANAGER`

  If the queue manager is running, the display is as follows (where the local node is named ACME):

  ```
  Queue manager SYS$QUEUE_MANAGER, running, on ACME::
  ```

  If the following is displayed instead, the required queue files have not yet been created. The files do not exist after an initial installation of OpenVMS and must be created.

  ```
  -RMS-E-FNF, file not found
  ```

  To create these files, enter the following OpenVMS DCL command:

  ```
  $ START/QUEUE/MANAGER/NEW.
  ```

  For more information, refer to the *VSI OpenVMS System Manager's Manual, Volume 1: Essentials*. Information is also available in the SYS$MANAGER:SYSTARTUP_VMS.TEMPLATE file.

3.1. Recommended Order for Configuring TCP/IP Services

Table 3.1 lists the tasks involved in configuring TCP/IP Services, and the sections that describe these tasks.

Table 3.1. Configuring TCP/IP Services

Step	Task to perform...	Described in...
1	Assemble system information to prepare for running TCPIP $CONFIG.	Section 1.3

Step	Task to perform...	Described in...
2	If applicable, add your system to the OpenVMS Cluster to perform as a TCP/IP host	Section 3.2
3	Run TCPIP$CONFIG. (Alternatively, have TCP/IP Services configured automatically, as explained in step 4.) If you have a TCP/IP Services V4. *x* configuration on your system, answer prompts to convert existing databases or to create new ones.	Section 3.4
4	If you prefer, have TCP/IP Services software configured automatically by a DHCP server.	Section 3.3
5	Manually configure the TCP/IP Services core environment, clients, and servers using TCPIP $CONFIG.	Sections 3.4.4 through 3.4.6
6	Configure the optional components using TCPIP $CONFIG, as applicable.	Section 3.4.7
7	Start TCP/IP Services.	Section 3.6
8	Verify the configuration.	Section 3.9
9	Complete additional configuration tasks, as appropriate.	Section 3.10

Note

Configuration changes made to the TCP/IP Services software do not take effect until you start or restart the software. See Section 3.6.

3.2. Adding a System to an OpenVMS Cluster

Beginning with Version 5.5, the TCPIP$CONFIG.COM configuration procedure for TCP/IP Services can create OpenVMS accounts using larger system parameter values than in previous versions. Only new accounts get these larger values. These values are useful on OpenVMS Alpha systems but essential on OpenVMS I64 systems.

To have your OpenVMS I64 system join an OpenVMS Cluster as a TCP/IP host, VSI recommends adding the system to the cluster before you configure TCP/IP Services. The guidelines in Section 3.2.1 assume you have followed this recommendation.

If you configure TCP/IP Services before you add the system to a cluster, see Section 3.2.2.

3.2.1. Running a Newly Configured Host in the Cluster

The following recommendations assume you are configuring TCP/IP Services on the system after having added the system to the OpenVMS Cluster.

If TCP/IP Services has previously been installed on a node in the cluster and you encounter problems running a TCP/IP component on the system, modify the cluster SYSUAF to increase the parameter values for the account used by the affected component. The minimum recommended values are listed in Table 3.2.

Table 3.2. Minimum Values for SYSUAF Parameters

Parameter	Minimum Value
ASTLM	100
BIOLM	400
BYTLM	108000
DIOLM	50
ENQLM	100
FILLM	100
PGFLQUOTA [1]	50000
TQELM	50
WSEXTENT	4000
WSQUOTA	1024

[1]This parameter's value setting is especially critical.

The IMAP, DHCP, and XDM components can exhibit account parameter problems if the value assigned to PGFLQUOTA or to any of the other listed parameters is too low. Use the OpenVMS AUTHORIZE utility to modify SYSUAF parameters. For more information, refer to the *VSI OpenVMS System Management Utilities Reference Manual, Volume 1: A-L.*

3.2.2. Configuring TCP/IP Services Before Adding the System to the Cluster

If you configure TCP/IP Services before you add the system to a cluster, when you add the system to the cluster the owning UIC for each of the TCP/IP service SYS$LOGIN directories (TCPIP$ *service-name*, where *service-name* is the name of the service) may be incorrect. Use the OpenVMS AUTHORIZE utility to correct these UICs.

3.3. Automatic Configuration of TCP/IP Services Using DHCP Client

Beginning with Version 5.5, TCP/IP Services supports the DHCP client, which allows you to have your system configured automatically by a DHCP server. You can achieve this in one of two ways:

- If TCP/IP Services has never been configured on your system, you can run the TCP/IP Services startup procedure, SYS$STARTUP:TCPIP$STARTUP.COM. The startup procedure detects the fact

that the TCP/IP Services software has not been configured and asks whether you want the DHCP client to configure the host for you. Answer YES.

The startup procedure invokes TCPIP$CONFIG, which sets up the environment for the DHCP client and designates any unconfigured interfaces to be under DHCP client control. The procedure enables the following set of services automatically:

- FTP client
- TELNET client
- TELNET server
- SMTP

```
WORF_system> @sys$startup:tcpip$startup
%TCPIP-I-NOCONFIG, TCP/IP Services is not configured
Autoconfigure TCP/IP Services using DHCP client [YES]:
```

For more information about DHCP, refer to the *VSI TCP/IP Services for OpenVMS Management* manual.

- Run TCPIP$CONFIG. Choose Option 2 from the Core Environment Configuration menu, then choose Option 2–Interfaces. This option displays the Interface and Address Configuration menu from which to choose the interface you want to configure for DHCP. Select the option containing the interface you want to configure.

  Then choose Option 3 from the Interface Configuration menu, enabling the DHCP client to manage the address on that interface.

  Following is an example of the Interface and Address Configuration menu:

```
HP TCP/IP Services for OpenVMS Interface & Address Configuration Menu
                Hostname Details: Configured=Not Configured, Active=Not
 Configured

                Configuration options:
                1  -  WE0 Menu (EWA0: TwistedPair 1000mbps)
                2  -  IE0 Menu (EIA0: TwistedPair 100mbps)
               [E] -  Exit menu
                Enter configuration option:
```

  Following is an example of the Interface Configuration menu pertaining to the interface WE0 selection:

```
                HP TCP/IP Services for OpenVMS Interface WE0
 Configuration Menu
                Configuration options:
                1  - Add a primary address on WE0
                2  - Add an alias address on WE0
                3  - Enable DHCP client to manage address on WE0
               [E] - Exit menu
                Enter configuration option:
```

  This prompts you with the following:

```
Configure WE0 as the DHCP PRIMARY? (Y,N,HELP) [Y]:
```

Press return to accept the default.

The resulting display resembles the following:

```
HP TCP/IP Services for OpenVMS Interface & Address Configuration Menu
                Hostname Details: Configured=Not Configured, Active=Not
 Configured
                Configuration options:
                1  -  WE0 Menu (EWA0: TwistedPair 1000mbps) (Managed by
 DHCP client - PRIMARY)
                2  -  IE0 Menu (EIA0: TwistedPair 100mbps)
               [E] -  Exit menu
               Enter configuration option:
```

You can also use TCPIP$CONFIG to configure additional services and parameters, as needed.

Note

Verify that a DHCP Server is already setup and running on another system first; otherwise, you could receive errors when the DHCP Client tries to start, similar to the following:

```
 %TCPIP-I-DHCPC_STRD_CLNT, DHCP client started with PID 00000556
liam$dka0:[sys0.syscommon.][sysexe]tcpip$dhcp_client_conf.exe;1: timed out
 after 30 seconds
%TCPIP-E-DHCPC_TIMEOUT, controlling program timed out
%TCPIP-E-DHCPCONFERR, DHCP client failed to configure interface WE0
-TCPIP-E-DHCPC_TIMEOUT, controlling program timed out
```

The DHCP server needs the following files to be setup for success:

- nets.
- netmasks.
- dhcpcap.
- .ddnskeys
- server.pcy

3.4. Running TCPIP$CONFIG

The TCPIP$CONFIG configuration procedure displays menus from which you do the following:

- Make selections that enable services for your system. To select the default, press the Return key.
- Start or stop TCP/IP Services software.
- Verify the configuration.

To get started, enter:

```
$ @SYS$MANAGER:TCPIP$CONFIG
```

3.4.1. Converting Existing TCP/IP Services Configuration Files (Upgrade Only)

If you have a TCP/IP Services for OpenVMS (UCX) configuration in place (Version 4. *x*), and you have never configured a Version 5. *x* product on the system, the procedure begins by asking you whether to convert the Version 4. *x* (UCX) TCP/IP Services configuration files:

```
Convert the old configuration files [Y]
```

Unless you respond NO to the prompt, the procedure converts existing configuration files to new configuration files.

If you have already configured this product, the procedure indicates that no new configuration files are being created:

```
Checking TCP/IP Services for OpenVMS configuration database files.
No new database files were created.
```

The following sample output shows the start of the TCPIP$CONFIG procedure and a portion of the conversion of a previous configuration:

```
        TCP/IP Network Configuration Procedure
  This procedure helps you define the parameters required
  to run HP TCP/IP Services for OpenVMS on this system.
  NOTE:
  TCP/IP has been previously configured from an earlier version
  of this product.  You can avoid a complete reconfiguration of
  TCP/IP by allowing this procedure to automatically convert the
  old configuration files.  If you choose not to do this now, you
  will not be asked again.  At the end of the conversion you will
  be able to further modify your configuration.
Convert the old configuration files [Y]: Return
Preparing files for conversion...
    UCX$SERVICE.DAT        -> TCPIP$SERVICE.DAT
    UCX$HOST.DAT           -> TCPIP$HOST.DAT
    UCX$NETWORK.DAT        -> TCPIP$NETWORK.DAT
    UCX$ROUTE.DAT          -> TCPIP$ROUTE.DAT
    UCX$PROXY.DAT          -> TCPIP$PROXY.DAT
    UCX$CONFIGURATION.DAT  -> TCPIP$CONFIGURATION.DAT
    UCX$EXPORT.DAT         -> TCPIP$EXPORT.DAT
    UCX$PRINTCAP.DAT       -> TCPIP$PRINTCAP.DAT
       No new database files were created.

FTP SERVER Configuration

LPD SERVER Configuration

Service is not defined in the SYSUAF.
  Nonprivileged user access is not enabled.

By default, HP TCP/IP Services for OpenVMS configures
LPD such that nonprivileged users cannot modify queue entries.

Creating TCPIP$AUX identifier with a value of 3655
     HP TCP/IP Services for OpenVMS supports Line Printer Daemon
     Protocol (see RFC 1179).
       LPD requires the following:
```

```
          - Name of the local queue
          - Name of the remote queue
          - Name of the remote host
          - Spooling directory for the local queue
        To add or delete printers in the TCPIP PRINTCAP database, use the
        $RUN SYS$SYSTEM:TCPIP$LPRSETUP command.
.
.
.
```

3.4.2. Creating New TCP/IP Services Configuration Files

If you do not have an existing TCP/IP Services configuration in place from a previous version of the product, the procedure begins by creating configuration database files, as shown in the following sample output:

```
Checking TCP/IP Services for OpenVMS configuration database files.

 Creating SYS$COMMON:[SYSEXE]TCPIP$SERVICE.DAT;1
 Creating SYS$COMMON:[SYSEXE]TCPIP$HOST.DAT;1
 Creating SYS$COMMON:[SYSEXE]TCPIP$NETWORK.DAT;1
 Creating SYS$COMMON:[SYSEXE]TCPIP$ROUTE.DAT;1
 Creating SYS$COMMON:[SYSEXE]TCPIP$PROXY.DAT;1
 Creating SYS$COMMON:[SYSEXE]TCPIP$CONFIGURATION.DAT;1

 Interface - NONE configured.  DHCP will be the default.
```

3.4.3. Understanding the Configuration Menus

After the configuration files are converted or created, the Main Configuration menu is displayed:

```
    HP TCP/IP Services for OpenVMS Configuration Menu

    Configuration options:

           1  -  Core environment
           2  -  Client components
           3  -  Server components
           4  -  Optional components
           5  -  Shutdown HP TCP/IP Services for OpenVMS
           6  -  Startup HP TCP/IP Services for OpenVMS
           7  -  Run tests

           A  -  Configure options 1 - 4
          [E] -  Exit configuration procedure

Enter configuration option:
```

The options are as follows:

Option		Description
1	Core environment	Configure software associated with the Network, Internet, and Transport layers of the TCP/IP architecture (Section 3.4.4).

Option		Description
2	Client components	Configure application software and related services (Section 3.4.5).
3	Server components	Configure server software and related services (Section 3.4.6).
4	Optional components	Configure software necessary if you plan to allow Anonymous FTP access, enable Kerberos authentication for the TELNET server, enable failSAFE IP support, or run such products as PATHWORKS for OpenVMS (Advanced Server), Advanced Server for OpenVMS, DECnet over TCP/IP, or any applications that use the Stanford Research Institute (SRI) QIO application programming interface (Section 3.4.7)
5	Shutdown TCP/IP Services for OpenVMS	Stop TCP/IP Services (Section 3.7).
6	Startup TCP/IP Services for OpenVMS	Start TCP/IP Services (Section 3.8).
7	Run tests	Run the installation verification procedure (Section 3.9).
A	Configure options 1 - 4	Configure all the TCP/IP Services components (the core, client, server, and optional services). The procedure takes you through each of the configuration options.
E	Exit the configuration procedure	Return to the system prompt.

Note

If you do not have experience with the TCP/IP Services product, you should use the configuration menus provided by the TCPIP$CONFIG configuration procedure to configure the product (use options 1 through 4, or option A).

If you have experience configuring the software and want to bypass the configuration menus, you can add one or more command parameters when you run TCPIP$CONFIG. For information about the command parameters, see Section 3.5.

3.4.4. Configuring the Core Environment

To display the Core Environment Configuration menu, choose option 1 (Core environment) from the Main Configuration menu. If you chose option A from the Main Configuration menu to configure all the

TCP/IP Services components, the Core Environment Configuration menu is displayed first. The sample output in the following sections show the progression of the procedure when you choose option A.

You are required to configure the Domain, Interfaces, and Routing services; BIND Resolver and Time Zone are optional.

