HP TCP/IP Services for OpenVMS

Release Notes

March 2010

This document describes the new features and changes introduced with Version 5.7 of the HP TCP/IP Services for OpenVMS software product.

Revision/Update Information:	This is an updated document.
Software Version:	HP TCP/IP Services for OpenVMS Version 5.7
Operating Systems:	OpenVMS Version 8.4 for Integrity servers OpenVMS Alpha Version 8.4

Hewlett-Packard Company
Palo Alto, California

The HP TCP/IP Services for OpenVMS documentation is available on CD-ROM.

This document was prepared using DECdocument, Version 3.3-1b.

Contents

3 Restrictions and Limitations

4 Corrections

5 Documentation Update

A LPD/LPR Configuration

Tables

Preface

The HP TCP/IP Services for OpenVMS product is the HP implementation of the TCP/IP protocol suite and Internet services for OpenVMS Alpha and OpenVMS Integrity server systems. This document describes the latest release of the HP TCP/IP Services for OpenVMS product.

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

For installation instructions, see the *HP TCP/IP Services for OpenVMS Installation and Configuration* manual.

The release notes provide version-specific information that supersedes the information in the documentation set. The features, restrictions, and corrections in this version of the software are described in the release notes. Always read the release notes before installing the software.

Intended Audience

These release notes are intended for experienced OpenVMS and UNIX® system managers and assume a working knowledge of OpenVMS system management, TCP/IP networking, TCP/IP terminology, and some familiarity with the TCP/IP Services product.

Document Structure

These release notes are organized into the following chapters:

- Chapter 1 describes new features and special changes to the software that enhances its observed behavior.
- Chapter 2 describes changes to the installation, configuration, and startup procedures, and includes other related information that is not included in the *HP TCP/IP Services for OpenVMS Installation and Configuration* manual.
- Chapter 3 describes information about problems and restrictions, and includes notes describing changes to particular commands or services.
- Chapter 4 describes problems identified in previous versions of TCP/IP Services that have been fixed.
- Chapter 5 describes updates to information in the TCP/IP Services product documentation.

Related Documents

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

Table 1 TCP/IP Services Documentation

Manual	Contents
HP 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 before configuring your system to use the TCP/IP Services software. This manual also describes the other manuals in the TCP/IP Services documentation set and provides a glossary of terms and acronyms for the TCP/IP Services software product.
HP TCP/IP Services for OpenVMS Release Notes	The release notes provide version-specific information that supersedes the information in the documentation set. The features, restrictions, and corrections in this version of the software are described in the release notes. Always read the release notes before installing the software.
HP TCP/IP Services for OpenVMS Installation and Configuration	This manual explains how to install and configure the TCP/IP Services product.
HP 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, e-mail, TELNET, TN3270, and network printing.
HP TCP/IP Services for OpenVMS Management	This manual describes how to configure and manage the TCP/IP Services product.
HP TCP/IP Services for OpenVMS Management Command Reference	This manual describes the TCP/IP Services management commands.
HP TCP/IP Services for OpenVMS Management Command Quick Reference Card	This reference card lists the TCP/IP management commands by component and describes the purpose of each command.
HP TCP/IP Services for OpenVMS UNIX Command Equivalents Reference Card	This reference card contains information about commonly performed network management tasks and their corresponding TCP/IP management and UNIX command formats.
HP 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 RPC). This manual also describes the RPC programming interface and how to use the RPCGEN protocol compiler to create applications.
HP TCP/IP Services for OpenVMS Guide to SSH	This manual describes how to configure, set up, use, and manage the SSH for OpenVMS software.
HP 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.
HP 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.

(continued on next page)

Table 1 (Cont.) TCP/IP Services Documentation

Manual	Contents
HP TCP/IP Services for OpenVMS Tuning and Troubleshooting	This manual provides information about how to isolate the causes of network problems and how to tune the TCP/IP Services software for the best performance. It also provides information about using UNIX network management utilities on OpenVMS.
HP 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.

For additional information about HP OpenVMS products and services, see:

`http://www.hp.com/go/openvms`

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

Reader's Comments

HP welcomes your comments on this manual. Please send comments to openvmsdoc@hp.com.

How to Order Additional Documentation

For information about how to order additional documentation, see:

`http://www.hp.com/go/openvms/doc/order`

Conventions

In the product documentation, the name TCP/IP Services means any of the following:

- HP TCP/IP Services for OpenVMS Alpha
- HP TCP/IP Services for OpenVMS Integrity servers

In addition, please note that all IP addresses are fictitious.

The following conventions are used in the documentation.

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.) In the HTML version of this document, this convention appears as brackets, rather than 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 choices in parentheses if you specify 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 optional; 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 type	Bold type represents the introduction of a new term. It also represents the name of an argument, an attribute, or a reason.
italic type	Italic type 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 TYPE	Uppercase type indicates a command, the name of a routine, the name of a file, or the abbreviation for a system privilege.
`Example`	This typeface indicates code examples, command examples, and interactive screen displays. In text, this type also identifies URLs, UNIX commands and pathnames, PC-based commands and folders, and certain elements of the C programming language.
-	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.

1
New Features and Behavioral Enhancements

This chapter describes the new features of TCP/IP Services Version 5.7 as well as behavioral enhancements.

Note

TCP/IP Services Version 5.7 is supported on OpenVMS Alpha and OpenVMS for Integrity servers systems only. On VAX systems, use TCP/IP Services Version 5.3.

To use TCP/IP Services Version 5.7, you must upgrade to OpenVMS Version 8.4 or higher.

For information about installing and configuring TCP/IP Services, see the *HP TCP/IP Services for OpenVMS Installation and Configuration* guide.

1.1 New features

Table 1–1 lists the new features of TCP/IP Services Version 5.7 and the sections that describe them.

Table 1–1 TCP/IP Services for OpenVMS, New Features

Feature	Section	Description
Packet Processing Engine	1.1.1	This release includes Packet Processing Engine, a CPU for processing TCP/IP that increases the performance efficiency.
FTP Anonymous Light	1.1.2	This release includes FTP Anonymous Light, used for restricting user access for a particular set of directories.

1.1.1 Packet Processing Engine

TCP/IP Packet Processing Engine (PPE) is modeled on the OpenVMS Dedicated Lock Manager. If you are familiar with Dedicated Lock Manager, you will only need to learn the different methods used to manage TCP/IP PPE.

TCP/IP runs on a single CPU, which is normally shared with other processes. However, some system loads result in near saturation of the TCP/IP CPU and causes TCP/IP to become a system-wide bottleneck. By dedicating a CPU for processing TCP/IP, a significant performance efficiency can be achieved, but, at the cost of dedicating a CPU for TCP/IP.

Note

Since TCP/IP PPE is recommended only in environments where the TCP/IP CPU is near saturation, dedicating a CPU to TCP/IP is a mere formality; except with significant payback.

Also, note that TCP/IP PPE can be dynamically enabled and disabled. System administrator can dynamically change the state of the TCP/IP PPE to suit the required load.

1.1.1.1 Configuring PPE

This section describes the hardware and software configuration required to configure PPE.

Hardware configuration

TCP/IP PPE will run only on systems with more than one active CPU. If TCP/IP PPE was running and the configuration changes such that there is only one active CPU remaining, the TCP/IP PPE becomes dormant.

Because, TCP/IP PPE dedicates an entire CPU for processing TCP/IP, it is recommended that TCP/IP must be enabled only on systems with a large number of CPUs, and only if the current TCP/IP CPU is nearing saturation.

Software configuration

For optimum performance, a CPU must be dedicated to PPE.

Normally, the TCP/IP BG0: driver shares the CPU with other fastpath drivers and processes. However, to achieve the best results with TCP/IP PPE, it is necessary to configure BG0: to be the only driver using the nominated CPU; all other fastpath drivers must be moved to other CPUs.

If TCP/IP PPE is running and other drivers are associated with the same CPU as BG0:, it results in suboptimal performance for both drivers.

Sample configuration

1. Configure the BG driver to be dedicated to CPU 3. For optimum results, ensure that no other fastpath devices share CPU 3.

   To examine the fastpath devices that are using CPU 3, execute the following:

   ```
   $ SHOW FASTPATH
   ```

2. If other fastpath drivers are assigned to that CPU, move them to a different CPU. For example, if the PEA0: device is assigned to CPU 3, move it to another CPU by executing the following:

   ```
   $ SET DEVICE PEA0 /PREF=5  ! move PEA0 to CPU 5.
   ```

3. Assign TCP/IP BG0: device to CPU 3 by executing the following:

```
$ SET DEVICE BG0/PREF=3
```

4. Verify that BG0: is the only fastpath driver assigned to CPU 3 by executing the following:

```
$ SHOW FASTPATH/CPU=3
```

1.1.1.2 Managing TCP/IP PPE

TCP/IP PPE is managed using the SYSCONFIG subsystem. To manage the TCP/IP PPE, complete the following steps:

Dynamically enable or disable PPE

1. To use sysconfig, at the DCL command line, execute the following:

```
$ @SYS$MANAGER:TCPIP$DEFINE_COMMANDS
```

2. To examine the current state of PPE, execute the following:

```
$ SYSCONFIG -q INET PPE_ENABLE
```

3. If the ppe_enable attribute is 0, TCP/IP PPE is disabled. To enable TCP/IP PPE, execute the following:

```
$ SYSCONFIG -r INET PPE_ENABLE=1
```

Note

Although, the "ppe_enable" attribute may indicate that TCP/IP PPE is enabled, you must also verify that PPE is running. As described in Section 1.1.1, PPE does not run if the number of active CPUs drops to 1. To verify that TCP/IP PPE is running, execute the following:

```
$ SHOW SYSTEM/PROC=TCPIP$INETPPE
```

An output similar to the following is displayed:

```
OpenVMS V8.4 on node GRYFFI  30-AUG-2009 13:32:03.22  Uptime  0 13:00:21

  Pid     Process Name   State  Pri   I/O       CPU         Page flts  Pages
22000438  TCPIP$INETPPE  CUR 3  63    10   0 12:49:32.25        91      108
```

The priority of this process is set to 63. This ensures that TCP/IP PPE is not rescheduled and no other process will use CPU 3.

You can also use the following command to verify that TCP/IP PPE is running:

```
$ MONITOR MODES/CPU=3 ! it will be 100% in Kernel Mode
```

To dynamically disable TCP/IP PPE, execute the following:

```
$ SYSCONFIG -r INET PPE_ENABLE=0
```

After a brief moment, the monitor display changes to show the CPU load distribution amongst the various modes.

Enabling TCP/IP PPE at system startup

To enable TCP/IP PPE after TCP/IP has started, use one of the following methods:

- Add the following to the TCPIP$ETC:SYSCONFIGTAB.DAT file:

```
inet:
        ppe_enable=1   # Enable TCP/IP PPE
```

  When TCP/IP is loaded, the ppe_enable flag will also be set.

  OR

- Add the SYSCONFIG command to the startup procedure. It is recommended that SYS$STARTUP:TCPIP$SYSTARTUP.COM must be modified with the following:

```
$ @SYS$MANAGER:TCPIP$DEFINE_COMMANDS
$ SYSCONFIG -r INET PPE_ENABLE=1  ! Enable TCP/IP PPE
```

1.1.1.3 Monitoring PPE

This section describes how to monitor PPE.

When PPE is disabled, the performance of the TCP/IP CPU can be monitored with following command:

```
$ MONITOR MODES/CPU=xx  ! where xx is the TCP/IP CPU Id
```

When PPE is enabled, the TCP/IP CPU runs 100% in the kernel mode, because the CPU is dedicated entirely to TCP/IP. Hence, the monitor command is not useful when PPE is running.

This section describes how to collect statistics when PPE is running. Also note that this method provides a much finer granularity and can also be used when PPE is disabled. This approach also helps you compare performance when PPE is enabled or disabled.