Note

Use the Interfaces menu (option 2) to set up an interface under control of the DHCP client. If you mark a DHCP client interface as primary, you might not need to set up the other Core Environment components. Ask your network manager whether these components are configured by DHCP. For more information, see the DHCP client documentation.

```
   HP TCP/IP Services for OpenVMS Core Environment Configuration
   Menu
   Configuration options:
           1 - Domain
           2 - Interfaces
           3 - Routing
           4 - BIND Resolver
           5 - Time Zone

           A  - Configure options 1 - 5
          [E] - Exit menu
Enter configuration option: A
Return
```

Note

If you have run the TCPIP$IP6_SETUP.COM procedure to enable IPv6, and then you run the TCPIP $CONFIG.COM command procedure, TCPIP$CONFIG.COM displays the following warning message prior to displaying the Core Environment configuration options. For more information, see Chapter 4.

```
                                - WARNING -
   This node has been configured for IPv6.  If you make any additional
   changes to the configuration of the interfaces, you must run
   TCPIP$IP6_SETUP again and update your host name information in
   BIND/DNS for the changes to take effect.
```

The following sections include sample output for the core environment components. The samples reflect a TCP/IP Services product configuration for a system on which other TCP/IP Services configurations are in place. The output varies for a new TCP/IP Services installation (see Appendix A).

Enter your responses to the menu questions using the information from your configuration planning worksheet (Section 1.3).

3.4.4.1. Domain Configuration

The following is sample output for configuring the domain:

```
       HP TCP/IP Services for OpenVMS Core Environment Configuration Menu
        Configuration options:
                 1  -  Domain
                 2  -  Interfaces
                 3  -  Routing
```

```
                4  -  BIND Resolver
                5  -  Time Zone
                A  -  Configure options 1 - 5
               [E] -  Exit menu
Enter configuration option: 1
DOMAIN Configuration
Enter Internet domain:
```

After you enter the domain name, the display resembles the following:

```
DOMAIN Configuration
Enter Internet domain: sqa.tcpip.zko.hp.com
Communication domain updated in configuration database
```

3.4.4.2. First-Time Configuration of Interfaces

The interface and address menus allow the configuration and management of both the permanent database as well as the live system. The menu supports multi-homed systems, which have multiple addresses and/or interfaces. The menus are context sensitive, so the menu options change according to the state of the system.

The following is sample output for configuring the Internet interface:

```
        Checking TCP/IP Services for OpenVMS configuration database files.
        HP TCP/IP Services for OpenVMS Configuration Menu
        Configuration options:
                 1  -  Core environment
                 2  -  Client components
                 3  -  Server components
                 4  -  Optional components
                 5  -  Shutdown HP TCP/IP Services for OpenVMS
                 6  -  Startup HP TCP/IP Services for OpenVMS
                 7  -  Run tests
                 A  -  Configure options 1 - 4
                [E] -  Exit configuration procedure
Enter configuration option: 1 Return
        HP TCP/IP Services for OpenVMS Core Environment Configuration Menu
        Configuration options:
                 1  -  Domain
                 2  -  Interfaces
                 3  -  Routing
                 4  -  BIND Resolver
                 5  -  Time Zone
                 A  -  Configure options 1 - 5
                [E] -  Exit menu
Enter configuration option: 2 Return
        HP TCP/IP Services for OpenVMS Interface & Address Configuration
 Menu
        Hostname Details: Configured=Not Configured, Active=Not Configured
        Configuration options:
                 1  -  WE0 Menu (EWA0: TwistedPair 1000mbps)
                 2  -  IE0 Menu (EIA0: TwistedPair 100mbps)
                [E] -  Exit menu
      Enter configuration option:
```

In this example, no changes are made to the interface. The systems TCP/IP hostname is displayed as Not Configured. This is automatically configured the first time an IP address is configured. The assigned systems TCP/IP hostname may be changed using the menu options for configuring addresses.

Additional information is provided for each interface name. For instance, the TCP/IP interface named WE0 corresponds to the OpenVMS device EWA0: and is twisted-pair. If you want to configure a standby interface for failSAFE IP failover support, see Section 3.4.4.4; otherwise, skip to Section 3.4.4.5.

3.4.4.3. Interface IP Address Configuration

To configure an interface, select the option of the desired interface, then select Option 1 - Add a primary address on `<chosen interface>`, and answer the prompts for the IP address, netmask and hostname information.

For example:

```
        HP TCP/IP Services for OpenVMS Interface & Address Configuration
 Menu
        Hostname Details: Configured=Not Configured, Active=Not Configured
        Configuration options:
        1  -  WE0 Menu (EWA0: TwistedPair 1000mbps)
        2  -  IE0 Menu (EIA0: TwistedPair 100mbps)
       [E] -  Exit menu
      Enter configuration option: 1
```

This menu allows the configuration of a primary or an alias address as well as giving control to DHCP-client for address assignment. The primary address is considered the most often used address for this interface, whereas an alias address is considered a secondary address. By default, data sent via an interface with a primary and an alias address is transmitted with the IP source address set to the primary address.

The following example shows that WE0 is configured with a primary IP address of 10.0.0.1 and an alias address of 10.0.1.1. The menus are driven as follows, after selecting option 1 from the previous menu.

```
      HP TCP/IP Services for OpenVMS Interface WE0 Configuration Menu
      Configuration options:
       1  - Add a primary address on WE0
       2  - Add an alias address on WE0
       3  - Enable DHCP client to manage address on WE0
      [E] - Exit menu
Enter configuration option: 1
    IPv4 Address may be entered with CIDR bits suffix.
    E.g. For a 16-bit netmask enter 10.0.1.1/16
    Enter IPv4 Address []: 10.0.0.1
    Default netmask calculated from class of IP address: 255.0.0.0
    IPv4 Netmask may be entered in dotted decimal notation,
    (e.g. 255.255.0.0), or as number of CIDR bits (e.g. 16)
Enter Netmask or CIDR bits [255.0.0.0]: 16
Enter hostname []: liam
```

The system displays the information entered. If it is correct, press Return to accept it.

The following output is displayed, showing all information entered and then the Interface and Address menu again to display the change you have just made, configuration, and interface.

```
Requested configuration:
      Address  : 10.0.0.1/16
      Netmask  : 255.255.0.0 (CIDR bits: 16)
      Hostname : liam
* Is this correct [YES]:
```

```
Added hostname liam (10.0.0.1) to host database
NOTE:
  The system hostname is not configured.
  It will now be set to liam (10.0.0.1).
  This can be changed later via the Interface Configuration Menu.
Updated system hostname in configuration database
Added address WE0:10.0.0.1 to configuration database
      HP TCP/IP Services for OpenVMS Interface & Address Configuration Menu
      Hostname Details: Configured=liam, Active=Not Configured
      Configuration options:
       1  -  WE0 Menu (EWA0: TwistedPair 1000mbps)
       2  -  10.0.0.1/16     liam                  Configured
       3  -  IE0 Menu (EIA0: TwistedPair 100mbps)
      [E] -  Exit menu
Enter configuration option:
```

In this example, Interface WE0 with 10.0.0.1 was configured as the address, 16 CIDR bits (255.255.0.0) as the netmask, and the hostname as LIAM.

The address may be entered with the number of CIDR bits or a netmask. This example used 16 CIDR-bits, which is equivalent to a netmask of 255.255.0.0.

Because this is the first address configured on the system, it automatically becomes the TCP/IP hostname, as is displayed under the NOTE: text.

The address 10.0.0.1 with a name of LIAM has automatically been assigned as the system's TCP/IP hostname. This automatic assignment occurs only when no other addresses are configured on the system.

After configuring an address the menu returns to the Interface and Address Configuration menu. It now displays the address 10.0.0.1/16 configured on WE0. The newly created address has its own menu option (2), which allows further modification of the specific address. Note that menu options for configuring the other interfaces have been incremented compared to the first screen capture.

The state of the address is described as Configured.

3.4.4.4. failSAFE IP Address Configuration

To provide high availability of an IP address, you can configure it on multiple interfaces on a node or across a cluster, then enable the failSAFE IP service. Note that only one instance of the address is active; the others are in standby mode. The failSAFE IP service continually monitors the health of interfaces and upon detecting an interface failure, the address is deactivated on the failed interface and a standby address becomes active.

When the failed interface recovers, failSAFE IP detects this and can return its IP address.

Configure the standby IP address as follows:

1. From the Core Environment Configuration menu, select option 2 (Interfaces). The Interface and Address Configuration menu appears.

2. From the Interface and Address Configuration menu, select the menu item for the IP Address you want to configure as an alias for failSAFE IP, then select Option 4 - Add standby aliases to configuration database (for failSAFE IP), then enter name of the interface for the failSAFE IP.

   In the following example, 10.10.1.1 was already configured as an alias for interface WE0. (This was done by selecting the option for an alias address instead of the option for a primary address.) There are now two IP addresses from which to choose for the failSAFE IP.

This example uses 10.10.1.1 for the failSAFE IP and for the IEO Interface. Select Option 3, then Option 4, then enter IE0 as follows:

Note

For information on configuring failSAFE IPv6 addresses, see Section 4.3.

```
      HP TCP/IP Services for OpenVMS Interface & Address Configuration
 Menu

      Hostname Details: Configured=liam, Active=Not Configured

     Configuration options:
    1  -  WE0 Menu (EWA0: TwistedPair 1000mbps)
    2  -  10.0.0.1/16     liam                  Configured
    3  -  10.10.1.1/16    abby                  Configured

    4  -  IE0 Menu (EIA0: TwistedPair 100mbps)

   [E] -  Exit menu
Enter configuration option: 3
      HP TCP/IP Services for OpenVMS Address Configuration Menu
       WE0 10.10.1.1/16 abby Configured WEA0
 Configuration options:
         1  - Change address
         2  - Set "abby" as the default hostname
         3  - Delete from configuration database
         4  - Add standby aliases to configuration database (for
 failSAFE IP)
        [E] - Exit menu
Enter configuration option: 4
Address 10.10.1.1/16 is currently configured on:
   WE0
Interfaces available for failover are:
  IE0
Enter an interface for failSAFE IP: IE0
Added alias address IEA0:10.10.1.1 to configuration database
     The failSAFE IP service, which monitors the health of interfaces,
     is not currently enabled.  Refer to the Optional Components Menu
     to configure the service.
Press
<ENTER> key to continue...
   HP TCP/IP Services for OpenVMS Interface & Address Configuration Menu
 Hostname Details: Configured=liam, Active=Not Configured
 Configuration options:
   1  -  WE0 Menu (EWA0: TwistedPair 1000mbps)
   2  -  10.0.0.1/16     liam                  Configured
   3  -  10.10.1.1/26    abby                  Configured
   4  -  IE0 Menu (EIA0: TwistedPair 100mbps)
   5  -  10.10.1.1/26        abby                  Configured
  [E] -  Exit menu
Enter configuration option:
```

3. When you have started TCP/IP services, you return to the Interface and Address Configuration menu to verify that your selected address is now in standby mode, as in the following example:

```
     HP TCP/IP Services for OpenVMS Interface & Address Configuration Menu
    Hostname Details: Configured=liam, Active=liam
    Configuration options:
      1  -  WE0 Menu (EWA0: TwistedPair 1000mbps)
      2  -  16.116.93.75/26     liam                 Configured,Active
      3  -  10.10.1.1/26        abby                 Configured,Active

      4  -  IE0 Menu (EIA0: TwistedPair 100mbps)
      5  -  10.10.1.1/26        abby                 Configured,Active-
   Standby
     [E] -  Exit menu
   Enter configuration option:
```

Note that item 5 now has `Configured,Active-Standby` as its status.

```
         HP TCP/IP Services for OpenVMS Address and Configuration Menu

          WE0 10.10.1.1/26 abby Configured,Active-Standby WE01

    Configuration options:

            1  - Change address
            2  - Set "abby.sqa.tcpip.zko.hp.com" as the default hostname
            3  - Delete from configuration database
            4  - Remove from live system
            5  - Add standby aliases to configuration database (for
    failSAFE IP)

           [E] - Exit menu

   Enter configuration option:
```

4. After configuring the standby IP address, you must configure and enable the failSAFE IP service, as explained in Section 3.4.7.2.

Note

You can also manually configure the failSAFE IP address using the TCP/IP management SET INTERFACE command or the `ifconfig` utility. The `ifconfig` utility provides a greater degree of management control and is recommended for more complex environments. For more information, refer to the *VSI TCP/IP Services for OpenVMS Management* manual.

3.4.4.5. Dynamic Routing Configuration

The following is sample output for configuring dynamic routing:

```
DYNAMIC ROUTING Configuration
 Dynamic routing has not been configured.
    You may configure dynamic ROUTED or GATED routing.
    You cannot enable both at the same time.  If you want
    to change from one to the other, you must disable the
    current routing first, then enable the desired routing.
    If you enable dynamic ROUTED routing, this host will use the
    Routing Information Protocol (RIP) - Version 1 to listen
    for all dynamic routing information coming from other
    hosts to update its internal routing tables.
```

```
    It will also supply its own Internet addresses to
    routing requests made from remote hosts.
    If you enable dynamic GATED routing, you will be able to
    configure this host to use any combination of the following
    routing protocols to exchange dynamic routing information
    with other hosts on the network:
        Routing Information Protocol (RIP) - Version 1 & 2
        Router Discovery Protocol (RDISC)
        Open Shortest Path First (OSPF)
        Exterior Gateway Protocol (EGP)
        Border Gateway Protocol (BGP-4)
        Static routes

* Do you want to configure dynamic ROUTED or GATED routing [NO]: YES Return
* Do you want to enable GATED routing configuration [NO]: Return
    ROUTED option
    If you enable the 'supply' option of dynamic routing,
    this host will supply dynamic routing information to
    other hosts on the network whether it is acting as an
    internetwork gateway or not.
* Do you want this host to supply its dynamic routing information
 [NO]: Return
```

3.4.4.5.1. Default Route Configuration

If you need to configure a default route, press Return at the first prompt, accepting the default of `NO` to the dynamic routing option, then press Return at the next prompt to accept the default of `YES` to the default route, then enter the name of the gateway and its IP address, as shown in the following example:

```
* Do you want to configure dynamic ROUTED or GATED routing [NO]: Return
        A default route has not been configured.
* Do you want to configure a default route [YES]: [return]
Enter your Default Gateway host name or address:
 cisco64net.sqa.tcpip.zko.hp.com
        cisco64net.sqa.tcpip.zko.hp.com is not in the local host database.
Enter Internet address for cisco64net.sqa.tcpip.zko.hp.com: 16.116.93.65
```

3.4.4.6. BIND Resolver Configuration

To configure the BIND resolver, select Option 4 from the Core Environment menu, enter the BIND server name and address, as shown in the following example:

```
   HP TCP/IP Services for OpenVMS Core Environment Configuration Menu
        Configuration options:
                 1  -  Domain
                 2  -  Interfaces
                 3  -  Routing
                 4  -  BIND Resolver
                 5  -  Time Zone
                 A  -  Configure options 1 - 5
                [E] -  Exit menu
Enter configuration option: 4
BIND RESOLVER Configuration
        A BIND resolver has not been configured.
        HP TCP/IP Services for OpenVMS supports the Berkeley Internet Name
        Domain (BIND) resolver.  BIND is a network service that enables
 clients
```

```
        to name resources or objects and share information with other
 objects
        on the network.
        Before configuring your system as a BIND resolver, you should
        first be sure that there is at least one system on the network
        configured as either a BIND primary or secondary server for
        this domain.
        You can specify a BIND server by its address or name;
        however, if specified by name, an entry for it must
        exist in the TCPIP$HOST database.
        You will be asked one question for each server.
        Press Return at the prompt to terminate the list.
Enter your BIND server name: odessy
        odessy is not in the local host database.
Enter Internet address for odessy: 16.116.93.66
Enter next BIND server name:
        HP TCP/IP Services for OpenVMS Core Environment Configuration Menu
        Configuration options:
                 1  -  Domain
                 2  -  Interfaces
                 3  -  Routing
                 4  -  BIND Resolver
                 5  -  Time Zone
                 A  -  Configure options 1 - 5
                [E] -  Exit menu
Enter configuration option:
```

To view the current BIND resolver configuration, select Option 4 from the Core Environment menu. Press Return to accept the default if you do not want to reconfigure the BIND resolver, as shown in the following example:

```
        HP TCP/IP Services for OpenVMS Core Environment Configuration Menu
        Configuration options:
                 1  -  Domain
                 2  -  Interfaces
                 3  -  Routing
                 4  -  BIND Resolver
                 5  -  Time Zone
                 A  -  Configure options 1 - 5
                [E] -  Exit menu
Enter configuration option: 4
BIND RESOLVER Configuration
A BIND resolver has already been configured.
BIND Resolver Configuration
  Transport:  UDP
  Domain:     sqa.tcpip.zko.hp.com
  Retry:         2
  Timeout:       5
  Servers:    odessy
  Path:       No values defined
* Do you want to reconfigure BIND [NO]:
```

The following is sample output for configuring the BIND resolver:

```
A BIND resolver has already been configured.
BIND Resolver Configuration
  Transport:  UDP
  Domain:     budget.acme.com
```

```
  Retry:          4
  Timeout:        4
  Servers:     island.budget.acme.com
  Path:        No values defined
* Do you want to reconfigure BIND [NO]: Return
```

In this example, no changes are made to the BIND resolver.

3.4.4.7. Time Zone Configuration

The following is sample output for configuring the time zone:

```
  TCPIP uses timezone information provided by the OpenVMS Operating
  System. No additional timezone configuration is needed for TCPIP
  when the operating system is configured correctly.
  This section verifies the current OpenVMS timezone configuration.
  A warning message (TCPIP-W-) indicates that corrective action should
  be taken. TCPIP will appear to operate but components may display
  either the wrong time or a time inconsistent with other applications.
%TCPIP-I-INFO, Logical name SYS$TIMEZONE_RULE found.
-TCPIP-I-INFO, Software for automatic Summer/Winter time (TDF) change
-TCPIP-I-INFO, is present.
-TCPIP-I-INFO, Further action to ensure TDF change is not necessary.
%TCPIP-I-NORMAL, timezone information verified
Press Return to continue ...
```

After you configure the core environment, press Return or choose option E to exit from the Core Environment menu. If you chose option A from the Main Configuration menu to configure all the TCP/IP Services components, the Client Components Configuration menu displays next; otherwise, the procedure returns to the Main Configuration menu.

3.4.5. Configuring the Client Environment

To display the Client Components Configuration menu, choose option 2 (Client components) from the Main Configuration menu. If you chose option A from the Main Configuration menu to configure all the TCP/IP Services components, the Client Components Configuration menu displays automatically after you finish configuring the core environment services.

From the Client Components Configuration menu, choose option A to configure all the client services. Alternatively, you can configure one client service at a time. The sample output in the following sections show the progression of the procedure when you choose option A.

Note

Starting with Version 5.4 of TCP/IP Services, you can configure and use Secure Shell (SSH) to provide secure login, remote command execution, file copying, and file transfer.

The SSH client and server on this version of TCP/IP Services cannot use configuration files from previous versions of SSH. If the SSH client and server detect systemwide configuration files from an older version of SSH, the client and server will fail to start. For more information, refer to the TCP/IP Services release notes.

```
HP TCP/IP Services for OpenVMS Client Components Configuration Menu
Configuration options:
        1  - DHCP Client      Disabled Stopped
        2  - FTP Client       Enabled  Stopped
        3  - NFS Client       Enabled  Started
```

```
        4  - REXEC and RSH    Enabled  Started
        5  - RLOGIN           Enabled  Started
        6  - SMTP             Enabled  Started
        7  - SSH Client       Enabled  Stopped
        8  - TELNET           Enabled  Started
        9  - TELNETSYM        Disabled Stopped
        A  - Configure options 1 - 9
       [E] - Exit menu
```

Note that the sample Client Components Configuration menu shows most clients enabled and all of them stopped. Clients are enabled for startup if they have been enabled in the TCP/IP Services configuration database (TCPIP$CONFIGURATION.DAT). The enabled services are started the next time TCP/IP Services is started. You can also start (or stop) a specific service, without having to restart TCP/IP Services, by choosing the Start service option from that service's configuration menu. In addition, you can use command procedures to start or stop a specific service, as explained in Section 3.11.3.

The initial status of the services depends on whether you have other TCP/IP Services installations in place on the system, and whether the software or individual services have been started. On a new system, all the services would be disabled (the default). The status of services is also affected by the selections you made from the Core Environment menu.

To minimize resource consumption, enable and start only those services that you are sure to use. Disable those you do not plan to use.

To configure all the client services, choose option A.

The following is an example of the output for configuring an FTP client. The configuration output for other clients might vary. Note that after you configure a client (such as FTP) that has an associated server, the configuration prompts you about whether to configure the corresponding server.

```
Enter configuration option: 2 Return
FTP CLIENT Configuration

Service is enabled on specific node.
Service is stopped.

         FTP CLIENT configuration options:

                 1 - Disable service on this node
                 2 - Start service on this node
                [E] - Exit FTP_CLIENT configuration

Enter configuration option: 1 Return
The FTP SERVER is enabled.

* Do you want to configure the FTP SERVER [NO] ? Return
```

In the preceding example, the FTP client was originally enabled, and option 1 disables it. The configuration procedure indicates that the FTP server is enabled and asks whether you want to configure it as well.

The following example shows the configuration output that you might see if you want to enable an FTP client that had been disabled.

```
FTP CLIENT Configuration
Service is not enabled.
Service is stopped.
        FTP CLIENT configuration options:
```

```
                  1 - Enable service on this node
                  2 - Enable & Start service on this node
                 [E] - Exit FTP_CLIENT configuration
Enter configuration option: 2 Return
```

In this example, as with the previous one, the TCP/IP Services software has already been started, so you have the choice of starting the client as well as enabling it. If you choose option 1, the FTP service is enabled and FTP starts the next time TCP/IP Services is started. If you choose option 2, the FTP service is started immediately and then every time the TCP/IP Services is started.

If the TCP/IP Services software is not already started, then the FTP Client Components Configuration menu gives you only the option of enabling the service, as in the following example:

```
                  1 - Enable service on this node
                 [E] - Exit FTP_CLIENT configuration
```

After you configure the client service environment, press Return or choose option E to exit from the Client Components menu. If you chose option A from the Main Configuration menu to configure all the TCP/IP Services components, the Server Components Configuration menu displays next; otherwise, the procedure returns to the Main Configuration menu.

3.4.6. Configuring the Server Environment

To display the Server Components Configuration menu, choose option 3 (Server components) from the Main Configuration menu. If you chose option A from the Main Configuration menu to configure all the TCP/IP Services components, the Server Components Configuration menu displays automatically after you finish configuring the client services.

Note

Starting with Version 5.4 of the TCP/IP Services, you can configure and use Secure Shell (SSH) to provide secure login, remote command execution, file copying, and file transfer.

```
HP TCP/IP Services for OpenVMS Server Components Configuration Menu
  1 - BIND         Enabled  Started    12 - NTP         Enabled  Started
  2 - BOOTP        Disabled Stopped    13 - PC-NFS      Enabled  Started
  3 - DHCP         Disabled Stopped    14 - POP         Enabled  Started
  4 - FINGER       Enabled  Started    15 - PORTMAPPER  Enabled  Started
  5 - FTP          Enabled  Started    16 - RLOGIN      Enabled  Started
  6 - IMAP         Disabled Stopped    17 - RMT         Disabled Stopped
  7 - LBROKER      Disabled Stopped    18 - SNMP        Enabled  Stopped
  8 - LPR/LPD      Disabled Stopped    19 - SSH         Enabled  Started
  9 - METRIC       Enabled  Started    20 - TELNET      Enabled  Started
 10 - NFS          Enabled  Started    21 - TFTP        Enabled  Started
 11 - LOCKD/STATD  Disabled Stopped    22 - XDM         Enabled  Started


  A  -  Configure options 1 - 22
 [E] -  Exit menu
Enter configuration option:
```

Servers are enabled for startup if they have been added to the TCP/IP Services configuration database (TCPIP$CONFIGURATION.DAT), and they are started the next time TCP/IP Services is started. You can also start (or stop) a specific server, without having to restart TCP/IP Services, by choosing the Start service option from that server's configuration menu. In addition, you can use command procedures to start or stop a specific server, as explained in Section 3.11.3.

The initial status of the servers depends on whether you have other TCP/IP Services installations in place on the system, and whether the software or individual servers have been started. To minimize resource consumption, enable and start the specific servers you plan to use, and disable those you do not plan to use. You can choose option A to configure all the servers.

For servers that have associated client services (such as the FTP server and client), when you configure the server you are prompted about whether to configure the corresponding client.

Note

TELNET and RLOGIN are enabled from the client menu. If you want to disable the TELNET or RLOGIN server, then you must disable the service. To enable or disable the TELNET server or the RLOGIN server, use the Client Components Configuration menu, choose the appropriate client, and disable and stop the service by choosing the Disable and Stop service on this node option.

The following is an example of an XDM server configuration output. The configuration displays for other servers might vary.

```
Enter configuration option: 21 Return
XDM Configuration

Service is defined in the SYSUAF.
Service is not defined in the TCPIP$SERVICE database.
Service is not enabled.
Service is stopped.

 XDM configuration options:

   1 - Enable service on this node

  [E] - Exit XDM configuration

Enter configuration option:
```

Note

XDM requires the following DECwindows components to be installed:

- SYS$COMMON:[SYSLIB]DECW$XLIBSHR.EXE
- SYS$COMMON:[SYSLIB]DECW$XTLIBSHRR5.EXE

The TCPIP$CONFIG configuration procedure checks whether these components are installed. If they are not found, TCPIP$CONFIG notifies you and gives you the option of configuring XDM and installing the DECwindows components later before you attempt to activate XDM. The notification and prompt are as follows:

```
XDM requires DECwindows components that are not installed.
Attempts to activate XDM will fail.
Type C to continue with XDM configuration, or E to exit [ E ]:
```

After you configure the servers, press Return or choose option E to exit from the Server Components Configuration menu. If you chose option A from the Main Configuration menu to configure all the TCP/IP Services components, the Optional Components Configuration menu displays next; otherwise, the procedure returns to the Main Configuration menu.

3.4.7. Configuring the Optional Components

You may need to configure optional product components if you plan to do one or more of the following:

- Run the PATHWORKS for OpenVMS (Advanced Server), the Advanced Server for OpenVMS, or DECnet over TCP/IP software.
- Run or develop applications that use the Stanford Research Institute's (SRI) QIO application programming interface (API).
- Allow Anonymous FTP access.
- Initialize Kerberos authentication for the TELNET server.
- Where a node or cluster has multiple interfaces, enable failSAFE IP to monitor the health of network interface cards and, when an interface fails, to perform a failover to another interface to maintain network connectivity.

To display the Optional Components Configuration menu, choose option 4 (Optional components) from the Main Configuration menu. If you chose option A from the Main Configuration menu to configure all the TCP/IP Services components, the Optional Components Configuration menu displays automatically after you finish configuring the servers.

The Optional Components Configuration menu displays the following menu options:

```
HP TCP/IP Services for OpenVMS Optional Components Configuration
Menu
Configuration options:
        1 - Configure PWIP Driver (for DECnet-Plus and PATHWORKS)
        2 - Configure SRI QIO Interface (INET Driver)
        3 - Set up Anonymous FTP Account and Directories
        4 - Configure Kerberos Applications
        5 - Configure failSAFE IP
        A - Configure options 1 - 5
       [E] - Exit menu
Enter configuration option:
```

Choose the options that are appropriate for your system: the PWIP Driver, the SRI QIO Interface, Anonymous FTP Accounts and Directories, Kerberos authentication for TELNET, and failSAFE IP (provides IP address failover capability for multiple interfaces on a host or cluster).

- If you want to run PATHWORKS for OpenVMS (Advanced Server), Advanced Server for OpenVMS, or DECnet over TCP/IP, configure the PWIP driver by choosing option 1. In addition, refer to the appropriate documentation for the layered product.
- If you run or develop applications that use the SRI QIO API, choose option 2.
- If you want to allow Anonymous FTP access, choose option 3 to set up an Anonymous FTP account and directories. Make sure you obtain the necessary user information code (UIC) (see Section 1.2.8) and determine guest user privileges.
- If you want to provide the security benefits of Kerberos authentication for the TELNET server, choose option 4 to configure Kerberos. For details about configuring Kerberos support, see Section 3.4.7.1.
- If you want to provide IP address failover capability for multiple interfaces on a host or cluster, choose option 5 to configure failSAFE IP. For details about configuring failSAFE IP support,

see Section 3.4.7.2. More information is available also in the *VSI TCP/IP Services for OpenVMS Management* manual.