To gather statistics, enable profiling by executing the following:

```
$SYSCONFIG -r INET PROFILING=1
```

Note that with profiling enabled, there is a small processing overhead to collect the statistics. It is recommended to enable profiling only while gathering statistics. With profiling enabled, the statistics can be gathered using the TCPMON command as follows:

```
$ SET COMMAND TCPIP$EXAMPLES:TCPIP$TCP_MON
$ TCPMON/SHOW=INET
```

For more information on how to use the TCPMON command, see the help by executing the following:

```
$ HELP/LIBRARY=TCPIP$EXAMPLES:TCPIP$TCP_MON TCPMON
```

You can also use the Performance Data Collector (TDC) to monitor PPE. TDC can automatically gather the PPE statistics. For more information about TDC, visit the Web site at:

http://h71000.www7.hp.com/openvms/products/tdc/index.html

1.1.1.4 Comparison testing

With profiling enabled, you can compare performance data of when PPE is enabled and disabled. Assuming that you have a test that sufficiently saturates the TCP/IP CPU, complete the following steps to produce data sets that can be easily compared:

1. Enable profiling

   Profiling must be enabled while gathering statistics only. To enable profiling, execute the following:

   ```
   $ SYSCONFIG -r INET PROFILING=1
   ```

2. Ensure that PPE is disabled by executing the following:

   ```
   $ SYSCONFIG -r INET PPE_ENABLE=0
   ```

3. Run the stress test and monitor the performance as follows:

   - Using the MONITOR utility

     If the MONITOR utility shows that the TCP/IP CPU is not approaching saturation, enabling PPE will not yield any advantage.

     ```
     $ MONITOR MODES/CPU=xx ! xx = TCP/IP CPU
     ```

   - Using the TCPMON utility

     Capture the fine-granularity statistics and write them to a comma-separated value (CSV) file as well as display them on to the terminal. The CSV file can later be graphically analyzed using external programs, such as TLViz (from TDC) or a spreadsheet program.

     ```
     $ TCPMON /CSV=PPE_COMPARISON.CSV /DISPLAY [/SHOW=INET]
     ```

   - Run the Performance Data Collector (TDC)

     TDC provides the complete data set, which provides a whole-system view of performance.

     For more information about TDC, see the Web site at:

     `http://h71000.www7.hp.com/openvms/products/tdc/index.html`

4. Dynamically enabling PPE

   After collecting sufficient data with PPE disabled, dynamically enable PPE. There is no need to interrupt the data collection methods described in step 3.

   ```
   $ SYSCONFIG -r INET PPE_ENABLE=1
   ```

5. Comparing the data

   After gathering sufficient data with PPE disabled and enabled, compare the performance characteristics for the given test load. Stop the data collection and examine the data set.

6. Disable profiling

   There is a small overhead associated with profiling. So, it is recommended to disable profiling when statistics is not gathered.

   ```
   $ SYSCONFIG -r INET PROFILING=0
   ```

1.1.2 FTP Anonymous Light

FTP Anonymous Light can be used for restricting user access to a particular set of directories. A system administrator who wants to restrict an OpenVMS user's FTP access to a particular set of directories must set the TCPIP$FTP_ANONYMOUS_LIGHT parameter for that user.

Setting this parameter restricts the FTP operations for the user to a set of directories indicted by TCPIP$FTP_ANONYMOUS_DIRECTORIES. The TCPIP$FTP_ANONYMOUS_LIGHT can be defined in LOGIN.COM.

To restrict the FTP access for all users, the parameter must be defined using a system-wide logical. FTP Anonymous Light users must specify the correct password to log in. By default, when an anonymous user is prompted for the identity, any password is accepted. Optionally, the system administrator can also set TCPIP$FTP_ANONYMOUS_WELCOME to display a message upon successful login.

The following example illustrates how FTP Anonymous Light works:

```
"TCPIP$FTP_ANONYMOUS_DIRECTORY" = "TCPIP$ENETINFO1:[UCX]"
= "TCPIP$ENETINFO1:[UCX_AXP]"
= "TCPIP$ECO:"
= "TCPIP$PATCH:"
= "COMMON_SYSDISK:[FAL$SERVER]"
= "TCPIP$INTERNAL:"
"TCPIP$FTP_ANONYMOUS_LIGHT" = "1"
"TCPIP$FTP_ANONYMOUS_LOG" = "SYS$LOGIN:TCPIP$FTP_ANONYMOUS.LOG"
"TCPIP$FTP_ANONYMOUS_WELCOME" = "FTP Anonymous Light demo"

ftp plane.tcpip.zko.hp.com
220 plane.tcpip.zko.hp.com FTP Server (Version 5.6) Ready.
Connected to plane.zko.hp.com.
Name (plane.zko.hp.com:test):
331 Username test requires a Password
Password:
230-FTP Anonymous Light demo
230 Guest login OK, access restrictions apply.
FTP> cd sys$system
550 insufficient privilege or file protection violation  ❶

FTP> cd tcpip$eco
250-CWD command successful.
250 New default directory is TCPIP$ENETINFO1:[TCPIP$ENGINEERING_CHANGE_ORDERS]❷

FTP> cd sys$login
250-CWD command successful.
250 New default directory is WORK4$:[TEST]
FTP> bye
221 Goodbye.
```

Field	Description
❶	This directory is not included in TCPIP$FTP_ANONYMOUS_DIRECTORY, so access is restricted
❷	This directory is included in TCPIP$FTP_ANONYMOUS_DIRECTORY, so access is allowed

An output similar to the following is saved in the log file:

```
20-JUN-2008 05:21:45.64 Anonymous Light User:test from Host:16.116.92.100
20-JUN-2008 05:22:39.61 Anonymous Light User:test status:00010001
                        CWD dir:TCPIP$ENETINFO1:[TCPIP$ENGINEERING_CHANGE_ORDERS]
20-JUN-2008 05:23:13.49 Anonymous Light User:test status:00010001
                        CWD dir:WORK4$:[TEST]
20-JUN-2008 05:23:19.15 Anonymous Light User:test status:00000000
                        RETR file:WORK4$:[TEST]A.TXT;30
20-JUN-2008 05:23:26.07 Anonymous Light User:test logged out
```

Although the system administrator does not specify the directory, SYS$LOGIN is always added to TCPIP$FTP_ANONYMOUS_DIRECTORY. As a result, the Anonymous Light users will always have access to their SYS$LOGIN.

At some instances, the system administrator may not want the user to access their SYS$LOGIN. To prevent the user from accessing the SYS$LOGIN, the system administrator must define TCPIP$FTP_ANONYMOUS_NOSYSLOGIN for that particular user. This parameter is useful when a user has changed the directory in LOGIN.COM and when the system administrator does not want to grant access to SYS$LOGIN.

1.1.2.1 Access restrictions for FTP operations

The FTP Anonymous Light feature restricts user access to a particular set of directories. To increase the system administrator's flexibility, a new set of parameters can be defined to restrict user operations.

The FTP server checks for the existence of the following four parameters:

- TCPIP$FTPD_NOLIST - LIST and NLST commands
- TCPIP$FTPD_NOREAD - RETR commands
- TCPIP$FTPD_NOWRITE - STOR, STOU, APPE, RNFR, RNTO, DELE, MKD, and RMD commands
- TCPIP$FTPD_NODELETE - DELE and RMD commands

If the parameter is defined, the FTP server will reject all.

These new access restrictions are applicable in addition to any restrictions implied by the protections of the underlying files, directories, volumes, and devices.

If TCPIP$FTPD_NOLIST is defined, the usage of wildcards is not allowed in FTP operations. This is necessary to prevent FTP users from obtaining a list of the files in the directory by attempting to retrieve or delete all the files. Table 1–2 lists the FTP restriction logicals that are used to control their operation:

Table 1–2 FTP restriction logicals

Client command	FTP Logical
Directory	TCPIP$FTPD_NOLIST
View	TCPIP$FTPD_NOREAD
Put	TCPIP$FTPD_NOWRITE
Get	TCPIP$FTPD_NOREAD
Append	TCPIP$FTPD_NOWRITE
Rename	TCPIP$FTPD_NOWRITE

(continued on next page)

Table 1–2 (Cont.) FTP restriction logicals

Client command	FTP Logical
Create	TCPIP$FTPD_NOWRITE
Delete	TCPIP$FTPD_NOWRITE

For example, if the System Administrator does not want a user to delete files through FTP, set TCPIP$FTPD_NODELETE for that user.

The following example illustrates how to set the TCPIP$FTPD_NODELETE and TCPIP$FTPD_NOLIST:

```
"TCPIP$FTPD_NODELETE" = "1"
"TCPIP$FTPD_NOLIST" = "1"

$ ftp plane.tcpip.zko.hp.com
220 plane.tcpip.zko.hp.com FTP Server (Version 5.6) Ready.
Connected to plane.zko.hp.com.
Name (plane.zko.hp.com:test): test
331 Username test requires a Password
Password:
230-FTP Anonymous Light demo
230 Guest login OK, access restrictions apply.
FTP> directory *
200 PORT command successful.
550 Cannot execute LIST command, Access denied. ❶

%TCPIP-E-FTP_NOSUCHFILE, no such file *
FTP> delete a.txt
550 Cannot execute DEL command, Access denied.❷

FTP> bye
221 Goodbye.
```

Field	Description
❶	The DIRECTORY command is not allowed because a wildcard present in the command and TCPIP$FTPD_NOLIST is defined.
❷	The DELETE command is not allowed because the TCPIP$FTPD_NODELETE logical is set.

FTP restriction logicals can be used in conjunction with FTP Anonymous Light to restrict user access through FTP, helping to mitigate a risk to the system that has been problematic for system administrators.

1.2 Enhancements

Table 1–3 lists the enhancements of TCP/IP Services Version 5.7 and the sections that describe them.

Table 1–3 TCP/IP Services for OpenVMS, Enhancements

Enhancement	Section	Description
TCPIP$CONFIG	1.2.1	Interface Configuration Menu is enhanced.
LPD configurable port	1.2.2	LPR/LPD port can be configured.
FTP over SSL	1.2.3	FTP software is enhanced to use the security features provided by SSL.
SMTP cluster ability	1.2.4	SMTP is made cluster aware.
SMTP ASCII file configuration	1.2.5	Supports the SMTP configurable fields.
SMTP Persistent receiver	1.2.6	The SMTP receiver process is made persistent.
POP ASCII file configuration	1.2.7	Supports the POP configurable fields.
POP server support for external authentication	1.2.8	Supports the POP server for external authentication.

1.2.1 TCPIP$CONFIG

With support for IP as the cluster interconnect (IPCI), Interface Configuration Menu now supports the following:

- Management of interfaces and addresses on another cluster member that shares the same TCPIP$CONFIGURATION database.
- Addresses that can be configured for use with IPCI.

1.2.1.1 Configuring interfaces and addresses on a remote cluster member

Assuming that the cluster members share the same TCPIP$CONFIGURATION database, each cluster member can be configured from the same console. This only affects the TCPIP$CONFIGURATON database; it is not possible to manage the active addresses on a remote cluster member.

An output similar to the following is displayed for the TCPIP$CONFIG Interface * Address Configuration menu from one of the node in a cluster:

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

Hostname Details: Configured=kirra-g0, Active=kirra-g0

Configuration options:

  0  -  Set The Target Node (Current Node: KIRRA)
  1  -  IE0 Menu (EIA0: TwistedPair 1000mbps)
  2  -  19.176.56.100/23    kirra-g0             Configured,Active
  3  -  19.176.56.101/23    kirra-g1             Configured,Active-Standby
  4  -  19.176.57.100/23    hogwarts-nfs         Configured,Active-Standby
  5  -  19.176.56.25/23     ns1                  Configured,Active-Standby
  6  -  IE1 Menu (EIB0: TwistedPair 1000mbps)
  7  -  19.176.56.101/23    kirra-g1             Configured,Active
  8  -  19.176.56.100/23    kirra-g0             Configured,Active-Standby
  9  -  19.176.57.100/23    hogwarts-nfs         Configured,Active-Standby
 10  -  19.176.56.25/23     ns1                  Configured,Active-Standby
  I  -  Information about your configuration
[E] -  Exit menu
```

```
Enter configuration option: 0 ❶
Enter name of node to manage [KIRRA]: GRYFFI ❷
Enter system device for GRYFFI [$1$DGA62:]: ❸
Enter system root for GRYFFI [SYS0]: ❹

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

 Hostname Details: Configured=gryffindor-e0

 Configuration options:

   0  -  Set The Target Node (Current Node: GRYFFI - $1$DGA62:[SYS0.])
   1  -  IE0 Menu (EIA0: TwistedPair 100mbps)
   2  -  19.176.56.65/23     gryffindor-e0         Configured
   3  -  19.176.56.81/23     gryffindor-e1         Configured
   4  -  19.176.57.100/23    hogwarts-nfs          Configured
   5  -  19.176.56.25/23     ns1                   Configured
   6  -  IE1 Menu (EIB0: TwistedPair 100mbps)
   7  -  19.176.56.81/23     gryffindor-e1         Configured
   8  -  19.176.56.65/23     gryffindor-e0         Configured
   9  -  19.176.57.100/23    hogwarts-nfs          Configured
  10  -  19.176.56.25/23     ns1                   Configured
   I  -  Information about your configuration
  [E] -  Exit menu