The following example shows the output for configuring the PWIP driver:

```
Enter configuration option: 1 Return
TCPIP Transport for DECnet and Pathworks Service Configuration

Service is enabled on specific node.
Service is stopped.

 TCPIP Transport for DECnet and Pathworks Service configuration options:

    1 - Disable service on this node

   [E] - Exit PWIP_DRIVER configuration

Enter configuration option:
```

3.4.7.1. Configuring and Enabling Kerberos Support

To configure the TELNET service to support Kerberos, follow these steps. For more details about Kerberos features, including prerequisites and instructions for using Kerberos, refer to the *VSI TCP/IP Services for OpenVMS Management* manual.

Note

Before you begin the following steps, make sure the TELNET service is stopped.

1. From the TCPIP$CONFIG.COM procedure Main Configuration menu, choose option 2 (Client components).
2. From the list of client services, choose option 6 (TELNET).
3. From the TELNET Configuration menu, choose option 1 (Enable service on all nodes). This step creates the TCPIP$TELNET user account and directory.
4. Return to the Main Configuration menu.
5. From the Main Configuration menu, choose option 4 (Optional components).
6. From the Optional Components Configuration menu, choose option 4 (Configure Kerberos Applications). The following menu is displayed:

   ```
   Kerberos Applications Configuration Menu
   TELNET Kerberos is not defined in the TCPIP$SERVICE database.
         Configuration options:
                 1  -  Add Kerberos for TELNET server
                 2  -  Remove Kerberos for TELNET server
                [E] -  Exit menu
   Enter configuration option:
   ```

7. From the Kerberos Applications Configuration menu, choose option 1 (Add Kerberos for TELNET Server).
8. Exit the command procedure.

9. When you are prompted to start the TELNET service, enter N.

10. Start the TELNET service by executing the TELNET startup procedure, as shown in the following example:

```
$ @SYS$STARTUP:TCPIP$TELNET_STARTUP.COM
%TCPIP-I-INFO, image SYS$SYSTEM:TCPIP$TELNET_SERVER.EXE installed
%TCPIP-I-INFO, image SYS$SYSTEM:TCPIP$TELNET.EXE installed
%TCPIP-I-INFO, logical names created
%TCPIP-I-INFO, telnet service enabled
%TCPIP-I-INFO, telnet (kerberos) service enabled
%TCPIP-S-STARTDONE, TCPIP$TELNET startup completed
```

    The information message confirms that the TELNET Kerberos service has been enabled.

3.4.7.2. Configuring and Enabling failSAFE IP Support

Two steps are necessary to configure failSAFE IP:

1. Configure the standby IP address on the interfaces for which failover is desired, as explained in Section 3.4.4.4; these are the failover target interfaces for each home interface.

2. Configure failSAFE IP support by choosing option 5 (Configure failSAFE IP) from the Optional Components Configuration menu.

In addition, you can configure failSAFE IP IPv6 addresses. Information about this is in Section 4.3.

Choosing option 5 from the Optional Components Configuration menu displays the following menu. Note that in this menu, Option 1 (Enable service on all nodes) appears only in a cluster configuration. Choose Option 1 to enable failSAFE IP on all nodes in the cluster, or choose option 2 to enable failSAFE IP on the local node only.

```
        failSAFE configuration options:
                 1 - Enable service on all nodes
                 2 - Enable service on this node
                 3 - Enable & Start service on this node
                [E] - Exit FAILSAFE configuration
Enter configuration option:
```

For more details about failSAFE IP, refer to the *VSI TCP/IP Services for OpenVMS Management* manual.

3.5. Using TCPIP$CONFIG Option Commands to Bypass TCPIP$CONFIG Menus

If you are an experienced TCP/IP Services user, you may want to bypass the configuration menus to enable or disable functionality, as follows:

1. Log in to the SYSTEM account.

2. Run the TCPIP$CONFIG command procedure and include appropriate options and keywords in the command line, using the following format:

```
@SYS$MANAGER:TCPIP$CONFIG [option] {DISABLE | ENABLE} [CLUSTER]
```

    In this format, *option* can be one of the options described in the following table. The table also describes the function of the DISABLE, ENABLE, and CLUSTER keywords.

Option	Description
ALL	Configures the core environment and all client and server services.
CLIENT	Configures all client services and related software.
MINIMUM	Configures the domain, Internet interfaces, Rlogin client, FTP client, FTP server, TELNET client, and TELNET server. Prompts you for optional components.
SERVER	Configures all servers and related software.
WORKSTATION	Configures the BIND resolver, the domain, dynamic routing, Internet interfaces, time zone, remote login, remote shell, remote executive, FTP client, FTP server, TELNET client, TELNET server, and SMTP.
Keyword	**Description**
CLUSTER	Configures all specified components clusterwide (except for the BIND server and SMTP, which you cannot configure clusterwide).
ENABLE	Enables the specified components.
DISABLE	Disables the specified components.

For example, the following command enables the client services for the entire cluster:

```
$ @SYS$MANAGER:TCPIP$CONFIG CLIENT ENABLE CLUSTER
```

Note

The procedure implements two levels of enabling and disabling: clusterwide and node specific (except for SMTP, which is configured and enabled as node specific only).

3.6. Making Configuration Changes Take Effect

Configuration changes made to TCP/IP Services software do not take effect until you start (or restart) the affected services. You may need to restart TCP/IP Services or simply the individual services affected, as explained in Table 3.3.

Table 3.3. Making Configuration Changes Take Effect

When you change the following services...	Do the following to make the changes take effect	Comments
Core environment (domain, Internet interface, routing, BIND resolver, time zone)	Start or restart the TCP/IP Services software.	Do this before you run tests (verification procedures) or customize the environment. Methods to start TCP/IP Services are described in Sections 3.8 and 3.11.

When you change the following services...	Do the following to make the changes take effect	Comments
Client, server, or optional services only	If you did not make changes to the core environment, you need only start or restart each affected service individually. Do this by choosing the Start service option in the service's configuration menu. Alternatively, you can use each service's startup command procedure. If you also made changes to core environment services, start TCP/IP Services.	Usage of startup command procedures for individual services is explained in Section 3.11.3.

Note

You can have the TCP/IP Services software started automatically each time the OpenVMS operating system is rebooted, or you can restart the software manually, as explained in Section 3.11.

3.7. Stopping TCP/IP Services Using TCPIP $CONFIG

Stop TCP/IP Services on your system by choosing option 5 (Shutdown VSI TCP/IP Services for OpenVMS) from the Main Configuration menu, as in the following example:

```
HP TCP/IP Services for OpenVMS Configuration Menu

    Configuration options:

            1  -  Core environment
            2  -  Client components
            3  -  Server components
            4  -  Optional components
            5  -  Shutdown HP TCP/IP Services for OpenVMS
            6  -  Startup HP TCP/IP Services for OpenVMS
            7  -  Run tests

            A  -  Configure options 1 - 4
           [E] -  Exit configuration procedure

Enter configuration option: 5
```

The TCP/IP Services shutdown procedure displays a series of messages similar to the following example (the messages displayed depend on the configuration):

```
Begin Shutdown...
%TCPIP-I-INFO, TCP/IP Services shutdown beginning at  5-SEP-2004
15:26:14.39
%TCPIP-S-SHUTDONE, TCPIP$FINGER shutdown completed
%TCPIP-S-SHUTDONE, TCPIP$FTP_CLIENT shutdown completed
%TCPIP-S-SHUTDONE, TCPIP$FTP shutdown completed
%TCPIP-S-SHUTDONE, TCPIP$INET_DRIVER shutdown completed
```

```
%TCPIP-S-SHUTDONE, TCPIP$METRIC shutdown completed
%TCPIP-S-SHUTDONE, TCPIP$NFS_CLIENT shutdown completed
%TCPIP-S-SHUTDONE, TCPIP$NFS shutdown completed
%TCPIP-S-SHUTDONE, TCPIP$NTP shutdown completed
%TCPIP-S-SHUTDONE, TCPIP$PCNFS shutdown completed
%TCPIP-S-SHUTDONE, TCPIP$POP shutdown completed
%TCPIP-S-SHUTDONE, TCPIP$PORTMAPPER shutdown completed
%TCPIP-S-SHUTDONE, TCPIP$PROXY shutdown completed
%TCPIP-S-SHUTDONE, TCPIP$PWIP_DRIVER shutdown completed
%TCPIP-S-SHUTDONE, TCPIP$REXEC shutdown completed
%TCPIP-S-SHUTDONE, TCPIP$RLOGIN shutdown completed
%TCPIP-S-SHUTDONE, TCPIP$RSH shutdown completed
%TCPIP-S-SHUTDONE, TCPIP$SMTP shutdown completed
%TCPIP-S-SHUTDONE, TCPIP$SNMP shutdown completed
%TCPIP-S-SHUTDONE, TCPIP$SSH_CLIENT shutdown completed
%TCPIP-S-SHUTDONE, TCPIP$SSH shutdown completed
%TCPIP-S-SHUTDONE, TCPIP$TELNET shutdown completed
%TCPIP-S-SHUTDONE, TCPIP$TFTP shutdown completed
%TCPIP-S-SHUTDONE, TCPIP$XDM shutdown completed
%TCPIP-I-SERVSTOPPED, BIND service already stopped
%TCPIP-S-SHUTDONE, TCPIP$BIND shutdown completed
%TCPIP-S-SHUTDONE, TCP/IP Kernel shutdown completed
%TCPIP-S-SHUTDONE, TCP/IP Services shutdown completed at  5-SEP-2004
15:26:17.78
Shutdown request completed.
```

3.8. Starting TCP/IP Services Using TCPIP $CONFIG

After configuring the core environment, start TCP/IP Services on your system by choosing option 6 (Startup VSI TCP/IP Services for OpenVMS) from the Main Configuration menu, as in the following example:

```
HP TCP/IP Services for OpenVMS Configuration Menu

    Configuration options:

            1  -  Core environment
            2  -  Client components
            3  -  Server components
            4  -  Optional components
            5  -  Shutdown HP TCP/IP Services for OpenVMS
            6  -  Startup HP TCP/IP Services for OpenVMS
            7  -  Run tests

            A  -  Configure options 1 - 4
           [E] -  Exit configuration procedure

Enter configuration option: 6
```

The TCP/IP Services startup procedure displays a series of messages similar to the following example (the messages displayed depend on the configuration):

```
Begin Startup...
%TCPIP-I-INFO, TCP/IP Services startup beginning at 5-SEP-2004
15:27:08.34
```

```
%TCPIP-I-NORMAL, timezone information verified
%RUN-S-PROC_ID, identification of created process is 00000D42
%TCPIP-I-SETLOCAL, setting domain and/or local host
%TCPIP-I-STARTCOMM, starting communication
%TCPIP-I-SETPROTP, setting protocol parameters
%TCPIP-I-DEFINTE, defining interfaces
%TCPIP-I-STARTNAME, starting name service
%TCPIP-I-STARTDROUT, starting dynamic routing
%RUN-S-PROC_ID, identification of created process is 00000C4E
%TCPIP-S-STARTDONE, TCP/IP Kernel startup completed
%TCPIP-S-STARTDONE, TCPIP$BIND startup completed
%TCPIP-I-PROXYLOADED, loaded 0 NFS proxy records
%TCPIP-I-LOADSERV, loading TCPIP server proxy information
%TCPIP-I-SERVLOADED, auxiliary server loaded with 0 proxy records
-TCPIP-I-SERVSKIP, skipped 0 communication proxy records
-TCPIP-I-SERVTOTAL, total of 0 proxy records read
%TCPIP-S-STARTDONE, TCPIP$PROXY startup completed
%TCPIP-S-STARTDONE, TCPIP$PORTMAPPER startup completed
%TCPIP-S-STARTDONE, TCPIP$FINGER startup completed
%TCPIP-S-STARTDONE, TCPIP$FTP startup completed
%TCPIP-S-STARTDONE, TCPIP$FTP_CLIENT startup completed
%TCPIP-S-STARTDONE, TCPIP$INET_DRIVER startup completed
%TCPIP-S-STARTDONE, TCPIP$METRIC startup completed
%TCPIP-I-NOMAP, no filesystem mapping information available
%TCPIP-S-STARTDONE, TCPIP$NFS startup completed
%TCPIP-S-STARTDONE, TCPIP$NFS_CLIENT startup completed
%TCPIP-S-STARTDONE, TCPIP$NTP startup completed
%TCPIP-S-STARTDONE, TCPIP$PCNFS startup completed
%TCPIP-S-STARTDONE, TCPIP$POP startup completed
%RUN-S-PROC_ID, identification of created process is 000002DC
%TCPIP-S-STARTDONE, TCPIP$PWIP_DRIVER startup completed
%TCPIP-S-STARTDONE, TCPIP$REXEC startup completed
%TCPIP-S-STARTDONE, TCPIP$RLOGIN startup completed
%TCPIP-S-STARTDONE, TCPIP$RSH startup completed
%TCPIP-S-STARTDONE, TCPIP$SMTP startup completed
%TCPIP-S-STARTDONE, TCPIP$SSH startup completed
%TCPIP-S-STARTDONE, TCPIP$SSH_CLIENT startup completed
%TCPIP-S-STARTDONE, TCPIP$TELNET startup completed
%TCPIP-S-STARTDONE, TCPIP$TFTP startup completed
%TCPIP-S-STARTDONE, TCPIP$XDM startup completed
%TCPIP-S-STARTDONE, TCP/IP Services startup completed at 5-SEP-2004
15:27:50.47
Startup request completed.
Press Return to continue ...
```

Note

The TCPIP-I-NOMAP message in this example appears only if no file systems are mapped in the TCP/IP configuration database. If you need NFS services, set up mapping to a valid file system, as explained in the *VSI TCP/IP Services for OpenVMS Management* manual. If you do not need NFS services, you can safely ignore this message; you can prevent recurrence of this message during future startups by disabling the NFS server using the TCPIP$CONFIG configuration procedure.

3.9. Verifying the Configuration

You can verify the configuration by running the installation verification procedure (IVP).

You should run the IVP if any of the following apply:

- You loaded the Product Authorization Key (PAK), and you want to verify that the lower-layer software and the Portmapper service are installed correctly.
- You did not load the PAK, but you want to verify that TCP/IP Services is installed correctly for DECwindows to display the TCP/IP Services applications.
- You require the software to transfer device socket packets that continuously vary in size between a sender and a receiver.
- You need to test the Portmapper service with a pair of client/server programs. The IVP reports the time it took to run the test to SYS$OUTPUT.
- You need to test your SNMP service.