Enter configuration option:
```

Field	Description
❶	If node GRYFFI is another cluster member that shares the same TCPIP$CONFIGURATION database, to manage the interfaces and addresses on node GRYFFI, select option "0".
❷	Enter the SCSNODE name of the other node in the cluster to manage. In this case, it is GRYFFI.
❸	To support the management of IPCI, it is necessary to confirm the system root on the remote node. The remote cluster member's system device is determined using SYSMAN.
❹	The remote clusters member's system root is determined using SYSMAN. The new TCPIP$CONFIG window now displays the configuration on node GRYFFI. Changes to this screen will affect node GRYFFI's permanent TCP/IP configuration only.

1.2.2 LPD configurable port

LPR/LPD provided by TCP/IP services for OpenVMS 5.6 and prior versions connects directly to port 515 on a remote server and sends the data as specified in the RFC 1179. With TCP/IP services for OpenVMS 5.7, this remote port is made configurable. A system manager can choose any ephemeral port.

1.2.2.1 Configuring the remote port

In the printcap file, TCPIP$PRINTCAP.DAT, for each printer entry, a new field, `rt` is added, which can be used to configure remote port.

For example:

```
LOOP_BOGUS_P_1|loop_bogus_p_1:\
                      :lf=/TCPIP$LPD_ROOT/000000/LOOP_BOGUS_P_1.LOG:\
 :lp=LOOP_BOGUS_P_1:\
                :rm=qtvtcp.digitalindiasw.net:\
                :rp=bogus_p_1:\
                :rt#2333:\
               :sd=/TCPIP$LPD_ROOT/LOOP_BOGUS_P_1:
```

1.2.2.2 Using the LPD configurable port for secure printing

Using the `rt` field in the printer entry in TCPIP$PRINTCAP.DAT, the LPD jobs is sent over an SSH encrypted tunnel. You can configure SSH port forwarding to establish a tunnel from port (rt) on a system to an LPD receiver port (default is 515 or any other port on which LPD service is configured manually) on another system where the LPD receiver is listening. For sample LPD/LPR configurations, see Appendix A.

1.2.3 FTP over SSL

The Transport Layer Security/Secure Socket Layer (TLS/SSL) feature enables the FTP software to use the security features provided by SSL. When this feature is enabled, FTP provides a secured FTP session and a secure file transfer. FTP over SSL is compliant with RFC 4217 and RFC 2228.

1.2.3.1 Configuring an FTP server for SSL

To configure an FTP server and to allow the FTP server to handle incoming client connections which are over SSL, the certificates and keys must be copied at the following location:

```
Certificate file : SSL$CERTS:SERVER.CRT
Key file: SSL$KEYS:SERVER.KEY
```

The key and certificate file of the server must be placed in this directory and must be named as SERVER.CRT and SERVER.KEY. During the FTP server startup, if it does not find either the key or the certificate file in the required location, the FTP server will not support SSL.

1.2.3.2 Using FTP client in an SSL environment

You can use FTP over SSL to connect to the server by invoking the client using the following commands:

```
$FTP /SSL <server>
```

Or

```
$FTP
FTP> CONNECT /SSL <server>
```

If you connect to the server using the `/SSL` qualifier, both the control and data connection use SSL by default. By default, the `PROT P` command is sent by the client to the server indicating that the data connection will use SSL.

If you want the data connection communication to happen in clear text, you can issue the `PROT C` command on the FTP client CLI.

```
ftp> PROT C
```

The OpenVMS FTP client and server also supports the Clear Command Channel (CCC) mode of operation. The CCC mode can be used in NAT environments that need a clear command channel to setup NAT for FTP/SSL. An FTP Client issues the `CCC` command to indicate to the server that the command channel must not be encrypted. Note that the data channel will remain encrypted. As a result, the file transfer will continue to be secured by SSL.

For example, if you want the control connection to not be encrypted, execute the `CCC` command at the FTP client CLI:

```
ftp> CCC
```

Note

The CCC command can be issued only after logging into the FTP server with a valid username and password.

If you want to use the copy operation in FTP, COPY/FTP, the syntax is as follows:

```
copy /ftp/ssl=(data,ccc) <src system>   <dst system>
```

If you do not want the data connection to be encrypted, specify NODATA in the preceding command instead of DATA.

If you want CCC (by default), specify CCC, else specify NOCCC.

1.2.3.3 Considerations during configuration

- If the server does not find the SEREVER.CRT and SERVER.KEY, the server will not accept the AUTH TLS command. However, the server will continue to accept regular FTP connections.

  An SSL enabled client will still be able to connect to non-SSL enabled server and displays the following message:

  ```
  AUTH command will fail, session will continue in plain text.
  ```

- A non-SSL enabled client will be able to login to SSL enabled server.

1.2.4 SMTP cluster ability

SMTP provided by TCP/IP Services for OpenVMS is cluster aware. It exploits the high availability and load balancing features of a cluster. The name of the generic queue is now TCPIP$SMTP, without the node name as the suffix. This is a common SMTP generic queue for all nodes in the cluster.

1.2.4.1 Configuration

The following configurable parameters can be found in the TCPIP$SMTP.CONF file:

- Number-Of-Queues-Per-Node: Specifies the number of execution SMTP queues created on each node of a cluster. The default value is 1. The execution queue will have the name format as follows:

  ```
  TCPIP$SMTP_<emphasis>(<nodename>_<n>)
  ```

- Queue-name: Specifies the name of generic SMTP queue. The default is TCPIP$SMTP.

Note

The SMTP configuration files, the SMTP home directory and the MAIL box must be placed in a disk that is visible to all nodes in the cluster.

1.2.5 SMTP ASCII file configuration

TCPIP$SMTP.CONF can also be used to configure the trace and debug parameters, but the precedence will be changed.

The existing configuration based on logical names and `TCPIP> SET CONFIGURATION SMTP` is obsolete. The SMTP rollover tool, TCPIP$SMTP_V57_ROLLOVER.EXE, can be used to upgrade the TCP/IP software to Version 5.7. Up on upgrade, the SMTP startup procedure will automatically change over to new ASCII file based configuration method. It creates the TCPIP$SMTP.CONF file in the TCPIP$SMTP_COMMON directory. Up on successful rollover, SYS$MANAGER:TCPIP$SMTP_V57_ROLLOVER.FLG is created.

Include the appropriate SMTP parameters in this file. The configuration template file, TCPIP$SMTP.CONF_TEMPLATE, contains the description of all SMTP configurable parameters and its usage.

Note

Only the debug and tracing logicals will take higher precedence, and the other logical will be ignored.

1.2.6 SMTP Persistent receiver

The SMTP receiver process is made persistent so that it does not die after receiving each mail. Prior to Version 5.7, for each new mail, a new SMTP receiver process was created and it died after receiving the mail. Starting with Version 5.7, each receiver process services multiple incoming mails as configured.

1.2.6.1 Configurable parameters

Following are the configurable parameters used in SMTP persistent receiver:

- Persistent-Server: Enables the persistence of the SMTP receiver if set to ON. The default value is OFF.
- Loop-max: Specifies the maximum number of times the SMTP receiver must retry a connection. The default is no maximum (the same as setting this option to 0). This behavior requires the Persistent-Server option to be specified.
- Idle-Timeout: Specifies the time that the SMTP receiver waits for an incoming SMTP connection, in OpenVMS delta time format. The default is 5 minutes. This behavior requires the Persistent-Server option be specified.

1.2.7 POP ASCII file configuration

HP TCP/IP Services for OpenVMS, Version 5.7 supports all the POP configurable fields through the TCPIP$POP.CONF file, except the POP tracing logical names.

The existing configuration based on logical names is obsolete. The POP rollover tool, TCPIP$POP_V57_ROLLOVER.EXE, can be used to upgrade the TCP/IP software to Version 5.7. Up on upgrade, the POP startup procedure will automatically change over to new ASCII file-based configuration method. It will create TCPIP$POP.CONF file in SYS$SYSDEVICE:[TCPIP$POP] directory. Up on successful rollover, SYS$MANAGER:TCPIP$POP_V57_ROLLOVER.FLG will be created.

Include the appropriate POP configuration parameters in this file. The configuration template file, TCPIP$POP.CONF_TEMPLATE, contains the description of all the POP configurable parameters and its usage.

1.2.8 POP server support for external authentication

POP Server support for external authentication adds the capability to POP clients to authenticate an user on an OpenVMS system. The POP server uses the SYS$ACM system service that provides this capability.

OpenVMS Authentication and Credentials Management Extensions (ACME) subsystem provides the authentication services.

The new configuration parameter, No-SYSACM-User-Pass, is added to support the Username and Password authentication on the ACME agents. The ACME agents can be VMS native authentication extensions or any other Agents such as LDAP, which can authenticate the VMS user externally. When you configure the POP to make use of POP external authentication, you must ensure that the ACME agents are up and running.

No-SYSACM-User-Pass can be assigned with 0 or 1 as follows:

No-SYSACM-User-Pass: <Boolean Value>

Where: <Boolean Value> is either:

- 0 / FALSE: POP Server uses SYS$ACM system service for username and password authentication.

  OR

- 1 / TRUE : POP Server does not use SYS$ACM system service for username and password authentication.

By default, the No-SYSACM-User-Pass is set to TRUE, that is, the POP server is configured to use the native VMS authentication using SYS$GETUAI.

Note

The external authentication using $ACM support for APOP shared secret string authentication is not provided.

2

Installation, Configuration, Startup, and Shutdown

This chapter includes notes and changes made to the installation and configuration of TCP/IP Services, as well as startup and shutdown procedures. Use this chapter in conjunction with the *HP TCP/IP Services for OpenVMS Installation and Configuration* manual.

2.1 Installing Over V5.3 Early Adopter's Kits (EAKs)

If you have installed one or more of the following V5.3 EAKs, you must use the PCSI REMOVE command to remove the EAKs before you install TCP/IP Services V5.7:

- SSH for OpenVMS EAK
- failSAFE IP EAK

Note

If you install the current TCP/IP Services version after removing the failSAFE IP EAK, you must run TCPIP$CONFIG.COM to reestablish your target and home interfaces.

2.2 Upgrading from TCP/IP Services Version 4.*x*

Upgrading from versions prior to V5.0 has not been qualified for this release.

2.3 Adding a system to an OpenVMS Cluster

The TCPIP$CONFIG.COM configuration procedure for TCP/IP Services Version 5.6 creates 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, HP recommends adding the system to the cluster before you configure TCP/IP Services. The guidelines in Section 2.3.1 assume you have followed this recommendation.

If you configure TCP/IP Services before you add the system to a cluster, see Section 2.3.2.

2.3.1 Running a newly configured host on 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 the cluster and you encounter problems running a TCP/IP component on the system, modify the cluster System Authorization File (SYSUAF) to raise the parameter values for the account used by the affected component. The minimum recommended values are listed in Table 2–1.

Table 2–1 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, see *HP OpenVMS System Management Utilities Reference Manual: A-L*.

2.3.2 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.

2.3.3 Disabling or enabling SSH server

When you use the TCPIP$CONFIG.COM configuration procedure to disable or enable the SSH server, the following prompt is displayed:

```
* Create a new default Server host key? [YES]:
```

Unless you have a specific reason for creating a new default server host key, you should enter "N" at this prompt. If you accept the default, clients with the old key will need to obtain the new key. For more information, see Section 3.15.6.

2.4 SSH configuration files must be updated

Note that this section refers to upgrades from a version prior to V5.4 ECO.

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. The client will display the following warning message, and the server will write the following warning message to the SSH_RUN.LOG file:

```
You may have an old style configuration file. Please follow the
instructions in the release notes to use the new configuration
files.
```

If the SSH client detects a user-specific configuration file from an older version of SSH, the SSH client will display the warning and will allow the user to proceed.

To preserve the modifications made to the SSH server configuration file and the SSH client configuration file, you must edit the templates provided with the new version of SSH, as follows:

1. Extract the template files using the following commands:

   ```
   $ LIBRARY/EXTRACT=SSH2_CONFIG SYS$LIBRARY:TCPIP$TEMPLATES.TLB -
   _$ /OUT=TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]SSH2_CONFIG.
   ```

   ```
   $ LIBRARY/EXTRACT=SSHD2_CONFIG SYS$LIBRARY:TCPIP$TEMPLATES.TLB -
   _$ /OUT=TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]SSHD2_CONFIG.
   ```

   These commands copy the new template files into the SSH2 configuration directory with a new version number.

2. Copy the modifications made in the old versions of the configuration files to the new versions.

3. Start SSH using the following command:

   ```
   $ @SYS$STARTUP:SSH_STARTUP.COM
   $ @SYS$STARTUP:SSH_CLIENT_STARTUP.COM
   ```

2.5 Troubleshooting SMTP and LPD shutdown problems

If SMTP or LPD shutdown generates errors indicating that the queue manager is not running, check your site-specific shutdown command procedure (VMS_SYSHUTDOWN.COM). If this procedure contains the command to stop the queue manager (STOP/QUEUE/MANAGER), make sure this command is after the command that runs the TCPIP$SHUTDOWN.COM command procedure.

Note

You do not have to stop the queue manager explicitly. The queue manager is automatically stopped and started when you restart the system.

3
Restrictions and Limitations

This chapter provides information about problems and restrictions in the current version of TCP/IP Services, and also includes other information specific to a particular command or service, such as changes in command syntax or messages.

3.1 IP Security

The IP Security (IPSec) feature that is included with this kit is not currently supported. HP recommends that you must not use IPSec in a production environment.

3.2 Dnssec_signzone utility may hang

The `dnssec_signzone` utility may hang when invoked from a foreign symbol. The utility will neither exhibit this behavior when it is executed from the command line using a foreign symbol or MCR, nor when the `-r` option is used to specify a source of entropy.

3.3 COPY /FTP restriction

COPY /FTP does not properly support ODS-5 filesystem files.

3.4 OpenVMS Mails

OpenVMS mails sent to a distribution list, to an invalid remote addresses does not get bounced. However, the mail to an invalid local address gets bounced.

3.5 Netstat utility

An IP address added to a tunnel interface cannot be seen with ifconfig. The new address cannot be seen unless you execute `netstat -rn`.

3.6 SMTP configured for cluster awareness

If SMTP is configured for cluster awareness, the disk on which the SMTP configuration files are saved must be mounted before the TCP/IP software is started. The system will hang up on TCP/IP startup, if the disk is not mounted.

3.7 Manually configuring an interface as DHCP leads to startup problems

Manually configuring an interface to be managed via DHCP may lead to an error, TCPIP-E-DEFINTE, when starting TCP/IP. This causes TCP/IP to not start properly. To work around this problem, shutdown TCP/IP, then on the interface that was manually configured as DHCP, issue the following command: `$ tcpip set config inter` *ifname*`/PRIMARY` Now restart TCP/IP.

3.8 SLIP restrictions

The serial line IP protocol (SLIP) is not supported in this release.

3.9 Advanced Programming Environment restrictions and guidelines

The header files provided in TCPIP$EXAMPLES are provided as part of the advanced TCP/IP programming environment. The following list describes restrictions and guidelines for using them:

- Use of the functions and data structures described in TCPIP$EXAMPLES:RESOLV.H is limited to 32-bit pointers. The underlying implementation will only handle 32-bit pointers. Previously, 64-bit pointers were wrongly accepted, resulting in undefined behavior for the underlying implementation.
- The IP.H and IP6.H header files are incomplete in the OpenVMS environment. They contain `include` directives for header files that are not provided in this version of TCP/IP Services. Refer to the *HP TCP/IP Services for OpenVMS Sockets API and System Services Programming* for more information.

3.10 BIND/DNS restrictions

BIND Version 9 has the following restrictions:

- Certain DNS server implementations do not support AAAA (IPv6 address) records. When queried for an AAAA (IPv6) record type by the BIND resolver, these name servers will return an NXDOMAIN status, even if an A (IPv4) record exists for the same domain name. These name servers should be returning NOERROR as the status for such a query. This problem can result in delays during host name resolution.

  BIND Version 9.3.1, which is supported with this release of TCP/IP Services, and prior versions of BIND do not exhibit this problem.

- Serving secure zones

  When acting as an authoritative name server, BIND Version 9 includes KEY, SIG, and NXT records in responses as specified in RFC 2535 when the request has the DO flag set in the query.

- Secure resolution

  Basic support for validation of DNSSEC signatures in responses has been implemented but should be considered experimental.

  When acting as a caching name server, BIND Version 9 is capable of performing basic DNSSEC validation of positive as well as nonexistence responses. You can enable this functionality by including a `trusted-keys` clause containing the top-level zone key of the DNSSEC tree in the configuration file.

  Validation of wildcard responses is not currently supported. In particular, a `"name does not exist"` response will validate successfully even if the server does not contain the NXT records to prove the nonexistence of a matching wildcard.

Proof of insecure status for insecure zones delegated from secure zones works when the zones are completely insecure. Privately secured zones delegated from secure zones will not work in all cases, such as when the privately secured zone is served by the same server as an ancestor (but not parent) zone.

Handling of the CD bit in queries is now fully implemented. Validation is not attempted for recursive queries if CD is set.

- Secure dynamic update

  Dynamic updating of secure zones has been partially implemented. Affected NXT and SIG records are updated by the server when an update occurs. Use the `update-policy` statement in the zone definition for advanced access control.

- Secure zone transfers

  BIND Version 9 does not implement the zone transfer security mechanisms of RFC 2535 because they are considered inferior to the use of TSIG or SIG(0) to ensure the integrity of zone transfers.

- SSL$LIBCRYPTO_SHR32.EXE requirement

  In this version of TCP/IP Services, the BIND Server and related utilities have been updated to use the OpenSSL shareable image SSL$LIBCRYPTO_SHR32.EXE. There is now a requirement that this shareable image from OpenSSL V1.2 or higher be installed on the system before starting the BIND Server. It must also be installed before using the following BIND utilities:

  ```
  BIND_CHECKCONF
  BIND_CHECKZONE
  DIG
  DNSSEC_KEYGEN
  DNSSEC_SIGNZONE
  HOST
  NSUPDATE
  RNDC_CONFGEN
  ```

3.11 IPv6 restrictions

The following sections describe restrictions in the use of IPv6.

3.11.1 Mobile IPv6 restrictions

Mobile IPv6 is not supported in this release.

3.11.2 IPv6 requires the BIND Resolver

If you are using IPv6, you must enable the BIND resolver. To enable the BIND resolver, use the TCPIP$CONFIG.COM command procedure. From the `Core environment` menu, select BIND Resolver.

You must specify the BIND server to enable the BIND resolver. If you do not have access to a BIND server, specify the node address 127.0.0.1 as your BIND server.

3.12 NFS restrictions

The following sections describe problems and restrictions with NFS.

3.12.1 NFS Server problems and restrictions

The following restrictions apply to the NFS server:

- When performing a mount operation or starting the NFS server with OPCOM enabled, the TCP/IP Services MOUNT server can erroneously display the following message:

  ```
  %TCPIP-E-NFS_BFSCAL, operation MOUNT_POINT failed on file /dev/dir
  ```

  This message appears even when the MOUNT or NFS startup has successfully completed. In the case of a mount operation, if it has actually succeeded, the following message will also be displayed:

  ```
  %TCPIP-S-NFS_MNTSUC, mounted file system /dev/dir
  ```

- If the NFS server and the NFS client are in different domains and unqualified host names are used in requests, the lock server (LOCKD) fails to honor the request and leaves the file unlocked.

  When the server attempts to look up a host using its unqualified host name (for example, `johnws`) instead of the fully qualified host name (for example, `johnws.abc com`), and the host is not in the same domain as the server, the request fails.

  To solve this type of problem, you can do one of the following:

  – When you configure the NFS client, specify the fully qualified host name, including the domain name. This ensures that translation will succeed.

  – Add an entry to the NFS server's hosts database for the client's unqualified host name. Only that NFS server will be able to translate this host name. This solution will not work if the client obtains its address dynamically from DHCP.

3.12.2 NFS Client problems and restrictions

- If the OpenVMS NFS client is executing the MOUNT commands from the script in a non-sequential manner, a wrong unit number is returned causing the NFS exported directory to mount on a wrong device number because of the timing issue.

  For example, the following mount command makes NFS to be mounted on DNFS8 instead of the requested device DNFS4.

  ```
  $ TCPIP MOUNT DNFS4:[<directory>]/HOST=<host-name>
    /PATH=<path-name>/SUPER/PROCESSOR=UNIQUE
  ```

  Workaround

  Execute the mount commands such that the device numbers are sequential.

  For example, instead of the following set of commands:

  ```
  $ TCPIP MOUNT DNFS3:[<directory>]/HOST=<host-name>
    /PATH=<path-name>/SUPER/PROCESSOR=UNIQUE
  $ TCPIP MOUNT DNFS2:[<directory>]/HOST=<host-name>
    /PATH=<path-name>/SUPER/PROCESSOR=UNIQUE
  $ TCPIP MOUNT DNFS1:[<directory>]/HOST=<host-name>
    /PATH=<path-name>/SUPER/PROCESSOR=UNIQUE
  ```

Change the sequence as follows:

```
$ TCPIP MOUNT DNFS1:[<directory>]/HOST=<host-name>
  /PATH=<path-name>/SUPER/PROCESSOR=UNIQUE
$ TCPIP MOUNT DNFS2:[<directory>]/HOST=<host-name>
  /PATH=<path-name>/SUPER/PROCESSOR=UNIQUE
$ TCPIP MOUNT DNFS3:[<directory>]/HOST=<host-name>
  /PATH=<path-name>/SUPER/PROCESSOR=UNIQUE
```

- SYMLINKs fail to work for NFS client disks.
- To get proper timestamps, when the system time is changed for daylight savings time (DST), dismount all DNFS devices. (The TCP/IP management command SHOW MOUNT should show zero mounted devices.) Then remount the devices.
- The NFS client does not properly handle file names with the semicolon character on ODS-5 disk volumes. (For example, `a^;b.dat;5` is a valid file name.) Such file names are truncated at the semicolon.
- The NFS client included with TCP/IP Services uses the NFS Version 2 protocol only.
- With the NFS Version 2 protocol, the value of the file size is limited to 32 bits.
- The ISO Latin-1 character set is supported. The UCS-2 characters are not supported.
- File names, including file extensions, can be no more than 236 characters long.
- Files containing characters not accepted by ODS-5 on the active OpenVMS version or whose name and extension exceeds 236 characters are truncated to zero length. This makes them invisible to OpenVMS and is consistent with prior OpenVMS NFS client behavior.

3.13 NTP problems and restrictions

The NTP server has a stratum limit of 15. The server does not synchronize to any time server that reports a stratum of 15 or greater. This may cause problems if you try to synchronize to a server running the UCX NTP server, if that server has been designated as "free running" (with the `local-master` command). For proper operation, the `local-master` designation must be specified with a stratum no greater than 14.

3.14 SNMP problems and restrictions

This section describes restrictions to the SNMP component for this release. For more information about using SNMP, refer to the *HP TCP/IP Services for OpenVMS SNMP Programming and Reference* manual.

3.14.1 Incomplete restart

When the SNMP master agent and subagents fail or are stopped, TCP/IP Services is often able to restart all processes automatically. However, under certain conditions, subagent processes may not restart. When this happens, the display from the DCL command SHOW SYSTEM does not include TCPIP$OS_MIBS and TCPIP$HR_MIB. If this situation occurs, restart SNMP by entering the following commands:

```
$ @SYS$STARTUP:TCPIP$SNMP_SHUTDOWN.COM
$ @SYS$STARTUP:TCPIP$SNMP_STARTUP.COM
```

3.14.2 SNMP IVP error

On slow systems, the SNMP Installation Verification Procedure can fail because a subagent does not respond to the test query. The error messages look like this:

```
   .
   .
   .
Shutting down the SNMP service... done.

Creating temporary read/write community SNMPIVP_153.

Enabling SET operations.

Starting the SNMP service... done.