Before you run the IVP, make sure TCP/IP Services has started and you have SYSPRV, OPER, NETMBX, and TMPMBX privileges.

You can run the IVP from the TCPIP$CONFIG configuration procedure or by command line at the OpenVMS DCL prompt. When you run the IVP from TCPIP$CONFIG, you have the option of running an additional test that verifies the SNMP configuration.

3.9.1. Running the IVP from the TCPIP$CONFIG Command Procedure

In the TCP/IP Services for OpenVMS Main Configuration menu, choose option 7 (Run tests). The Test menu appears, as in the following example:

```
HP TCP/IP Services for OpenVMS TEST Menu
        Test options:
                  1  -  Internet IVP
                  2  -  SNMP IVP
                  A  -  Tests 1 - 2
                 [E] -  Exit menu
Enter test option:
```

Choose the appropriate option for the test you want to perform.

3.9.2. Running the IVP from the OpenVMS DCL Prompt

To run the IVP at the DCL prompt, any time after exiting the configuration procedure, enter the following command. This procedure performs the same test as option 1 (Internet IVP) of the TCPIP $CONFIG Test menu.

```
$ @SYS$TEST:TCPIP$IVP
```

3.9.3. Verifying the TCP/IP Services Internet Configuration

When you choose either option 1 or option A from the TCPIP$CONFIG Test menu, or if you run the TCPIP$IVP command procedure at the command line, the IVP tests the basic TCP/IP Services software configuration, as in the following example. Here, the test completes successfully:

```
Enter test option: 1 Return
```

```
Begin IVP...
%%% TCPIP IVP: started %%%
UDP/IP test started at 5-SEP-2004 16:13:03.62
UDP/IP test ended at 5-SEP-2004 16:13:03.69
UDP/IP transferred successfully in 0 seconds 4198400 bytes
TCP/IP test started at 5-SEP-2004 16:13:04.20
TCP/IP test ended at 5-SEP-2004 16:13:04:28
TCP/IP transferred successfully in 0 seconds 4198400 bytes
RAW_IP test started at 5-SEP-2004 16:13:41.71
RAW_IP test ended at 5-SEP-2004 16:13:41.72
RAW_IP transferred successfully in 0 seconds 251000 bytes
%%% TCPIP IVP: completed successfully %%%
IVP request completed.
Press Return to continue ...
```

If the IVP does not complete successfully, the procedure displays error messages. All IVP errors use the same format as OpenVMS system messages. For example:

```
%TCPIP-E-IDENT, explanation of error.
```

Table 3.4 lists some common problems that cause IVP error messages. If the recommended action does not correct the problem, contact your VSI support representative.

Table 3.4. Troubleshooting IVP Errors

If the problem is...	Do the following...
Network configuration is incorrect.	Shut down TCP/IP Services and rerun the configuration procedure.
Startup fails.	Check the system parameters in the MODPARAMS.DAT file and adjust them if necessary. (See Section 1.2.7.) Then shut down and restart TCP/IP Services.
Installation kit is defective.	Request a replacement kit.
IVP fails because the PAK is missing.	Register a TCP/IP Services for OpenVMS PAK.

3.9.4. Verifying the SNMP Configuration

If you choose either option 2 or option A from the TCPIP$CONFIG Test menu, the IVP tests the SNMP service, as in the following example:

```
Begin SNMP IVP...
The SNMP IVP requires that TCPIP/IP Services be running.
It performs the following startups and shutdowns on the
SNMP service only (other TCP/IP services are not affected):
- If SNMP is running, shuts down SNMP before initial
  configuration
- Starts SNMP and runs tests
- Shuts down SNMP and restores initial configuration
- Before exiting, starts SNMP
Shutting down the SNMP service... done.
Creating temporary read/write community SNMPIVP_6520.
Enabling SET operations.
Starting up the SNMP service... done.
      Saving sysContact: Ralph Nickleby
```

```
  Setting sysContact to: Julius Caesar
   Retrieved sysContact: Julius Caesar
(Retrieved value matches SET value.)
Restoring sysContact to: Ralph Nickleby
    Saving snmpEnableAuthenTraps: 2 (disabled)
Setting snmpEnableAuthenTraps to: 1 (enabled)
 Retrieved snmpEnableAuthenTraps: 1 (enabled)
(Retrieved value matches SET value.)
 Restoring snmpEnableAuthenTraps: 2 (disabled)
Disabling SET operations.
Deleting temporary read/write community SNMPIVP_6520.
Shutting down and restarting the SNMP service...
Shutting down the SNMP service... done.
Starting up the SNMP service... done.
SNMP IVP request completed.
Press Return to continue ...
```

If one of the SNMP tests fails, you will see messages such as the following:

```
SNMPIVP: unexpected text in response to SNMP request:
"No reply."
See file SYS$SYSDEVICE:[TCPIP$SNMP]TCPIP$SNMP_REQUEST.DAT for more
details.
Verify that SNMP trace is not enabled.
sysContact could not be retrieved. Status = 0
The SNMP IVP has NOT completed successfully.
```

In this case, the error could indicate that not all SNMP components have started, or that SNMP tracing is enabled and needs to be disabled. For information about SNMP trace, refer to the *VSI TCP/IP Services for OpenVMS Management* manual.

Note

If `options debug` is listed in the `resolv.conf` file, the SNMP ivp will fail. Refer to the Release Notes for further information.

3.10. Additional Configuration Tasks

After you run TCPIP$CONFIG and enable the functionality and components appropriate for your network, you need to complete additional configuration tasks to enable access to product applications. TCP/IP Services provides a management command interface and logical names you can use to modify or customize the software for your environment.

The additional configuration tasks include:

- Populating databases (for example, for BIND and DHCP)
- Setting up user accounts
- Setting up communication and NFS proxies
- Defining print queues
- Setting up, exporting, and maintaining file systems
- Tuning the system for optimum performance

Many of the services require additional configuration or optimization. For more information about how to configure each service, refer to the *VSI TCP/IP Services for OpenVMS Management* manual.

3.11. Starting and Stopping TCP/IP Services

You can use commands in your OpenVMS startup file to have TCP/IP Services started and stopped automatically when the OpenVMS system starts up or shuts down, as explained in Section 3.11.1. These commands start and stop all the TCP/IP Services components installed on your system. Alternatively, you can start and stop individual TCP/IP Services client or server services without affecting other TCP/IP Services components currently running. For information about starting and stopping individual services, see Section 3.11.3.

If necessary, you can start and stop TCP/IP Services manually, as explained in Section 3.11.2. You can also start and stop user-written services, as explained in Section 3.11.4.

3.11.1. Automatically Starting and Stopping TCP/IP Services

To allow TCP/IP Services software to start automatically when the system starts up, and to stop automatically when the system shuts down, edit the SYS$COMMON:[SYSMGR]SYSTARTUP_VMS.COM file to remove the exclamation point (!) from the beginning of the following line:

```
$!$ @SYS$STARTUP:TCPIP$STARTUP.COM
```

If your system had earlier versions of TCP/IP Services, UCX$STARTUP.COM and UCX $SHUTDOWN.COM files might be present. These are no longer applicable; delete any definition of them from SYS$MANAGER:SYSTARTUP_VMS.COM.

If you want TCP/IP Services to start after you log in to your OpenVMS account, the OpenVMS systemwide login procedure (typically SYS$MANAGER:SYLOGIN.COM) must have world read and execute protections (W:RE).

To display the current protections, enter the following command:

```
$ DIR/PROTECTION SYS$MANAGER:SYLOGIN.COM
```

For information about protections, refer to the OpenVMS documentation.

3.11.2. Starting and Stopping TCP/IP Services Manually

To start TCP/IP Services manually, enter the following command:

```
$ @SYS$STARTUP:TCPIP$STARTUP
```

To stop TCP/IP Services manually, enter the following command:

```
$ @SYS$STARTUP:TCPIP$SHUTDOWN
```

3.11.3. Starting and Stopping Individual Services

On a system already running TCP/IP Services, you can configure an individual server or client component without affecting the other TCP/IP Services components running on your system and without having to restart TCP/IP Services.

Most services can be shut down and started independently. This is useful when you change parameters or logical names that require the service to be restarted.

The following files are provided:

- SYS$STARTUP:TCPIP$ *service*_STARTUP.COM allows you to start the *service* service.
- SYS$STARTUP:TCPIP$ *service*_SHUTDOWN.COM allows you to shut down the *service* service.

To preserve site-specific parameter settings and commands, create the following files. These files are not overwritten when you reinstall TCP/IP Services:

- SYS$STARTUP:TCPIP$ *service*_SYSTARTUP.COM can be used as a repository for site-specific definitions and parameters to be invoked when *service* is started.
- SYS$STARTUP:TCPIP$ *service*_SYSHUTDOWN.COM can be used as a repository for site-specific definitions and parameters to be invoked when *service* is shut down.

In these file names, *service* is the name of the service to be started or shut down. For example, use TCPIP$NTP_SHUTDOWN to shut down the NTP service.

For more information, refer to the *VSI TCP/IP Services for OpenVMS Management* manual.

3.11.4. Starting and Stopping User-Written Services

TCP/IP Services supplies command procedures for starting and stopping user-written services. To start a user-written service, enter the following command:

```
$ SYS$STARTUP:TCPIP$CUSTOMER_SERVICE_STARTUP service
```

To stop the user-written service, enter the following command:

```
$ SYS$STARTUP:TCPIP$CUSTOMER_SERVICE_SHUTDOWN service
```

In either command, specify the name of the service as defined using the TCP/IP management command SET SERVICE.

Note

Remember that any service name with lowercase characters is interpreted by the startup and shutdown procedures as uppercase unless you enclose the name in quotation marks. If you defined the service using quotation marks to preserve the case, be sure to use quotation marks when you specify the service name with the startup or shutdown command.

3.12. Specifying TCP/IP Services as the Transport for DECwindows Applications

To enable TCP/IP Services as the transport interface for DECwindows applications, add the following line to the SYS$MANAGER:DECW$PRIVATE_SERVER_SETUP.COM command procedure:

```
$ DECW$SERVER_TRANSPORTS == "DECNET,LOCAL,TCPIP"
```

Then restart DECwindows:

```
$ @SYS$STARTUP:DECW$STARTUP RESTART
```

If DECnet or DECnet-Plus software runs on the system, start it.

To display DECwindows applications from a DECwindows client (remote host) to a DECwindows server (your workstation), proceed as follows:

1. Set up security on the remote host.
2. Add the remote client to the local hosts database.
3. Add to SYS$MANAGER:DECW$PRIVATE_SERVER_SETUP.COM the following line:

   ```
   $ DECW$SERVER_TRANSPORTS == "DECNET,LOCAL,TCPIP"
   ```

4. Set the display for the applications to the remote host:

   ```
   $ SET DISPLAY/CREATE/NODE=remote-host/TRANSPORT=TCPIP
   ```

Chapter 4. Configuring IPv6

After configuring TCP/IP Services for OpenVMS with the TCPIP$CONFIG.COM command procedure, you can configure your system to communicate in an IPv6 network environment by performing the tasks described in this chapter.

Starting with Version 5.5, TCP/IP Services introduced many significant changes and improvements to the IPv6 configuration procedure (TCPIP$IP6_SETUP.COM). For instructions on configuring your node as an IPv6 host or router, use the documentation in this chapter rather than that provided in the *VSI TCP/IP Services for OpenVMS Guide to IPv6*.

The following table describes each section in this chapter and, where relevant, indicates the section of the *VSI TCP/IP Services for OpenVMS Guide to IPv6* that it replaces. The section on configuring failSAFE IP IPv6 addresses is newly documented with this release of TCP/IP Services for OpenVMS. For information about IPv6 concepts and processes, DNS domain name and address registration, and so forth, continue to refer to Chapter 2 of the *VSI TCP/IP Services for OpenVMS Guide to IPv6*.

Section...	**Describes....**	**Replaces *VSI TCP/IP Services for OpenVMS Guide to IPv6* Section ...**
4.1	How to configure your system as an IPv6 host.	2.5.1
4.2	How to configure your system as an IPv6 router.	2.6.1
4.3	How to configure failSAFE IP IPv6 addresses.	N/A

You can configure your node as either an IPv6 host or IPv6 router. You make this choice while running the IPv6 configuration procedure (TCPIP$IP6_SETUP.COM). After you run this configuration procedure and restart TCP/IP Services, IPv6 processes associated with your choices are started on your system.

Note

Before running the TCPIP$IP6_SETUP.COM configuration procedure, IPv4 must already be configured on your system. (The TCPIP$CONFIG.COM configuration procedure configures IPv4.)

If you are upgrading TCP/IP Services from a previous release, you must run the TCPIP $IP6_SETUP.COM configuration procedure again.

The IPv6 configuration procedure requires you to specify:

- Whether the system is to be configured as an IPv6 host or an IPv6 router.
- Whether the system needs a 6to4 interface (required for communicating between IPv4-only networks and IPv6 sites). If so, you must specify the system's IPv4 address, the 6to4 tunnel address prefix, whether the system will support a 6to4 relay router and, if applicable, the address of a relay router.
- You must specify the interface names of interfaces that will be enabled for IPv6.
- Whether to configure an automatic tunnel. If so, you must also specify the IPv4 address of the tunnel's endpoint.

- You must specify whether the system requires IPv6-over-IPv4 tunnels. For each tunnel, you need to supply the tunnel's source IPv4 address, the tunnel's destination IPv4 address, and the address prefix for the IPv6-over-IPv4 tunnel. You can create multiple IPv6-over-IPv4 tunnels.
- Whether the system requires IPv6-over-IPv6 tunnels. For each tunnel, you must supply the tunnel's source IPv6 address, the tunnel's destination IPv6 address, and the address prefix for the IPv6-over-IPv6 tunnel. You can create multiple IPv6-over-IPv6 tunnels.
- Whether the system requires manual IPv6 routes. For each route, you must supply the address prefix of the destination IPv6 network, the interface to use to send traffic for the route, and the link-local IPv6 address of the first router in the path or the IPv4-compatible IPv6 address of the automatic tunnel to use. You can create multiple manual IPv6 routes.
- For an IPv6 router, you also must specify:
  - Whether to enable the RIPng protocol on each interface.
  - Whether to advertise an IPv6 address prefix on each interface and, if so, the IPv6 address prefix.
  - For each tunnel you create, whether to enable the RIPng protocol on the tunnel, whether to advertise an IPv6 address prefix on the tunnel interface, and if so, the IPv6 address prefix.
  - For each manual route you create, the interface to use to forward traffic to the remote IPv6 network.