SNMPIVP: unexpected text in response to SNMP request:
"- no such name - returned for variable 1"
See file SYS$SYSDEVICE:[TCPIP$SNMP]TCPIP$SNMP_REQUEST.DAT for more
details.
sysContact could not be retrieved.  Status = 0
The SNMP IVP has NOT completed successfully.
SNMP IVP request completed.
Press Return to continue ...
```

You can ignore these types of messages in the IVP.

3.14.3 Using existing MIB subagent modules

If an existing subagent does not execute properly, you may need to relink it against the current version of TCP/IP Services to produce a working image. Some subagents (such as those for HP Insight Management Agents for OpenVMS) also require a minimum version of OpenVMS and a minimum version of TCP/IP Services.

The following restrictions apply:

- In general, only executable images linked against the following versions of the eSNMP shareable image are upward compatible with the current version of TCP/IP Services:
  - UCX$ESNMP_SHR.EXE from TCP/IP Services Version 4.2 ECO 4
  - TCPIP$ESNMP_SHR.EXE from TCP/IP Services Version 5.0A ECO 1

  Images built under versions other than these can be relinked with one of the shareable images, or with TCPIP$ESNMP_SHR.EXE in the current version of TCP/IP Services.
- The underlying eSNMP API changed from DPI in TCP/IP Services Version 5.0 to AgentX in later versions of TCP/IP Services. Therefore, executable images linked against older object library versions of the API (*$ESNMP.OLB) must be relinked against either the new object library or the new shareable image. Linking against the shareable image ensures future upward compatibility and results in smaller image sizes.

  Note

  Although images may run without being relinked, backward compatibility is not guaranteed. Such images can result in inaccurate data or run-time

problems.

- This version of TCP/IP Services provides an updated version of the UCX$ESNMP_SHR.EXE shareable image to provide compatibility with subagents linked under TCP/IP Services Version 4.2 ECO 4. Do not delete this file.
- The SNMP server responds correctly to SNMP requests directed to a cluster alias. Note, however, that an unexpected host may be reached when querying from a TCP/IP Services Version 4.*x* system that is a member of a cluster group but is not the current impersonator.
- The SNMP master agent and subagents do not start if the value of the logical name TCPIP$INET_HOST does not yield the IP address of a functional interface on the host when used in a DNS query. This problem does not occur if the server host is configured correctly with a permanent network connection (for example, Ethernet or FDDI). The problem can occur when a host is connected through PPP and the IP address used for the PPP connection does not match the IP address associated with the TCPIP$INET_HOST logical name.
- Under certain conditions observed primarily on OpenVMS VAX systems, the master agent or subagent exits with an error from an internal `select( )` socket call. In most circumstances, looping does not occur. If looping occurs, you can control the number of iterations by defining the TCPIP$SNMP_SELECT_ERROR_LIMIT logical name.
- The MIB browser provided with TCP/IP Services (TCPIP$SNMP_REQUEST.EXE) supports `getnext` processing of OIDs that include the 32-bit OpenVMS process ID as a component. However, other MIB browsers may not provide this support.

  For example, the following OIDs and values are supported on OpenVMS:

  ```
  1.3.6.1.2.1.25.4.2.1.1.1321206828 = 1321206828
  1.3.6.1.2.1.25.4.2.1.1.1321206829 = 1321206829
  1.3.6.1.2.1.25.4.2.1.1.1321206830 = 1321206830
  ```

  These examples are from `hrSWRunTable`; the `hrSWRunPerfTable` may be affected as well.
- You can ignore the following warning that appears in the log file if a null OID value (0.0) is retrieved in response to a `Get`, `GetNext`, or `GetBulk` request:

  ```
  o_oid; Null oid or oid->elements, or oid->nelem == 0
  ```

3.14.4 Upgrading SNMP

After upgrading to the current version of TCP/IP Services, you must disable and then enable SNMP using the TCPIP$CONFIG.COM command procedure. When prompted for "this node" or "all nodes," select the option that reflects the previous configuration.

3.14.5 Communication controller data not completely updated

When you upgrade TCP/IP Services and then modify an existing communication controller, programs that use the communication controller might not have access to the updated information.

To ensure that programs like the MIB browser (SNMP_REQUEST) have access to the new data about the communication controller, do the following:

1. Delete the communication controller using the TCP/IP management command DELETE COMMUNICATION_CONTROLLER.
2. Reset the communication controller by running the TCPIP$CONFIG.COM command procedure and exiting.
3. Restart the program (such as SNMP) by entering the following commands:

   ```
   $ @SYS$STARTUP:SNMP_SHUTDOWN.COM

   $ @SYS$STARTUP:SNMP_STARTUP.COM
   ```

4. Use the TCP/IP management command LIST COMMUNICATION_CONTROLLER to display the information.

3.14.6 SNMP MIB browser usage

If you use either the `-l` (loop mode) or `-t` (tree mode) flag, you cannot also specify the `-m` (maximum repetitions) flag or the `-n` (nonrepeaters) flag. The latter flags are incompatible with loop mode and tree mode.

Incorrect use of the `-n` and `-m` flags results in the following types of messages:

```
$ snmp_request mynode.co.com public getbulk -v2c -n 20 -m 10 -t 1.3.6.1.2.1
Warning: -n reset to 0 since -l or -t flag is specified.
Warning: -m reset to 1 since -l or -t flag is specified.
1.3.6.1.2.1.1.1.0 = mynode.company.com
```

3.14.7 Duplicate subagent identifiers

With this version of TCP/IP Services, two subagents can have the same identifier parameter. Be aware, however, that having two subagents with the same name makes it difficult to determine the cause of problems reported in the log file.

3.14.8 Community name restrictions

The following restrictions on community names are imposed by TCPIP$CONFIG.COM:

- Do not specify community names that include a space character.
- A quotation mark (") specified as part of a community name might be handled incorrectly. Check the validity of the name with the SHOW CONFIGURATION SNMP command, and if necessary, correct the name with the SET CONFIGURATION SNMP command.

3.14.9 eSNMP programming and subagent development

The following notes pertain to eSNMP programming and subagent development.

- In the documentation, the terms "extension subagent", "custom subagent", and "user-written subagent" refer to any subagent other than the standard subagents for MIB-II and the Host Resources MIB, which are provided as part of the TCP/IP Services product.

- In the [.SNMP] subdirectory of TCPIP$EXAMPLES, files with the .C, .H, .COM, .MY, and .AWK extensions contain additional comments and documentation.
- The TCPIP$SNMP_REQUEST.EXE, TCPIP$SNMP_TRAPSND.EXE, and TCPIP$SNMP_TRAPSND.EXE programs are useful for testing during extension subagent development.
- For information about prototypes and definitions for the routines in the eSNMP API, see the TCPIP$SNMP:ESNMP.H file.

3.14.10 SNMP installation verification program restriction

The SNMP Installation Verification Program will not run correctly if `debug` or `trace` options are turned on for any TCP/IP Services for OpenVMS component.

For example, including the line:

```
options debug
```

in `TCPIP$ETC:RESOLV.CONF` results in unsuccessful completion status.

The problem also exists if socket tracing is turned on and directed to `SYS$OUTPUT` with the following command:

```
$ DEFINE TCPIP$SOCKET_TRACE SYS$OUTPUT
```

The additional output produced by these and other `debug` or `trace` options can cause problems with the SNMP IVP because it was designed to parse output from a standard configuration only.

Note

To run the SNMP IVP test either run the program directly:

```
$ RUN SYS$SYSROOT:[SYSTEST.TCPIP]TCPIP$SNMPIVP.EXE
```

or execute the TCPIP configuration menu:

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

and then select option "7 - Run tests" and then option "2 - SNMP IVP".

3.15 SSH problems and restrictions

This section contains the following information:

- SSH-related security advisories (Section 3.15.1)
- SSH general notes and restrictions (Section 3.15.2)
- UNIX features that are not supported by SSH (Section 3.15.3)
- SSH command syntax notes and restrictions (Section 3.15.4)
- SSH authentication notes and restrictions (Section 3.15.5)
- SSH keys notes and restrictions (Section 3.15.6)
- SSH session restrictions (Section 3.15.7)
- SSH messages notes and restrictions (Section 3.15.8)
- SSH remote command notes and restrictions (Section 3.15.9)

- SSH batch mode restrictions (Section 3.15.10)
- X11 port forwarding restrictions (Section 3.15.12)
- File transfer restrictions (all file sizes) (Section 3.15.13)
- File transfer restrictions (large files) (Section 3.15.14)

Note

References to SSH, SCP, or SFTP commands also imply SSH2, SCP2, and SFTP2, respectively.

3.15.1 SSH-Related security advisories

Computer Emergency Readiness Team (CERT®) advisories are issued by the CERT Coordination Center (CERT/CC), a center of Internet security expertise located at the Software Engineering Institute, a federally-funded research and development center operated by Carnegie Mellon University. CERT advisories are a core component of the Technical Cyber Security Alerts document featured by the United States Computer Emergency Readiness Team (US-CERT), which provides timely information about current security issues, vulnerabilities, and exploits.

CERT and HP Software Security Response Team (SSRT) security advisories might be prompted by SSH activity. CERT advisories are documented at the following CERT/CC web site:

`http://www.cert.org/advisories.`

Table 3–1 provides brief interpretations of several SSH-related advisories:

Table 3–1 CERT/SSRT Network Security Advisories

Advisory	Impact on OpenVMS
CERT CA-2003-24	OpenSSH only; OpenVMS is not vulnerable.
CERT CA-2002-36	A worst case consequence of this vulnerability is a denial of service (DoS) for a single connection of one of the following types: • Server process handling a connection from a malicious client • Client process connecting to a malicious server In either case, a malicious remote host cannot gain access to the OpenVMS host (for example, to execute arbitrary code), and the OpenVMS server is still able to receive a new connection.
CERT-2001-35	OpenVMS is not vulnerable. Affects SSH Version 1 only, which is not supported.
CERT CA-1999-15	RSAREF2 library is not used; OpenVMS is not vulnerable.
SSRT3629A/B	OpenVMS is not vulnerable.

3.15.2 SSH general notes and restrictions

This section includes general notes and restrictions that are not specific to a particular SSH application.

- The UNIX path `/etc` is interpreted by the OpenVMS SSH server as TCPIP$SSH_DEVICE:[TCPIP$SSH].
- The following images are not included in this release:
  - TCPIP$SSH_SSH-CERTENROLL2.EXE

    This image provides certificate enrolment.
  - TCPIP$SSH_SSH-DUMMY-SHELL.EXE

    This image provides access to systems where only file transfer functionality is permitted.
  - TCPIP$SSH_SSH-PROBE2.EXE

    This image provides the `ssh-probe2` command, which sends a query packet as a UDP datagram to servers and then displays the address and the SSH version number of the servers that respond to the query.

3.15.3 UNIX features that are not supported by SSH

This section describes features that are expected in a UNIX environment but are not supported by SSH for OpenVMS.

- The server configuration parameter `PermitRootLogin` is not supported.
- The client configuration parameter `EnforceSecureRutils` is not supported.
- There is no automatic mapping from the UNIX ROOT account to the OpenVMS SYSTEM account.
- The SSH1 protocol suite is not supported for terminal sessions, remote command execution, and file transfer operations. Parameters unique to SSH1 in the server and client configuration files are ignored.

3.15.4 SSH command syntax

This section includes notes and restrictions pertaining to command syntax.

- From a non-OpenVMS client, if you use OpenVMS syntax for names (such as device names), enclose the names in single quotation marks to prevent certain characters from being interpreted as they would be on a UNIX system.

  For example, in the following command, UNIX interprets the dollar sign ($) as a terminator in the device name SYS$SYSDEVICE:[*user*], resulting in SYS:[*user*].