After you use the TCPIP$IP6_SETUP.COM configuration procedure to configure your system as an IPv6 host or router, you can optionally configure your system as a BIND server (see the *VSI TCP/IP Services for OpenVMS Guide to IPv6*). In addition, you can configure failSAFE IP IPv6 addresses, as explained in Section 4.3.

Once you configure IPv6 using the TCPIP$IP6_SETUP.COM configuration procedure, you must enable IPv6 on your system by shutting down and restarting TCP/IP Services.

You can make other changes to your IPv6 configuration later. Chapter 4 of the *VSI TCP/IP Services for OpenVMS Guide to IPv6* describes how to make further changes.

4.1. Configuring an IPv6 Host

To configure your system as an IPv6 host, do the following:

1. Invoke the TCPIP$IP6_SETUP.COM configuration procedure by entering the following command:

   ```
   $ @SYS$MANAGER:TCPIP$IP6_SETUP
   ```

   The procedure displays information about the IPv6 network configuration procedure and tells you that you can configure the system as either an IPv6 host or an IPv6 router.

2. Choose to configure the system as an IPv6 host by taking the default to the following prompt (press Enter or enter NO):

   ```
   Configure this system as an IPv6 router? [NO]:
   ```

3. At the following prompt, indicate whether you want to configure a 6to4 interface:

   ```
   Configure a 6to4 interface? [NO]:
   ```

A 6to4 interface is needed if this host is connected to an IPv4-only network and needs to communicate with other 6to4 or native IPv6 sites. If this system is a host within a 6to4 site, do not create a 6to4 interface; a 6to4 address is automatically configured on this system using standard IPv6 mechanisms.

If you do not want to configure a 6to4 interface, press Enter. The configuration procedure continues at step 8.

If you want to configure a 6to4 interface, enter YES. The configuration procedure then displays the 6to4 tunnel interface:

```
The 6to4 tunnel is: TN1
```

You are prompted to enter information about the interface in subsequent steps.

4. Enter this host's IPv4 address:

```
Enter this node's IPv4 address to use when generating your site's
6to4 prefix:
```

Enter the IPv4 address in dotted-decimal format (*d.d.d.d*). The configuration procedure automatically generates a 6to4 site prefix based on the IPv4 address entered, and displays the prefix as in the following example:

```
Your 6to4 site prefix is: 2002:x:x::/48
```

5. Enter the address prefix for the 6to4 tunnel in response to the following prompt:

```
Enter an address prefix to use on interface
TN1 [2002:x:x::/64]
```

To accept the IPv6 address prefix generated in step 4, take the default.

Note

The high-order 48 bits of the 6to4 address prefix must be the same as your 6to4 site prefix.

---

6. Indicate whether you want to configure a 6to4 relay router:

```
Configure a 6to4 relay router? [NO]:
```

A relay router is needed to connect your system to native IPv6 sites. If you do not configure a relay router, your system can connect to other 6to4 sites but not to native IPv6 sites.

If you do not want to configure a 6to4 relay router, press Enter. The configuration procedure continues at step 8.

If you want to configure a 6to4 relay router, enter YES.

7. Specify the address of a relay router:

```
Enter the 6to4 address of a 6to4 relay router
[2002:C058:6301::]:
```

The address of the default relay router is displayed. To use the default, press Enter. Otherwise, enter the 6to4 unicast address of a 6to4 relay router.

8. For each interface on your system, the configuration procedure asks whether you want to enable IPv6 on that interface, as in the following example, where *ddn* is the interface name (such as WE0):

   ```
   Enable IPv6 on interface ddn? [YES]:
   ```

   If you want to enable IPv6 on this interface, press Enter; if you do not, enter NO.

   If your system has multiple interfaces, the procedure repeats this question for each interface.

9. Indicate whether you want to configure an automatic tunnel:

   ```
   Configure an IPv6 over IPv4 automatic tunnel interface? [NO]:
   ```

   If you do not want to configure an automatic tunnel, press Enter; the procedure continues at step 11. If you want to configure an automatic tunnel, enter YES; the procedure displays the automatic tunnel interface as in the following example. In step 10, the procedure prompts you for the tunnel's address.

   ```
   The automatic tunnel is: TN0
   ```

Note

Because of potential IPv4-compatible address routing problems, VSI recommends that you avoid using automatic tunnels.

10. Enter the IPv4 address to use when constructing the automatic tunnel's endpoint:

    ```
    Enter this node's IPv4 address to use when creating
    your automatic tunnel:
    ```

    Enter the IPv4 address in dotted-decimal format (*d.d.d.d*).

11. The configuration procedure asks whether you want to create an IPv6-over-IPv4 configured tunnel:

    ```
    Create IPv6 over IPv4 configured tunnels? [NO]:
    ```

    If you want to create an IPv6-over-IPv4 configured tunnel, enter YES. You are prompted for information about this tunnel in subsequent steps.

    If you do not want to create an IPv6-over-IPv4 configured tunnel, press Enter; the procedure continues at step 16.

12. Enter the tunnel's source IPv4 address in response to the following prompt:

    ```
    Enter the source IPv4 address of tunnel ITn:
    ```

    Enter the tunnel's source IPv4 address in the dotted-decimal format (*d.d.d.d*).

13. Enter the tunnel's destination IPv4 address in response to the following prompt:

    ```
    Enter the destination IPv4 address of tunnel ITn:
    ```

    Enter the tunnel's destination IPv4 address in dotted-decimal format *d.d.d.d*. The tunnel's destination address must differ from the source address entered in step 12.

14. Enter an address prefix to use on the tunnel interface:

    ```
    Enter an address prefix to use on interface ITn [DONE]:
    ```

If a router is not advertising a global address prefix on this tunnel interface, enter a 64-bit address prefix. You can configure multiple address prefixes for this configured tunnel. You are prompted for additional address prefixes until you enter DONE.

If you do not want the host to use an IPv6 address prefix on the tunnel interface, press Enter.

15. The configuration procedure asks whether you want to create another IPv6-over-IPv4 configured tunnel:

    ```
    Create another IPv6 over IPv4 configured tunnel? [NO]:
    ```

    If you want to create another IPv6-over-IPv4 configured tunnel, enter YES. The procedure repeats steps 12 through 14 for each additional configured tunnel you choose to create.

    If you do not want to create another IPv6-over-IPv4 configured tunnel, press Enter. The procedure continues at step 16.

16. Indicate whether you want to create an IPv6-over-IPv6 configured tunnel:

    ```
    Create IPv6 over IPv6 configured tunnels? [NO]:
    ```

    If you want to create an IPv6-over-IPv6 configured tunnel, enter YES. You are prompted to enter information about this tunnel in subsequent steps.

    If you do not want to create an IPv6-over-IPv6 configured tunnel, press Enter; the configuration procedure continues at step 21.

17. Enter the tunnel's source IPv6 address in response to the following prompt:

    ```
    Enter the source IPv6 address of tunnel ITn:
    ```

    Enter the tunnel's source IPv6 address in the dotted-decimal format (*d.d.d.d*).

18. Enter the IPv6-over-IPv6 tunnel's destination IPv6 address in response to the following prompt:

    ```
    Enter the destination IPv6 address of tunnel ITn:
    ```

    Enter an IPv6 address in dotted-decimal format *d.d.d.d*. The tunnel's destination address must differ from the source address entered in step 17.

19. Enter an address prefix to use on the tunnel interface:

    ```
    Enter an address prefix to use on interface ITn [DONE]:
    ```

    If a router is not advertising a global address prefix on this tunnel interface, enter a 64-bit address prefix. You can configure multiple address prefixes for this configured tunnel. You are prompted for additional address prefixes until you enter DONE.

    If you do not want the host to use an IPv6 address prefix on the tunnel interface, press Enter.

20. The configuration procedure asks whether you want to create another IPv6-over-IPv6 configured tunnel:

    ```
    Create another IPv6 over IPv6 configured tunnel? [NO]:
    ```

    If you want to create another IPv6-over-IPv6 configured tunnel, enter YES. The procedure repeats steps 17 through 19 for each additional configured tunnel you choose to create.

If you do not want to create another IPv6-over-IPv6 configured tunnel, press Enter.

21. The procedure asks whether you want to configure manual IPv6 routes.

```
Configure manual IPv6 routes? [NO]:
```

If you want to configure a manual IPv6 route to an adjacent router or remote IPv6 network, enter YES; subsequent prompts ask you for information about the route. Otherwise, press Enter; the configuration procedure continues at step 26.

22. Indicate the address prefix of a destination IPv6 network:

```
Enter the destination network address prefix:
```

Enter the IPv6 address prefix of the destination IPv6 network, or enter DEFAULT for the default route.

23. Enter the name of the interface through which you will send traffic to the remote IPv6 network:

```
Enter interface to use when forwarding messages:
```

24. Enter the link-local IPv6 address of the first router in the path to the destination network. This address along with the IPv6 address prefix constitute the static routing table entry.

```
Enter the next node's IPv6 address:
```

If the next node is on the same link as this node or is reachable through a configured tunnel, enter the link-local address. If the next node is reachable through an automatic tunnel, enter the IPv4-compatible IPv6 address. For all other connections, enter the IPv6 address.

25. Indicate whether you want to define another manual route to an adjacent router or remote IPv6 network:

```
Configure another manual IPv6 route? [NO]:
```

If you want to define another manual route, enter YES. The configuration procedure repeats steps 22 through 24 for each additional manual IPv6 route you choose to define. If you do not want to define another manual route, press Enter.

26. At this point, the configuration procedure displays a summary of your new IPv6 host configuration, as shown in the following example:

```
    You configured this node as an IPv6 host with the
    following:
Daemons:
  ND6HOST   Dynamic Updates Disabled
Interfaces:
  WE0       Dynamic Address Configuration Enabled
  TN1       6to4 Tunneling Enabled using 5.6.7.8
            Prefix 2002:506:708::/64
            Relay Router 2002:90A:B0C:1::1
Manual Routes:
  2002::/16                  TN1       FE80::5.6.7.8
  DEFAULT                    TN1       2002:90A:B0C:1::1
```

27. The configuration procedure asks whether you want to create a new host configuration file based on the choices you have made:

```
      Create new IPv6 network configuration files? [YES]:
```

If you are not satisfied with the configuration, enter NO; the configuration procedure ends immediately without changing the current IPv6 network configuration.

If you are satisfied with the configuration, press Enter. The configuration procedure creates a new host configuration file and displays the following information:

```
      A  new  IPv6  configuration  file,  SYS$SYSTEM:TCPIP
$INET6_CONFIG.DAT,
      has been created.  The previous configuration file  (if any)  has
 been
      renamed to SYS$SYSTEM:TCPIP$INET6_CONFIG.DAT_OLD.
      This new IPv6 network configuration will become active the  next
 time
      TCP/IP Services for OpenVMS is started.
```

4.2. Configuring an IPv6 Router

To configure your system as an IPv6 router, follow the steps provided in this section.

1. Invoke the TCPIP$IP6_SETUP.COM configuration procedure by entering the following command:

   ```
   $ @SYS$MANAGER:TCPIP$IP6_SETUP
   ```

   The procedure displays information about the IPv6 network configuration procedure and tells you that you can configure the system as either an IPv6 host or an IPv6 router.

2. Choose to configure the system as an IPv6 router by entering YES at the following prompt:

   ```
      Configure this system as an IPv6 router? [NO]:
   ```

3. Indicate whether you want to configure a 6to4 interface:

   ```
      Configure a 6to4 interface? [NO]:
   ```

   A 6to4 interface is needed to configure a border router. If you do not want to configure a 6to4 interface, press Enter. The configuration procedure continues at step 7.

   If you want to configure a 6to4 interface, enter YES. The configuration procedure then displays the 6to4 tunnel interface:

   ```
            The 6to4 tunnel is: TN1
   ```

   You are prompted to enter information about the interface in subsequent steps.

4. Enter the node's IPv4 address in response to the following prompt:

   ```
      Enter this node's IPv4 address to use when generating
      your site's 6to4 prefix:
   ```

   Enter the IPv4 address in dotted-decimal format (*d.d.d.d*). The configuration procedure automatically generates a 6to4 site prefix based on the IPv4 address entered, and displays the prefix as in the following example:

   ```
         Your 6to4 site prefix is: 2002:x:x::/48
   ```

This site prefix is advertised to hosts on the interfaces attached to the IPv6 site. This address must be a valid, globally unique IPv4 address configured on the router's interface to the IPv4 network.

5. The configuration procedure asks whether you want this system to function as a 6to4 relay router:

   ```
   Configure a 6to4 relay router? [NO]:
   ```

   If hosts in this border router's 6to4 site need to communicate with native IPv6 sites (IPv6 only), configure this system as a 6to4 relay router. Enter YES.

   If you do not want the system to function as a 6to4 relay router, press Enter. The configuration procedure continues at step 7.

6. Specify the address of a relay router:

   ```
   Enter 6to4 address of a 6to4 relay router
   [2002:C058:6301::]:
   ```

   The address of the default relay router is displayed. To use the default, press Enter. Otherwise, enter the 6to4 unicast address of a 6to4 relay router.

7. For each interface on your system, the procedure asks whether you want to enable IPv6 on that interface, as in the following example, where *ddn* is the interface name (such as WE0):

   ```
   Enable IPv6 on interface ddn [YES]?
   ```

   If you want to enable IPv6 on this interface, press Enter; if not, enter NO.

   For each interface on your system, the configuration procedure repeats steps 7 through 9.

8. Indicate whether you want the router to run the RIPng protocol on the designated interface:

   ```
   Enable RIPng on interface ddn? [YES]:
   ```

   The RIPng protocol allows this router to exchange IPv6 routes with other routers. If you want the router to run the RIPng protocol, press Enter; otherwise, enter NO.

9. The configuration procedure asks whether you want the router to advertise an IPv6 address prefix on the designated interface:

   ```
   Enter an address prefix to advertise on interface
   ddn [DONE]:
   ```

   If you want the router to advertise an IPv6 address prefix, enter a 64-bit address prefix for the interface. You can configure multiple address prefixes for this interface. You are prompted for additional address prefixes until you enter DONE.

   If you do not want the router to advertise an IPv6 address prefix on the designated interface, enter DONE.

10. Indicate whether you want to configure an automatic tunnel:

    ```
    Configure an IPv6 over IPv4 automatic tunnel interface? [NO]:
    ```

    If you do not want to configure an automatic tunnel, press Enter. The configuration procedure continues at step 12.

If you want to configure an automatic tunnel, enter YES; the procedure displays the automatic tunnel interface as in the following example, and in the next step prompts you for the tunnel's address.

```
The automatic tunnel is: TN0
```

Note

Because of potential IPv4-compatible address routing problems, VSI recommends that you avoid using automatic tunnels.

11. Enter the IPv4 address to use when constructing the automatic tunnel's endpoint:

    ```
    Enter the IPv4 address to use when creating
    your automatic tunnel:
    ```

    Enter the IPv4 address in dotted-decimal format (*d.d.d.d*).

12. The configuration procedure asks whether you want to create an IPv6-over-IPv4 configured tunnel:

    ```
    Create IPv6 over IPv4 configured tunnels? [NO]:
    ```

    If you want to create an IPv6-over-IPv4 configured tunnel, enter YES. You are prompted for information about this tunnel in subsequent steps.

    If you do not want to create an IPv6-over-IPv4 configured tunnel, press Enter; the procedure continues at step 18.

13. Enter the tunnel's source IPv4 address:

    ```
    Enter the source IPv4 address of tunnel ITn:
    ```

    Enter the tunnel's source IPv4 address in the dotted-decimal format (*d.d.d.d*).

14. Enter the tunnel's destination IPv4 address in response to the following prompt:

    ```
    Enter the destination IPv4 address of tunnel ITn:
    ```

    Enter an IPv4 address in dotted-decimal format *d.d.d.d*. The tunnel's destination address must differ from the source address entered in step 13.

15. Indicate whether you want to enable the RIPng protocol:

    ```
    Enable RIPng on interface ITn? [YES]:
    ```

    The RIPng protocol allows this router to exchange IPv6 routes with other routers. If you want to enable the RIPng protocol on the tunnel interface, press Enter; if you do not, enter NO.

16. Indicate whether you want the router to advertise an IPv6 address prefix on the tunnel interface:

    ```
    Enter an address prefix to advertise on interface ITn? [DONE]:
    ```

    If you want the router to advertise an IPv6 address prefix, enter a 64-bit address prefix for the designated interface. You can configure multiple address prefixes for this interface. You are prompted for additional address prefixes until you enter DONE.

    If you do not want the router to use an IPv6 address prefix on the tunnel interface, enter DONE.

17. The configuration procedure asks whether you want to create another IPv6-over-IPv4 configured tunnel:

    ```
    Create another IPv6 over IPv4 configured tunnel? [NO]:
    ```

    If you want to create another IPv6-over-IPv4 configured tunnel, enter YES. The procedure repeats steps 13 through 16 for each additional configured tunnel you choose to create.

    If you do not want to create another IPv6-over-IPv4 configured tunnel, press Enter.

18. The procedure asks whether you want to create an IPv6-over-IPv6 configured tunnel:

    ```
    Create IPv6 over IPv6 configured tunnels? [NO]:
    ```

    If you want to create an IPv6-over-IPv6 configured tunnel, enter YES. You are prompted to enter information about this tunnel in subsequent steps.

    If you do not want to create an IPv6-over-IPv6 configured tunnel, press Enter; the configuration procedure continues at step 24.

19. Enter the tunnel's source IPv6 address in response to the following prompt:

    ```
    Enter the source IPv6 address of tunnel ITn:
    ```

    Enter the tunnel's source IPv6 address in the dotted-decimal format (*d.d.d.d*).

20. Enter the IPv6-over-IPv6 tunnel's destination IPv6 address in response to the following prompt:

    ```
    Enter the destination IPv6 address of tunnel ITn:
    ```

    Enter an IPv6 address in dotted-decimal format *d.d.d.d*. The tunnel's destination address must differ from the source address entered in step 19.

21. Indicate whether you want to enable the RIPng protocol on the interface:

    ```
    Enable RIPng on interface ITn? [YES]:
    ```

    The RIPng protocol allows this router to exchange IPv6 routes with other routers. Press Enter if you want to enable the RIPng protocol on this interface; enter NO if you do not.

22. Indicate whether you want the router to advertise an IPv6 address prefix on the tunnel interface:

    ```
    Enter an address prefix to advertise on interface ITn? [DONE]:
    ```

    If you want the router to advertise an IPv6 address prefix, enter a 64-bit address prefix for the designated interface. You can configure multiple address prefixes for this interface. You are prompted for additional address prefixes until you enter DONE.

    If you do not want the router to use an IPv6 address prefix on the tunnel interface, enter DONE.

23. You are asked whether you want to create another IPv6-over-IPv6 configured tunnel:

    ```
    Create another IPv6 over IPv6 configured tunnel? [NO]:
    ```

    If you want to create another IPv6-over-IPv6 configured tunnel, enter YES. The procedure repeats steps 19 through 22 for each additional configured tunnel you choose to create.

    If you do not want to create another IPv6-over-IPv6 configured tunnel, press Enter.

24. Indicate whether you want to define manual routes to an adjacent router or remote IPv6 network:

```
Configure manual IPv6 routes? [NO]?
```

    If you want to define a manual IPv6 route, enter YES. In subsequent steps, the procedure asks you to specify information for that route.

    If you do not want to define manual routes, enter NO; the procedure continues at step 29.

25. Enter an address prefix of a destination IPv6 network:

```
Enter the destination network address prefix:
```

    Enter the address prefix of the destination IPv6 network, or enter DEFAULT for the default route.

26. Enter the name of the interface through which you will send traffic to the remote IPv6 network:

```
Enter interface to use when forwarding messages:
```

27. The procedure asks you to enter the link-local IPv6 address of the first router in the path to the destination network. This address along with the IPv6 address prefix constitute the static routing table entry.

```
Enter the next node's IPv6 address:
```

    If the next node is on the same link as this node or is reachable through a configured tunnel, enter the link-local address. If the next node is reachable through an automatic tunnel, enter the IPv4-compatible IPv6 address. For all other connections, enter the IPv6 address.

28. Indicate whether you want to configure another manual IPv6 route to an adjacent router or remote IPv6 network:

```
Configure another manual IPv6 route? [NO]:
```

    If you want to configure another manual route, enter YES. The configuration procedure repeats steps 25 through 27 for each additional manual IPv6 route you choose to configure. If you do not want to configure another manual route, press Enter.

29. At this point, the configuration procedure displays a summary of your new IPv6 router configuration, as shown in the following example:

```
    You configured this node as an IPv6 router with the
    following:
Daemons:
  IP6RTRD
Interfaces:
  WE0       RIP Enabled
  IT0       RIP Enabled
            Tunnel Source ::1
            Tunnel Destination ::2
            Prefix AAAA::/64
            Prefix BBBB::/64
  TN1       6to4 Tunneling Enabled using 1.2.3.4
            Relay Router 2002:C058:6301::
Manual Routes:
  ::4/64                    WE0       ::5
```

30. The configuration procedure asks whether you want to create router configuration files based on the choices you have made:

```
      Create new IPv6 network configuration files? [YES]:
```

    If you are not satisfied with the configuration, enter NO; the configuration procedure ends immediately without changing the current IPv6 network configuration.

    If you are satisfied with the configuration, press Enter. The configuration procedure creates new router configuration files and displays the following information:

```
      A  new  IPv6  configuration  file,  SYS$SYSTEM:TCPIP
$INET6_CONFIG.DAT,
      has been created.  The previous configuration file  (if any)  has
 been
      renamed to SYS$SYSTEM:TCPIP$INET6_CONFIG.DAT_OLD.
      A new IPv6 configuration file, SYS$SYSTEM:TCPIP$IP6RTRD.CONF, has
      been created.  The previous configuration file  (if any)  has been
      renamed to SYS$SYSTEM:TCPIP$IP6RTRD.CONF_OLD.
      This new IPv6 network configuration will become active the  next
 time
      TCP/IP Services for OpenVMS is started.
```

4.3. Configuring failSAFE IP IPv6 Addresses

Standby failSAFE IP IPv6 addresses must be configured manually. IPv6 supports addresses with various scopes; only link-local addresses need to be configured with standby addresses. (Link-local addresses are those that have high-order bits with the hexadecimal value FE80.)

To configure standby failSAFE IP IPv6 addresses, follow these steps:

1. Determine the link-local IPv6 addresses that have been dynamically created on each interface by using the `ifconfig` command, as in the following example. The last line for each interface contains the IPv6 link-local address. Note that the IPv4 addresses have already been configured with standby addresses. (The instructions for configuring IPv4 standby addresses are given in Section 3.4.4.4.)

```
$ ifconfig -a
IE0: flags=c43
<UP,BROADCAST,RUNNING,MULTICAST,SIMPLEX>
     failSAFE IP Addresses:
        inet 16.176.56.81 netmask fffffe00 broadcast 10.0.255.255 (on
 GRYFFIIE1)
    *inet 16.176.56.65 netmask ff000000 broadcast 16.255.255.255 ipmtu
 1500
    *inet6 fe80::202:a5ff:fe60:a368
IE1: flags=c43
<UP,BROADCAST,RUNNING,MULTICAST,SIMPLEX>
     failSAFE IP Addresses:
        inet 16.176.56.65 netmask fffffe00 broadcast 10.0.255.255 (on
 GRYFFIIE0)
    *inet 16.176.56.81 netmask fffffe00 broadcast 16.176.57.255 ipmtu
 1500
    *inet6 fe80::202:a5ff:fe60:a369
```

2. Create standby IPv6 addresses by executing the following commands, specifying the IPv6 addresses obtained in step 1:

```
$ ifconfig ie1 inet6 alias fe80::202:a5ff:fe60:a368
$ ifconfig ie0 inet6 alias fe80::202:a5ff:fe60:a369
```

In this example, the link-local IPv6 address configured on interface IE0 is added to IE1 as a standby. Similarly, the IPv6 address configured on interface IE1 is added to IE0 as a standby.

3. Restart the failSAFE IP service to make the configuration changes take effect (see Section 3.6). To make the changes take effect each time TCP/IP Services starts, edit SYS$STARTUP:TCPIP $SYSTARTUP.COM and add the following commands, which include the same `ifconfig` commands specified in step 2:

```
$!
$! IPv6 failSAFE Addresses
$!
$ ifconfig ie1 inet6 alias fe80::202:a5ff:fe60:a368
$ ifconfig ie0 inet6 alias fe80::202:a5ff:fe60:a369
$!
$! Restart failSAFE to pick up IPv6 address changes
$!
$ @sys$startup:tcpip$failsafe_shutdown
$ @sys$startup:tcpip$failsafe_startup
$!
```

Appendix A. Sample New TCP/IP Services Installation and Configuration

This appendix shows a sample installation and configuration of the TCP/IP Services product on a system on which the product has never been installed.

A.1. Sample New Installation Procedure

The following example shows a sample installation dialog for the TCP/IP Services. In this example, the installation takes place on an OpenVMS Alpha system on which the product has not been installed. If TCP/IP Services had been installed previously on the system, the installation dialog would differ slightly (see Chapter 2).

Note

The symbols *xx* in the following example represent the product's two-digit update version number.

Output for installations on OpenVMS I64 systems are similar. One difference is the TCP/IP Services product name: on OpenVMS I64 systems it is I64VMS TCPIP, while on OpenVMS Alpha systems it is DEC AXPVMS TCPIP (as shown in the following example).

```
Choose one or more items from the menu separated by commas: 1

The following product has been selected:
    DEC AXPVMS TCPIP V5.6-xx               Layered Product

Do you want to continue? [YES] Return

Configuration phase starting ...

You will be asked to choose options, if any, for each selected product and
 for
any products that may be installed to satisfy software dependency
 requirements.

DEC AXPVMS TCPIP V5.6-xx: HP TCP/IP Services for OpenVMS.

    Copyright 1976, 2006 Hewlett-Packard Development Company, L.P.

    Hewlett-Packard Development Company, L.P.
    HP TCP/IP Services for OpenVMS offers several license options.

Do you want the defaults for all options? [YES] Return

Do you want to review the options? [NO] Return

Execution phase starting ...
The following product will be installed to destination:
    DEC AXPVMS TCPIP V5.6-xx             DISK$ALPHASYS:[VMS$COMMON.]

Portion done: 0%...10%...20%...30%...40%...50%...60%...70%...80%...90%
%PCSI-I-PRCOUTPUT, output from subprocess follows ...
% TCPIP-I-PCSI_INSTALL
```

```
% - Execute SYS$MANAGER:TCPIP$CONFIG.COM to proceed with configuration of
%   HP TCP/IP Services.
%

Portion done: 100%
The following product has been installed:
    DEC VAXVMS TCPIP V5.6-xx              Layered Product

DEC VAXVMS TCPIP V5.6-xx: HP TCP/IP Services for OpenVMS.

    Check the release notes for current status of the product.
$
```

A.2. Sample New Configuration Procedure

The following example shows a sample configuration dialog for the TCP/IP Services, in which the following components are configured:

- Core environment
- TELNET client
- FTP server

In this example, the configuration takes place on a system on which the product has never been configured. If TCP/IP Services had been configured previously on the system, the dialog would differ significantly (see Chapter 3).

```
        HP TCP/IP Services for OpenVMS Configuration Menu
        Configuration options:
                 1  -  Core environment
                 2  -  Client components
                 3  -  Server components
                 4  -  Optional components
                 5  -  Shutdown HP TCP/IP Services for OpenVMS
                 6  -  Startup HP TCP/IP Services for OpenVMS
                 7  -  Run tests
                 A  -  Configure options 1 - 4
                [E] -  Exit configuration procedure
Enter configuration option: 1
        HP TCP/IP Services for OpenVMS Core Environment Configuration Menu
        Configuration options:
                 1  -  Domain
                 2  -  Interfaces
                 3  -  Routing
                 4  -  BIND Resolver
                 5  -  Time Zone
                 A  -  Configure options 1 - 5
                [E] -  Exit menu
Enter configuration option: 1
        HP TCP/IP Services for OpenVMS Core Environment Configuration Menu
        Configuration options:
                 1  -  Domain
                 2  -  Interfaces
                 3  -  Routing
                 4  -  BIND Resolver
                 5  -  Time Zone
                 A  -  Configure options 1 - 5
```

```
                [E] -  Exit menu
Enter configuration option: 1
DOMAIN Configuration
Enter Internet domain: yourdomain.com
        HP TCP/IP Services for OpenVMS Core Environment Configuration Menu
        Configuration options:
                 1  -  Domain
                 2  -  Interfaces
                 3  -  Routing
                 4  -  BIND Resolver
                 5  -  Time Zone
                 A  -  Configure options 1 - 5
                [E] -  Exit menu
Enter configuration option: 2
      HP TCP/IP Services for OpenVMS Interface & Address Configuration Menu
 Hostname Details: Configured=Not Configured, Active=Not Configured
 Configuration options:
   1  -  WE0 Menu (EWA0: TwistedPair 100mbps)
   2  -  IE0 Menu (EIA0: TwistedPair 100mbps)
   3  -  IE1 Menu (EIB0: TwistedPair 100mbps)
  [E] -  Exit menu
Enter configuration option: 1
      HP TCP/IP Services for OpenVMS Interface WE0 Configuration Menu
 Configuration options:
         1  - Add a primary address on WE0
         2  - Add an alias address on WE0
         3  - Enable DHCP client to manage address on WE0
        [E] - Exit menu
Enter configuration option: 1
      HP TCP/IP Services for OpenVMS Interface WE0 Configuration Menu
 Configuration options:
         1  - Add a primary address on WE0
         2  - Add an alias address on WE0
         3  - Enable DHCP client to manage address on WE0
        [E] - Exit menu
Enter configuration option: 1
    IPv4 Address may be entered with CIDR bits suffix.
    E.g. For a 16-bit netmask enter 10.0.1.1/16
Enter IPv4 Address []: 10.0.1.1/16
Enter hostname []: yourmachine
Requested configuration:
      Address  : 10.0.1.1/16
      Netmask  : 255.255.0.0 (CIDR bits: 16)
      Hostname : yourmachine
* Is this correct [YES]: Return
Added hostname yourmachine (10.0.1.1) to host database
NOTE:
  The system hostname is not configured.
  It will now be set to yourmachine (10.0.1.1).
  This can be changed later via the Interface Configuration Menu.
Updated system hostname in configuration database
Added address WE0:10.0.1.1 to configuration database
      HP TCP/IP Services for OpenVMS Interface & Address Configuration Menu
 Hostname Details: Configured=yourmachine, Active=Not Configured
 Configuration options:
   1  -  WE0 Menu (EWA0: TwistedPair 100mbps)
   2  -  10.0.1.1/16         yourmachine           Configured
   3  -  IE0 Menu (EIA0: TwistedPair 100mbps)
```

```
   4  -  IE1 Menu (EIB0: TwistedPair 100mbps)
  [E] -  Exit menu
Enter configuration option: Return
        HP TCP/IP Services for OpenVMS Core Environment Configuration Menu
        Configuration options:
                 1  -  Domain
                 2  -  Interfaces
                 3  -  Routing
                 4  -  BIND Resolver
                 5  -  Time Zone
                 A  -  Configure options 1 - 5
                [E] -  Exit menu
Enter configuration option: 3
DYNAMIC ROUTING Configuration
        Dynamic routing has not been configured.
        You may configure dynamic ROUTED or GATED routing.
        You cannot enable both at the same time.  If you want
        to change from one to the other, you must disable the
        current routing first, then enable the desired routing.
        If you enable dynamic ROUTED routing, this host will use the
        Routing Information Protocol (RIP) - Version 1 to listen
        for all dynamic routing information coming from other
        hosts to update its internal routing tables.
        It will also supply its own Internet addresses to
        routing requests made from remote hosts.
        If you enable dynamic GATED routing, you will be able to
        configure this host to use any combination of the following
        routing protocols to exchange dynamic routing information
        with other hosts on the network:
            Routing Information Protocol (RIP) - Version 1 & 2
            Router Discovery Protocol (RDISC)
            Open Shortest Path First (OSPF)
            Exterior Gateway Protocol (EGP)
            Border Gateway Protocol (BGP-4)
            Static routes
* Do you want to configure dynamic ROUTED or GATED routing [NO]:
        A default route has not been configured.
* Do you want to configure a default route [YES]:
Enter your Default Gateway host name or address: yourgateway.yourdomain.com
        yourgateway.yourdomain.com is not in the local host database.
Enter Internet address for yourgateway.yourdomain.com: 10.0.2.1
        HP TCP/IP Services for OpenVMS Core Environment Configuration Menu
        Configuration options:
                 1  -  Domain
                 2  -  Interfaces
                 3  -  Routing
                 4  -  BIND Resolver
                 5  -  Time Zone
                 A  -  Configure options 1 - 5
                [E] -  Exit menu
Enter configuration option: 4
BIND RESOLVER Configuration
        A BIND resolver has not been configured.
        HP TCP/IP Services for OpenVMS supports the Berkeley Internet Name
        Domain (BIND) resolver.  BIND is a network service that enables
 clients
        to name resources or objects and share information with other
 objects
```

```
        on the network.
        Before configuring your system as a BIND resolver, you should
        first be sure that there is at least one system on the network
        configured as either a BIND primary or secondary server for
        this domain.
        You can specify a BIND server by its address or name;
        however, if specified by name, an entry for it must
        exist in the TCPIP$HOST database.
        You will be asked one question for each server.
        Press Return at the prompt to terminate the list.
Enter your BIND server name: yourserver
        yourserver is not in the local host database.
Enter Internet address for yourserver: 10.0.2.2
Enter next BIND server name: Return
        HP TCP/IP Services for OpenVMS Core Environment Configuration Menu
        Configuration options:
                 1  -  Domain
                 2  -  Interfaces
                 3  -  Routing
                 4  -  BIND Resolver
                 5  -  Time Zone
                 A  -  Configure options 1 - 5
                [E] -  Exit menu
       HP TCP/IP Services for OpenVMS Configuration Menu
        Configuration options:
                 1  -  Core environment
                 2  -  Client components
                 3  -  Server components
                 4  -  Optional components
                 5  -  Shutdown HP TCP/IP Services for OpenVMS
                 6  -  Startup HP TCP/IP Services for OpenVMS
                 7  -  Run tests
                 A  -  Configure options 1 - 4
                [E] -  Exit configuration procedure
Enter configuration option: 2

      HP TCP/IP Services for OpenVMS Client Components Configuration Menu
        Configuration options:
                 1  -  DHCP Client      Disabled Stopped
                 2  -  FTP Client       Disabled Stopped
                 3  -  NFS Client       Disabled Stopped
                 4  -  REXEC and RSH    Disabled Stopped
                 5  -  RLOGIN           Disabled Stopped
                 6  -  SMTP             Disabled Stopped
                 7  -  SSH Client       Disabled Stopped
                 8  -  TELNET           Disabled Stopped
                 9  -  TELNETSYM        Disabled Stopped
                 A  -  Configure options 1 - 9
                [E] -  Exit menu
Enter configuration option: 8
TELNET Configuration
Service is defined in the SYSUAF.
Service is defined in the TCPIP$SERVICE database.
Service is not enabled.
Service is stopped.
        TELNET configuration options:
                 1 - Enable service on this node
                 2 - Enable & Start service on this node
```

```
                [E] - Exit TELNET configuration
Enter configuration option: 2
%TCPIP-I-INFO, image SYS$SYSTEM:TCPIP$TELNET.EXE installed
%TCPIP-I-INFO, logical names created
%TCPIP-I-INFO, service enabled
%TCPIP-S-STARTDONE, TCPIP$TELNET startup completed
Press
<ENTER> key to continue ...
      HP TCP/IP Services for OpenVMS Client Components Configuration Menu
        Configuration options:
                 1  -  DHCP Client      Disabled Stopped
                 2  -  FTP Client       Disabled Stopped
                 3  -  NFS Client       Disabled Stopped
                 4  -  REXEC and RSH    Disabled Stopped
                 5  -  RLOGIN           Disabled Stopped
                 6  -  SMTP             Disabled Stopped
                 7  -  SSH Client       Disabled Stopped
                 8  -  TELNET           Enabled  Started
                 9  -  TELNETSYM        Disabled Stopped
                 A  -  Configure options 1 - 9
                [E] -  Exit menu

Enter configuration option: Return
        HP TCP/IP Services for OpenVMS Configuration Menu
        Configuration options:
                 1  -  Core environment
                 2  -  Client components
                 3  -  Server components
                 4  -  Optional components
                 5  -  Shutdown HP TCP/IP Services for OpenVMS
                 6  -  Startup HP TCP/IP Services for OpenVMS
                 7  -  Run tests
                 A  -  Configure options 1 - 4
                [E] -  Exit configuration procedure
Enter configuration option: 3
HP TCP/IP Services for OpenVMS Server Components Configuration Menu
  Configuration options:
    1 - BIND         Disabled Stopped      12 - NTP          Disabled
 Stopped
    2 - BOOTP        Disabled Stopped      13 - PC-NFS       Disabled
 Stopped
    3 - DHCP         Disabled Stopped      14 - POP          Disabled
 Stopped
    4 - FINGER       Disabled Stopped      15 - PORTMAPPER   Disabled
 Stopped
    5 - FTP          Disabled Stopped      16 - RLOGIN       Enabled
 Started
    6 - IMAP         Disabled Stopped      17 - RMT          Disabled
 Stopped
    7 - LBROKER      Disabled Stopped      18 - SNMP         Disabled
 Stopped
    8 - LPR/LPD      Disabled Stopped      19 - SSH          Disabled
 Stopped
    9 - METRIC       Disabled Stopped      20 - TELNET       Enabled
 Started
   10 - NFS          Disabled Stopped      21 - TFTP         Disabled
 Stopped
```

```
   11 - LOCKD/STATD  Disabled Stopped      22 - XDM          Disabled
 Stopped
    A  -  Configure options 1 - 22
   [E] -  Exit menu
Enter configuration option: 5
FTP Configuration
Service is defined in the SYSUAF.
Service is defined in the TCPIP$SERVICE database.
Service is not enabled.
Service is stopped.
        FTP configuration options:
                 1 - Enable service on this node
                 2 - Enable & Start service on this node
                [E] - Exit FTP configuration
Enter configuration option: 2
%TCPIP-I-INFO, image SYS$SYSTEM:TCPIP$FTP_CHILD.EXE installed
%TCPIP-I-INFO, image SYS$SYSTEM:TCPIP$FTP_SERVER.EXE installed
%TCPIP-I-INFO, logical names created
%TCPIP-I-INFO, service enabled
%TCPIP-S-STARTDONE, TCPIP$FTP startup completed
Press
<ENTER> key to continue ...
The FTP CLIENT is not enabled.
* Do you want to configure FTP CLIENT [NO]:
HP TCP/IP Services for OpenVMS Server Components Configuration Menu
  Configuration options:
    1 - BIND         Disabled Stopped      12 - NTP          Disabled
 Stopped
    2 - BOOTP        Disabled Stopped      13 - PC-NFS       Disabled
 Stopped
    3 - DHCP         Disabled Stopped      14 - POP          Disabled
 Stopped
    4 - FINGER       Disabled Stopped      15 - PORTMAPPER   Disabled
 Stopped
    5 - FTP          Enabled  Started      16 - RLOGIN       Enabled
 Started
    6 - IMAP         Disabled Stopped      17 - RMT          Disabled
 Stopped
    7 - LBROKER      Disabled Stopped      18 - SNMP         Disabled
 Stopped
    8 - LPR/LPD      Disabled Stopped      19 - SSH          Disabled
 Stopped
    9 - METRIC       Disabled Stopped      20 - TELNET       Enabled
 Started
   10 - NFS          Disabled Stopped      21 - TFTP         Disabled
 Stopped
   11 - LOCKD/STATD  Disabled Stopped      22 - XDM          Disabled
 Stopped
    A  -  Configure options 1 - 22
   [E] -  Exit menu

Enter configuration option: Return
        HP TCP/IP Services for OpenVMS Configuration Menu
        Configuration options:
                 1  -  Core environment
                 2  -  Client components
                 3  -  Server components
                 4  -  Optional components
```

```
                5  -  Shutdown HP TCP/IP Services for OpenVMS
                6  -  Startup HP TCP/IP Services for OpenVMS
                7  -  Run tests
                A  -  Configure options 1 - 4
               [E] -  Exit configuration procedure
Enter configuration option: 6
Begin Startup...
%TCPIP-I-INFO, TCP/IP Services startup beginning at 22-JUN-2006 09:18:20.58
%TCPIP-I-NORMAL, timezone information verified
%RUN-S-PROC_ID, identification of created process is 00000896
%TCPIP-I-SETLOCAL, setting domain and/or local host
%TCPIP-I-STARTCOMM, starting communication
%TCPIP-I-SETPROTP, setting protocol parameters
%TCPIP-I-DEFINTE, defining interfaces
%TCPIP-I-STARTNAME, starting name service
%TCPIP-S-STARTDONE, TCP/IP Kernel startup completed
%TCPIP-I-NOSERVICES, no services configured for startup
%TCPIP-I-PROXYLOADED, loaded 0 NFS proxy records
%TCPIP-I-LOADSERV, loading TCPIP server proxy information
%TCPIP-I-SERVLOADED, auxiliary server loaded with 0 proxy records
-TCPIP-I-SERVSKIP, skipped 0 communication proxy records
-TCPIP-I-SERVTOTAL, total of 0 proxy records read
%TCPIP-S-STARTDONE, TCPIP$PROXY startup completed
%TCPIP-S-STARTDONE, TCP/IP Services startup completed at 22-JUN-2006
 09:18:23.54
Startup request completed.
Press
<ENTER> key to continue ...Return
        HP TCP/IP Services for OpenVMS Configuration Menu
        Configuration options:
                1  -  Core environment
                2  -  Client components
                3  -  Server components
                4  -  Optional components
                5  -  Shutdown HP TCP/IP Services for OpenVMS
                6  -  Startup HP TCP/IP Services for OpenVMS
                7  -  Run tests
                A  -  Configure options 1 - 4
               [E] -  Exit configuration procedure
Enter configuration option: E
```