  ```
  # ssh user@vmssystem directory SYS$SYSDEVICE:[user]
  ```

  To avoid this problem, enter the command using the following format:

  ```
  # ssh user@vmssystem directory 'SYS$SYSDEVICE:[user]'
  ```

3.15.5 SSH authentication

This section includes notes and restrictions pertaining to SSH authentication.

- The location of the SHOSTS.EQUIV file has been moved from TCPIP$SSH_DEVICE:[TCPIP$SSH] to TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2].
- If hostbased authentication does not work, the SSH server may have failed to match the host name sent by the client with the one it finds in DNS/BIND. You can check whether this problem exists by comparing the output of the following commands (ignoring differences in case of the output text):
  - On the server host:

    ```
    $ TCPIP
    TCPIP> SHOW HOST client-ip-address
    ```

  - On the client host:

    ```
    $ write sys$output -
    $_ "''f$trnlnm("TCPIP$INET_HOST")'.''f$trnlnm("TCPIP$INET_DOMAIN")'"
    ```

    If the two strings do not match, you should check the host name and domain configuration on the client host. It may be necessary to reconfigure and restart TCP/IP Services on the client host.
- If the user default directory in the SYSUAF user record is specified with angle brackets (for example, <*user-name*>) instead of square brackets ([*user-name*]), hostkey authentication fails. To solve this problem, change the user record to use square brackets.
- The pairing of user name and UIC in the OpenVMS rights database, as displayed by the AUTHORIZE utility's SHOW /IDENTIFIER command, must match the pairing in the SYSUAF record for that user name. If the pairings do not match, the following message error is displayed when the user attempts to establish an SSH session:

```
$ ssh hosta
%SYSTEM-F-ACCVIO, access violation, reason mask=00,
virtual address=000000000000 0000, PC=FFFFFFFF811A88E8, PS=0000001B

  Improperly handled condition, image exit forced.
    Signal arguments:   Number = 0000000000000005
                        Name   = 000000000000000C
                                 0000000000000000
                                 0000000000000000
                                 FFFFFFFF811A88E8
                                 000000000000001B

    Register dump:
    R0  = FFFFFFFFFFFFFFFE  R1  = 0000000000495D08  R2  = 000000000001DEE0
    R3  = 00000000004ABE18  R4  = 0000000000000000  R5  = 0000000000000000
    R6  = 0000000000000000  R7  = 0000000000000000  R8  = 0000000000000000
    R9  = 0000000000000000  R10 = 0000000000000000  R11 = 00000000002F7C20
    R12 = 0000000000000000  R13 = 0000000000498708  R14 = 00000000004EDF48
    R15 = 000000007AECFE10  R16 = 0000000000000000  R17 = 0000000000000000
    R18 = 0000000000000000  R19 = 000000007B624258  R20 = 0000000077770000
    R21 = 0000000000000008  R22 = FFFFFFFF77774A00  R23 = 0000000300000000
    R24 = 0000000000000001  R25 = 0000000000000001  R26 = 0000000000118A6C
    R27 = 000000007C062700  R28 = 0000000000000000  R29 = 000000007ADEF290
    SP  = 000000007ADEF290  PC  = FFFFFFFF811A88E8  PS  = 100000000000001B
```

To solve this, use the AUTHORIZE utility to correct the pairing of user name and UIC value in the OpenVMS rights database.

3.15.6 SSH keys

This section includes notes and restrictions pertaining to SSH keys.

- SSH client users can copy their own customized version of the SSH2_ CONFIG. file and modify the value of the variable `StrictHostKeyChecking`. By setting the value of this variable to "no," the user can enable the client to automatically copy the public key (without being prompted for confirmation) from an SSH server when contacting that server for the first time.

  A system manager can tighten security by setting the `StrictHostKeyChecking` variable to "yes" in the systemwide SSH2_CONFIG. file, and forcing users to use only the systemwide version of the file. In this case, to copy the public key from the server, users (and the system manager) must use another mechanism (for example, a privileged user can manually copy the public key). To enforce this tighter security response, the system manager can perform the following steps:

  1. Edit TCPIP$SSH_DEVICE:[TCPIP$SSH]SSH2_CONFIG. to include the following line:

     ```
     StrictHostKeyChecking  yes
     ```

  2. Restrict
     user access to TCPIP$SSH_DEVICE:[TCPIP$SSH]SSH2_CONFIG.
     For example:

     ```
     $ SET SECURITY/PROTECTION=(G,W) TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]SSH2_CONFIG.;
     ```

  3. Edit the SYS$STARTUP:TCPIP$SSH_CLIENT_STARTUP.COM command procedure to install the SSH server image with the READALL privilege. In the following example, change the existing line to the replacement line, as indicated:

     ```
        .
        .
        .
     $     image = f$edit("sys$system:tcpip$ssh_ssh2.exe","upcase")
     $!    call install_image 'image' ""          <== existing line
     $     call install_image 'image' "readall"   <== replacement
        .
        .
        .
     ```

  4. Enable the SSH client, as described in the *HP TCP/IP Services for OpenVMS Guide to SSH*.

  Note

  Steps 2 and 3 involve modification of system files. Therefore, it may be necessary to repeat the modifications after a future update of TCP/IP Services.

- If you do not specify the key file in the SSH_ADD command, and SSH_ADD finds no INDENTIFICATION. file, it adds only the first private key it finds in the [*username*.SSH2] directory.
- Do not use the SSH_KEYGEN `-e` option (used to edit the comment or passphrase of the key). This option does not work.

- With this release, the default size of keys generated by the SSH_KEYGEN utility is 2048 bits (for earlier releases, the default size was 1024 bits). Consequently, generation of keys takes longer — sometimes five to ten times longer. On slow systems, or during SSH configuration, key generation may seem to be hanging when it is not. No progress indicator is displayed. During SSH configuration, the following messages indicate the keys are being generated:

  ```
  Creating private key file: TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]HOSTKEY
  Creating public key file: TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]HOSTKEY.PUB
  ```

  Note

  While the keys are being generated, you might notice a delay. This does not indicate a hang.

3.15.7 SSH sessions

This section includes restrictions pertaining to SSH sessions.

- In an SSH session on the OpenVMS server, the originating client host name and the user name or port identification are not available. For example, in a TELNET session, the OpenVMS DCL command SHOW TERMINAL displays the following information about a UNIX client:

  ```
  Remote Port Info: Host: unixsys.myco.com Port:2728
  ```

  Likewise, information about an OpenVMS client appears as:

  ```
  Remote Port Info: Host: mysys.com Locn:_RTA4:/USER
  ```

  Neither of these lines is displayed in a similar SSH session; however, information for SSH sessions is available in the logical names SYS$REM_ID (username) and SYS$REM_NODE and SYS$REM_NODE_FULLNAME (hostname)

- Starting SSH sessions recursively (for example, starting one SSH session from within an existing SSH session) creates a layer of sessions. Logging out of the innermost session may return to a layer other than the one from which the session was started.
- SSH escape sequences are not fully supported. For example, you may have to enter the `Escape .` (escape character followed by a space and a period) exit sequence twice for it to take effect. On exit, the terminal is left in NOECHO and PASTHRU mode.
- On certain non-OpenVMS clients, after attempting to exit from an SFTP session, you must press Enter an extra time to return to the operating system prompt.

3.15.8 SSH messages

This section includes notes and restrictions pertaining to SSH session messages.

- Normally, the translation of the system logical name SYS$ANNOUNCE is displayed after authentication is complete. In this version of SSH, no automated mechanism exists for displaying this text as a prelogin banner.

  To provide a prelogin banner from a text file, create the file SSH_BANNER_MESSAGE. containing the text to be displayed before login.

To enter multiple lines in the banner text, make sure each line ends with an explicit carriage-return character except the last line.

Save the banner message file in the TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2] directory, with privileges that allow it to be read by the user account [TCPIP$SSH].

If you do not use the default file name and location for the message banner file, define them using the `BannerMessageFile` option in the TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]SSHD2_CONFIG. file. Specify the location and file name of your banner message file as the argument to the option using one of the following formats:

```
BannerMessageFile   TCPIP$SSH_DEVICE:[TCPIP$SSH]BANNER1.TXT
BannerMessageFile   /TCPIP$SSH_DEVICE/TCPIP$SSH/BANNER2.TXT
BannerMessageFile   /etc/banner3.txt
```

Note that the argument may be in either OpenVMS or UNIX format and is not case sensitive. (If multiple definitions for the same option are included in the configuration file, the last one listed will take effect.)

- Some SSH informational, warning, and error message codes are truncated in the display. For example:

  ```
  %TCPIP-E-SSH_FC_ERR_NO_S, file doesn't exist
  ```

- Some SSH log and trace output messages, and informational, warning, and error messages display file specifications as UNIX path names.

3.15.9 SSH remote commands

This section includes notes and restrictions pertaining to SSH remote commands.

- Command lines for remote command execution through SSH are limited to 153 characters.
- After you execute an SSH remote command, you may need to press the Enter key to get back to the DCL prompt.
- When you execute remote commands on the OpenVMS SSH server, the log file TCPIP$SSH_RCMD.LOG is created in the directory defined by the logical name SYS$LOGIN for your user account. This log file is not purged automatically.
- When you execute remote commands on an OpenVMS SSH client connected to a non-OpenVMS SSH server, output may not be displayed correctly. For example, sequential lines might be offset as if missing a linefeed, as in the following example:

```
$ ssh user@unixhost ls -a
  user's password:
  Authentication successful.
  .
   ..
     .TTauthority
                 .Xauthority
                           .cshrc
                                 .dt
                                    .dtprofile
```

To display the output correctly, use the -t option with the command, as in the following command example:

```
$ ssh -t user@unixhost ls -a
```

- Any OpenVMS command that refreshes the display can have unexpected results when executed as a remote SSH command. For example, the following command exhibits this behavior:

  ```
  $ MONITOR PROCESS /TOPCPU
  ```

  Executed locally, this command displays a bar chart that is continuously updated. When executed as a remote command, it displays each update sequentially. In addition, you cannot terminate the command using Ctrl/C.

3.15.10 SSH batch mode

This section includes batch mode restrictions.

- Because the SSH, SFTP, and SCP commands are implemented by code ported from UNIX sources, they do not support all of the standard OpenVMS behaviors for SYS$INPUT, SYS$OUTPUT, and SYS$ERROR in command procedures. For example:
  - SYS$INPUT is not the default batch command procedure.
  - Output written to a batch log file or other SYS$OUTPUT file may have an extra <CR> (ASCII decimal 13) or other explicit formatting characters.
  - You can direct SYS$OUTPUT to a file, as in the following example:

    ```
    $ ASSIGN OUT.DAT SYS$OUTPUT
    ```

- When you run these commands from an interactive command procedure, you should use the explicit UNIX batch mode flags, as listed in the following table:

For...	Use...
SSH (remote command execution or port forwarding),	`-o batchmode yes`
SCP,	`"-B"`
SFTP,	`"-B" {`*batchfile*`}`

- If you use the SSH command in batch mode with an interactive session (that is, not for remote command execution or setting up port forwarding), the batch job hangs.

  If the -s option is used in an interactive SSH session, or with an SSH command executed interactively in a DCL command procedure, the terminal session hangs. Ctrl/Y and Ctrl/C will not restore the DCL prompt. To release the hung terminal session, you must restart the SSH client and server.

- For the SFTP command, note the following:
  - If the command is used without the -B {*batchfile*} option, SFTP uses the following file by default: SYS$LOGIN:TCPIP$SFTP_BATCHFILE.TXT.

- When running in batch mode:
  - The SFTP command displays the final state-of-progress indicator; the SCP command does not.
  - The SSH command will not prompt for a password, password update, or passphrase. If one is required, the batch job fails.
  - The SSH command will not cause a new host key to be saved if the value of `StrictHostkeyChecking` is "no;" SSH will not prompt for one if the value is "ask."

    For other notes and restrictions pertaining to keys, see Section 3.15.6.
  - If an `ls` command is contained in the SFTP batch input, and the interactive output requires input from the keyboard to continue, then some of the output lines might be omitted from the batch log file.

3.15.11 ls fails after cd to a logical name from a Tru64 UNIX client

`ls` can fail when using `sftp cd` to a logical name from a Tru64 UNIX client.

For a workaround, try the following:

1. `cd` to the path for the directory in UNIX format, e.g., instead of: `cd tcpip$ssh_home`, use `cd /sys$sysdence/tcpip$ssh`.
2. Perform the `ls` specifying the logical name in the path, e.g., `ls /tcpip$ssh_home`.

3.15.12 SSH X11 port forwarding

This section includes X11 port forwarding restrictions and problems.

- To use X11 forwarding in native mode, the system must be running DECwindows MOTIF Version 1.3 or higher. In addition, the X Authority utility (xauth) is required on the system. The X11 server uses this utility for authenticating host/user connections. For more information on how to use this utility, see the HP DECwindows Motif for OpenVMS documentation.
- To display a remote X11 client application on your X11 server, you must set the display variable on the X11 client to the address of the X11 server the client is connecting to. You can verify that the variable is set correctly on an OpenVMS system by using the following DCL command:

  ```
  $ SHOW LOGICAL DECW$DISPLAY
  ```

  For WSA display devices, use the SHOW DISPLAY command to see the display variable value.

  To set the display variable on an OpenVMS client to point to your server, use the SET DISPLAY command as in the following example, where 127.127.1.1 is the server node address:

  ```
  $ SET DISPLAY/CREATE/NODE=127.127.1.1/TRANSPORT=TCPIP
  ```

  SSH on OpenVMS supports only local and TCP/IP transports. If you are using a local transport, you have to be at the system where the display is to appear, and that system must be running the X11 server. For local transport, use the following command to set the display:

  ```
  $ SET DISPLAY/CREATE/TRANSPORT=LOCAL
  ```

On UNIX systems, use the following command to set the display variable to point to a server node with address 16.20.176.33 and using the TCP/IP transports:

```
>setenv display 16.20.176.33:0.0
```

To use local transport, use the following UNIX command:

```
>setenv display :0.0
```

- To set up a standard port forwarding session for X11 on a remote OpenVMS system, HP recommends that you use remote port forwarding; local port forwarding will not work.

3.15.13 SSH file transfer (All File Sizes)

This section includes SSH restrictions pertaining to file transfer operations.

- Using the colon character ":" in the pathname for the source and destination filename parameters in an SCP command may cause a delay.

  Due to an overloading of the colon character in SCP syntax to indicate a hostname and in OpenVMS as a path delimiter, what is intended to be an OpenVMS logical name for a device or directory in an SCP file parameter may be checked as a hostname first and passed to a DNS lookup. Normally this is benign, but this could incur an otherwise unexplainable wait in an environment experiencing DNS lookup delays. To avoid the possibility of confusion, use UNIX-style filename syntax.

- On OpenVMS, setting the `ForcePTTYAllocation` keyword to "yes" in the SSH2_CONFIG. file can result in failures when performing file copy operations. (In other implementations of SSH, setting the keyword `ForcePTTYAllocation` to "yes" in the SSH2_CONFIG. file has the same effect as using the `-t` option to the SSH command.)

- When connected to some servers, the client can detect packet benign file transfer protocol packet-length errors. By default, no message is displayed.

  To display warning messages, type the following:

  ```
  $ DEFINE/SYS NO TCPIP$SSH_TOLERANT_PROTOCOL STATUS
  ```

  using either the "NO" or any string starting with an upper- or lowercase N.

  Following is an example of a warning message:

  ```
  Warning: packet length mismatch: expected 27,
  got 8; connection to non-standard server?
  ```

  To retain the logical name assignment through each reboot, add the DEFINE command to the appropriate startup command procedure.

- VMS Plus Mode:

  When the client and the server are OpenVMS systems running v5.6, they recognize each other as such and implement TCP/IP Services specific SFTP protocol extensions that allow transfer of files in either direction while preserving the key OpenVMS file attributes: record format and record attributes.

  The TCP/IP Services SCP client uses SFTP as the underlying protocol so VMS Plus mode works with SCP as well.

  VMS Plus mode supports only sequential organization files.

Remember that if a v5.6 system is connected with an older TCP/IP Services system that does not support VMS Plus mode, file attributes will not be preserved. VMS Plus mode can only be used if both sides support it.

- Talking to a system without VMS Plus:

  If one side of the file transfer, client or server, does not support VMS Plus mode for SFTP, file attributes will not be preserved.

  In this mode TCP/IP Services supports reading of any of the following types of sequential organization files:

  - Stream_LF
  - Variable Length
  - VFC
  - Fortran Carriage Control
  - Fixed Length
  - Undefined

  Note that which side is the server and which is the client is irrelevant. OpenVMS is simply running on the side that is reading the file. You can, for example, use SFTP client from OpenVMS to put a VFC file to UNIX, or you could use the SFTP client on the UNIX system to get the same file from the OpenVMS system. In either case, the OpenVMS system is reading the file and the Unix file is writing it.

  Copying some VFC files from OpenVMS to systems not running OpenVMS and then back to OpenVMS may result in a file that the OpenVMS `DIFFERENCES` command shows as different from the original file. This is unpreventable and the file as transferred out and back in is correct in that the `TYPE` and `PRINT` commands display it as expected and the output here is the same as that for the original file.

  Copying Fortran CC files from OpenVMS to systems other than OpenVMS will always result in a file that shows differences from the original. This is because on its transfer from OpenVMS to UNIX the Fortran CC attributes were converted to inline ASCII control character sequences that print the lines as the Fortran CC control bytes require. For example, the Fortran character for overstrike results in a pair of carriage returns for the line thus implementing an overstrike.

- TCP/IP Services supports only sequential file organization, not relative or indexed files

  To transfer these unsupported files you can package the file(s) into an OpenVMS saveset and transfer that or, depending on how many hops over which SFTP/SCP implementations and operating systems, you may need to use more extreme measures. One way that works consistently (provided that you have FTSV installed) is packaging files into a save set, then using SPOOL COMPRESS to make them into an self-extracting VMS image, then using UUENCODE to transform the image into an ASCII text file.

- Not all variants of UNIX path names are supported when referring to files on OpenVMS clients and servers.

- The SCP and SFTP commands from the following Windows clients have been tested and interoperate correctly with the OpenVMS SSH server:

  – PuTTY

– SSH Communications

Other versions and other clients may work, depending on protocol implementation and factors such as whether the client can handle OpenVMS-format file specifications.

- When using the SFTP command, pressing Ctrl/C does not display "Cancel" as expected. Also, Ctrl/T does not work as in DCL to display a status line; instead, it switches two adjacent characters, as on UNIX systems. Other problems with character handling have been fixed.
- The SFTP `ls` command pauses for an extended time after displaying a page of data and then continues with the next page. This occurs because the ssh server is sending back a complete directory listing, which the client filters; therefore, for directories with many files, the delay is due to the client waiting for listing results from the server. This is typical SFTP behavior, and not specific to OpenVMS.
- Using SCP or SFTP command to copy a file back to itself (either in local mode, or by connecting back to the client host) fails with the following error:

```
%TCPIP-E-SSH_FC_ERR_INVA, file record format invalid for copy
```

- The SCP command issued from a client using SSH Version 1 will not work with the OpenVMS SSH server. The OpenVMS server does not support SSH Version 1.

3.15.14 SSH transferring large files

This section includes restrictions pertaining to transferring large files:

- The minimum version of DECC$SHR running on your system must be that which was released with OpenVMS Version 8.2.
- You may need to adjust memory parameters (WSDEF, WSQUO, WSEXTENT, and PGFLQUO) to accommodate the memory requirements of the file copy client and server. The exact value depends on system resources and virtual memory configuration. For more information, see Section 2.3. For ssh filecopy, testing has shown that the main parameter to adjust is PGFLQUO.

3.15.15 SSH server signals internal credentials cache error

If an SSH client attempts to use gssapi-with-mic authentication to the TCP/IP Services for OpenVMS SSH server on a server host that is running Kerberos V2.1 and the SSH client user's TGT is forwardable (a kinit -f has been done) and the GssapiDelegateCredentials flag is set then the SSH server will signal the following error in the server log:

```
Internal credentials cache error
```

This error text may appear on the SSH client user's screen, depending on configuration.

This can be worked around in either of the following ways:

1. Upgrade to Kerberos V3.0 on the SSH server host.
2. Use the `kinit` without the `-f` flag on the SSH client.
3. Turn the GssapiDelegateCredentials configuration switch off on the SSH client.

Because forwarding of client credentials with gssapi-with-mic authentication to the OpenVMS SSH server is not supported setting GssapiDelegateCredentials is not necessary.

3.15.16 SFTP general problems and restrictions

This section includes SFTP general notes and restrictions.

- In an SFTP session, the ls command entered with the directory path in a OpenVMS syntax displays or lists the content of the directory in the UNIX syntax. For example:

```
sftp> ls [.ssh_testfiles]
./ssh_testfiles
./ssh_testfiles/98277_SLF.Z;1
```

- In a SFTP session, the ls -R command fails to handle sub-directories if the directory filename includes ODS-5 extended characters.
- The following sftp command with the "*.*" format does not provide the complete list of files:

```
sftp> ls [.ssh_testfiles]*.*
```

  However, you can use the following command formats to list all the files:

```
sftp> ls [.ssh_testfiles]*.*;*
sftp> ls [.ssh_testfiles]*
```

- The SFTP get command does not parse the correct version number to the file. For example, the following command gets the file with the version number, but the version number is invalid.

```
sftp> get TCPIP$FTP_SERVER.LOG;-5000000
```

- No error message is displayed with an SFTP get command on a file with an invalid version number and a wildcard character.
- In an SFTP session, the lrm command fails when the command is entered with wildcard character "*" as follows:

```
sftp> lrm *.*;*
Command failed.
sftp> lrm BIG_VFC.*;*
Command failed.
```

- The SFTP client exhibits a memory leak. It runs out of memory and generates an error message because of the extensive use of wildcard filenames in the get and put operations.

3.15.17 SFTP generates audit warnings with class device

This restriction applies only to those using AUDIT with class device as in the following command:

```
$ SET AUDIT/ALARM/ENABLE=ACCESS=ALL/CLASS=DEVICE
```

If the SFTP server generates audit warnings for a logical IO to a mailbox when the SFTP user exits SFTP, perform the following step to prevent this from occurring:

```
$ DEFINE/SYSTEM TCPIP$SSH_SERVER_WAIT_FOR_CHILD 1
```

3.15.18 BIND Resolver diagnostics creates an SSH packet corruption

When you turn on BIND Resolver Diagnostics using either of the following methods, you can create an SSH packet corruption:

- Define the logical name TCPIP$BIND_RES_OPTIONS to "debug".
- Add the following line to TCPIP$ETC:RESOLV.CONF:

  ```
  options debug
  ```

3.16 TCPDUMP restrictions

TCPDUMP works the same way on OpenVMS as it does on UNIX systems, with the following restrictions:

- On UNIX systems, tcpdump sets the NIC (Network Interface Controller) into promiscuous mode and everything in the transmission is sent to tcpdump.

  On OpenVMS systems, TCPDUMP only sees the packets destined for and sent from the local host. Therefore, TCPDUMP works in copy-all mode. Because it only sees a copy of the packets that are processed by the TCP/IP kernel, TCPDUMP can only trace natively IP, IPv6, and ARP protocols on Ethernet.

  TCPDUMP can format or filter packets that have been traced from another platform running TCPDUMP in promiscuous mode. In this case it will process other protocols, like DECnet.
- Ethernet is the only supported type of NIC. Other types of NICS (such as ATM, FDDI, Token Ring, SLIP, and PPP) are not supported.
- The -i option is not supported. On UNIX systems, this option specifies the interface that tcpdump is attached to.

  On OpenVMS systems, TCPDUMP obtains packets from the TCP/IP kernel.
- The -p option is not supported. On UNIX systems, this option specifies that tcpdump stops working in promiscuous mode.

  On OpenVMS, TCPDUMP does not work in promiscuous mode. Therefore, this option is set by default.
- If you are using the Ethereal software to dump IPv6 network traffic, use the following command format to write the data in the correct format:

  ```
  $ TCPDUMP -s 1500 -w filename
  ```
- Only one process at a time can issue traces. This restriction applies to both TCPTRACE and TCPDUMP.

3.17 TCP/IP Management Command restrictions

The following restrictions apply to the TCP/IP management commands:

- An IP address added to a tunnel interface cannot be seen with ifconfig. Execute netstat with -rn to view the new IP address.
- TCP/IP Services Version 5.4 introduced failSAFE IP, which obsoletes the IP cluster alias address. Consequently, the following TCP/IP management commands are no longer supported:
  - SET INTERFACE /NOCLUSTER
  - SHOW INTERFACE /CLUSTER

To display interface addresses, including IP cluster alias addresses, use the following TCP/IP management command:

```
TCPIP> ifconfig -a
```

To delete a cluster alias address from the active system, use a command similar to the following:

```
TCPIP> ifconfig ie0 -alias 10.10.10.1
```

The following TCP/IP management commands continue to be supported:

- SET INTERFACE/CLUSTER
- SET CONFIGURATION INTERFACE /CLUSTER
- SET CONFIGURATION INTERFACE /NOCLUSTER
- SHOW CONFIGURATION INTERFACE /CLUSTER

- SET NAME_SERVICE /PATH

  This command requires the SYSNAM privilege. If you enter the command without the appropriate privilege at the process level, the command does not work and you are not notified. If you enter the command at the SYSTEM level, the command does not work and you receive an error message.

- SET SERVICE command
  - When you modify parameters to a service, disable and re-enable the service for the modifications to take effect.
  - After a "SET SERVICE" command is used to define a new user defined TCP service, if the same "SET SERVICE" command is entered again, the service may appear disabled and cannot be re-enabled.

For more information on TCP/IP Services management commands, refer to the *HP TCP/IP Services for OpenVMS Management Command Reference* guide.

4
Corrections

This chapter describes the problems corrected in this version of TCP/IP Services.

4.1 Advanced Programming Environment problems fixed in this release

The following sections describe programming-related problems fixed in this release.

4.1.1 Buffer overflow in ntpq program

Problem:

The stack buffer overflows in the ntpq program.

Solution:

This problem is corrected in this release.

4.1.2 With PPE enabled, system crashes during shutdown

Problem:

When PPE is enabled, the system crashes during shutdown with the following message:

```
"SPLIPLLOW, IPL has fallen below level of owned spinlock(s)"
```

Solution:

This problem is corrected in this release.

4.2 BIND Server problems fixed in this release

The following sections describe BIND server problems fixed in this release.

4.2.1 Bind server crashes on receipt of dynamic update message

Problem:
Bind server crash can be caused on receipt of a specific remote dynamic update message.

Solution:

This problem is fixed in this release.

4.2.2 SYSTEM-W-NOSUCHFILE and %DCL-E-INVIFNEST Errors

Problem:
TCPIP$BIND_STARTUP.COM displays the %SYSTEM-W-NOSUCHFILE and %DCL-E-INVIFNEST errors when the SYS$SHARE:SSL$LIBCRYPTO_SHR32.EXE image is not present on the system.

Solution:

This problem is fixed in this release.

4.2.3 %LIBRAR-E-LOOKUPERR error in the BIND server

Problem:

While configuring TCP/IP, using TCPIP$CONFIG, in the BIND server, the %LIBRAR-E-LOOKUPERR error is displayed. TCPIP$CONFIG incorrectly looks for LOOPBACK_DB.

Solution:

This problem has been fixed in this release.

4.2.4 BINDSETUP fails to conform to the database filename

Problem:

TCPIP$BINDSETUP fails to conform to the new BIND local host database filename.

Solution:

This problem is corrected in this release.

4.2.5 Entering CTRL/C for TCPIP SHOW HOST (/NOLOCAL)

may display ACCIVO)
Problem:

On OpenVMS Integrity servers, entering CTRL/C for the `TCPIP SHOW HOST (/NOLOCAL)` command may display an ACCIVO error within the BIND resolver.

Solution:

This problem is corrected in this release.

4.2.6 Memory usage statistics

Problem:

This release adds the ability to generate and display the memory usage statistics for the BIND Server.

Solution:

To display the memory usage statistics for the BIND Server, define the logical name as follows:

```
$ DEFINE /SYSTEM TCPIP$BIND_MEMSTATS 1
```

TCPIP$BIND_MEMSTATS is an existing logical name. The value does not matter; but it must be defined.

Use either the `rndc stats` command or the `TCPIP SHOW NAME /STATISTICS` command to send the memory usage statistics to the file TCPIP$BIND.STATS. The memstats information will complement the server Statistics Dump information that is normally sent to the file.

4.2.7 Delay because of using "ROUTE ADD"

Problem:

There is a delay because of using the `ROUTE ADD` command when the BIND resolver is disabled.

Solution: This problem is corrected in this release.

4.2.8 Resolving the local host database names

Problem:

TCPDUMP, and potentially other applications, fails to resolve the local host database names. When _SOCKADDR_LEN is not defined, a call to the `getaddrinfo( )` function will not look in the local host database. When `getaddrinfo( )` was called with the hints argument as NULL, the routine fails with an ACCVIO.

Solution:

This problem is corrected in this release.

4.2.9 Unexpected IPv6-looking address in the TELNET client

Problem:

The `getaddrinfo( )` function sometimes returned AF_INET structures even when the AI_V4MAPPED flag was set. The most obvious effect was that attempting to reach an unresponsive host via TELNET would provoke a unexpected IPv6-looking address in the TELNET client and displays the `Trying ...` message.

Solution:

This problem is corrected in this release.

4.2.10 Specifying an invalid port number to getnameinfo()

Problem:

Specifying an invalid port number to `getnameinfo( )` results in an ACCVIO error.

Solution:

This problem is corrected in this release.

4.2.11 NI_* flag values for getnameinfo()

Problem:

The `getnameinfo( )` NI_* flag values were improperly changed for V5.6 when updating to the BIND 9 resolver. Changing these values broke applications that were built on pre_v5.6 versions of TCP/IP Services for OpenVMS.

Solution:

The NI_* flag values for the `getnameinfo( )` function were improperly changed with the V5.6 release. This would cause any applications using the NI_* flag values that were built against pre-V5.6 TCP/IP versions not to run as expected on TCP/IP V5.6. This problem has been corrected, and the flag values have been returned to their pre-V5.6 definitions. Note that any applications using the NI_* flag values that were built against V5.6 will no longer execute properly on V5.6 ECO1 or later. These applications must be rebuilt.

4.2.12 TCPIP$SYSTEM:HOSTS.DAT ASCII file

Problem:

The undocumented TCPIP$SYSTEM:HOSTS.DAT ASCII file is still provided during TCP/IP installation, but the file is no longer used by the BIND resolver.

Solution:

This problem is corrected in this release.

4.2.13 Query IDs

Problem:

Query IDs generated by the DNS server are vulnerable to cryptographic analysis.

Solution:

This problem is corrected in this release.

4.2.14 BIND cluster-wide startup and shutdown command procedures

Problem:

BIND cluster-wide startup and shutdown command procedures are generated with embedded physical device names, requiring extra effort upon changing to a new system disk.

Solution:

This problem is corrected in this release.

4.2.15 BIND9 Resolver aborts

Problem:

The BIND9 Resolver aborts when multiple threads called `getadrinfo` simultaneously, although, RFC 3493 describes `getaddrinfo` as a thread safe or re-entrant function.

Solution:

This problem is corrected in this release.

4.2.16 Spoofing and cache-poisoning attack in a BIND/DNS server

Problem:

The BIND/DNS server is vulnerable to a widely publicized spoofing and cache-poisoning attack.

Solution:

This problem is corrected in this release.

4.2.17 Spoofing and cache-poisoning attack in a UDP port

Problem:

The BIND/DNS cache server uses a fixed or an arbitrarily selected UDP port for out going DNS queries. This will lead to UDP port spoofing and cache-poisoning attack.

Solution:

This problem is corrected in this release.

4.2.18 Memory leaks in BIND Resolver functions

Problem:

The BIND Resolver functions, GETNAMEINFO, GETHOSTBYNAME, GETHOSTBYADDR GETNETBYNAME,GETNETBYADDR,GETSERVBYNAME and GETSERVBYPORT causes memory leaks and does not close the files properly when called from a multithreaded program.

Solution:

This problem is corrected in this release.

4.2.19 GETADDRINFO with nodename as NULL fails

Problem:

getaddrinfo with nodename as NULL fails with `BADHINTS: Not found in explore`

Solution:

This problem is corrected in this release.

4.3 DHCP component problems fixed in this release

The following sections describe the DHCP problems fixed in this release.

4.3.1 DHCP server fails to update the DNS server correctly

Problem:

When DNS updates are enabled, the DHCP server fails to update the DNS server correctly if the netmask for the client's network differs from 255.255.255.0.

Solution:

This problem is corrected in this release.

4.3.2 RMS-E-FLK errors when running the TCPIP$$SETHOSTNAME.COM script's SET HOST and SET NOHOST commands

Problem:

The DHCP client, when run in a cluster where the TCPIP$* data files are shared between cluster members, could incur RMS-E-FLK errors when running the TCPIP$$SETHOSTNAME.COM script's SET HOST and SET NOHOST commands.

Solution:

This problem is corrected in this release.

4.3.3 DHCP server listens on all interfaces

Problem:

The OpenVMS DHCP server cannot be disabled on one or more interfaces. The server always listens on all the interfaces.

Solution:

A new logical, TCPIP$DHCP_IGNOR_IFS is now supported to fix this problem.

4.3.4 DHCPSIGHUP command is issued twice

Problem:

The DHCPSIGHUP command is issued twice to update the DHCP Debug Level.

Solution:

This problem is corrected in this release.

4.3.5 DHCP server logs events on ignored interfaces

Problem:

DHCP server logs events on ignored interfaces. Logging events for ignored interfaces leads to huge log files.

Solution:

This problem is corrected in this release.

4.4 failSAFE IP problems fixed in this release

The following sections describe failSAFE IP problems fixed in this release.

4.4.1 failSAFE IP does not read its configuration file

Problem:

failSAFE IP does not read its configuration file if stored in the STREAM_LF format.

Solution:

This problem is corrected in this release.

4.4.2 failSAFE IP may pick the wrong interface to monitor

Problem:

In some configurations, the failSAFE IP may pick the wrong interface to monitor. This is displayed on OPCOM and in the logfile during failSAFE IP startup.

Solution:

This problem is corrected in this release.

4.4.3 If interface_list not specified, default behavior does not work

Problem:

If the `interface_list` is not specified, by default, all the interfaces must be monitored. One of the earlier ECO release did not support the default behavior.

Solution:

This problem is corrected in this release.

4.4.4 IP failover sometimes losses the default route

Problem:

failSAFE IP failover sometimes losses the default route when IPv6 is configured.

Solution:

This problem is corrected in this release.

4.4.5 First static route failover

Problem:

Under certain circumstances, only the first static route reliably fails over. This is typically the default route.

Solution:

This problem is corrected in this release.

4.5 FINGER Component problems fixed in this release

The following sections describe FINGER component problems fixed in this release.

4.5.1 File access restrictions when following symbolic links.

Problem:

The FINGER server does not properly enforce the file access restrictions when following symbolic links. The client is vulnerable to a format string attack.

Solution:

This problem is corrected in this release.

4.6 FTP Server and Client problems fixed in this release

The following sections describe FTP server and client problems fixed in this release.

4.6.1 OpenVMS, TCP/IP, or Non-VMS FTP client access to ODS-5 disk

Problem:
On a non-VMS FTP client, such as Windows, UNIX, or LINUX, the filenames are displayed in the VMS format with the "^" characters in the filename. Also, when retrieving the filenames using the non-VMS FTP client, the filename in OpenVMS format is displayed with "^", such as file^.1^.2^.3^.4.txt. For retrieving the files and saving them on the PC, the "^" characters must not be included in the filenames.

Solution:

This problem is corrected in this release.

4.6.2 FTP client copies multiple versions of a file and places them in reverse order

Problem:

The FTP client copies multiple versions of a file and places them in reverse order.

Solution:

This problem is fixed in this release.

4.6.3 TCPIP$FTP_1 server stops communicating with the FTP child processes

Problem:
When the FTP server limit is reached and no new connections were accepted the TCPIP$FTP_1 server stopped communicating with the FTP child processes on the system. After the limit was reached, the child processes hung waiting on a mailbox. Although, the process rejected the new incoming connections; it appeared that communication was lost with the old processes.

Solution:

This problem is fixed in this release.

4.6.4 FTP server error messages

Problem:
In certain scenarios, the OpenVMS FTP server reports the following error messages:

```
425-Can't build data connection for ...
425 Connect to network object rejected
```

Solution:

This problem is fixed in this release.

4.6.5 Users can still FTP with FTP client disabled

Problem:

Although the FTP client is disabled, users can ftp to another system. Because, FTP is a DCL command, the FTP client image can be invoked even if the FTP client service is shutdown.

Solution:

This problem is corrected in this release.

4.6.6 [VMS]COPY/FTP file with multiple-dot filename does not work

Problem:

On a remote Linux or HP-UX node, if the filename starts with a dot and has multiple dots within the name, for example, .test.001, the filename is truncated. That is, the characters before the second dot are not displayed.

Solution:

This problem is corrected in this release.

4.6.7 Addition of "." to a filename

Problem:

When using `FTP` or `$ COPY /FTP` to transfer files from an OpenVMS system to a UNIX system, the FTP client adds a "." character to a filename without extension.

Solution:

This problem is corrected in this release.

4.6.8 USER command in a session that is already logged in

Problem:

The FTP server, upon receiving a `USER` command in a session that is already logged in, failed to return a proper error, leading to a hang.

Solution:

A message similar to the following is displayed:

```
"503 User SMITH, is already logged in"
```

and the problem is fixed.

4.6.9 Construction of wildcarded filenames

Problem:

The FTP client does not properly construct wildcarded filenames. COPY /FTP TEST.EXE_OLD nodename"username password"::*.EXE creates a file named "_.EXE" on the remote system. Also, COPY /FTP TEST.EXE_OLD nodename"username password"::FILE.* creates a file named "FILE._" on the remote system.

Solution:

The FTP client properly constructs the wildcarded filenames.

4.6.10 "expanded" rooted logical name syntax

Problem:

FTP does not understand the "expanded" rooted logical name syntax.

Solution:

This problem is corrected in this release.

4.6.11 FTP server terminates when there are many connections and disconnections

Problem:

The FTP server terminates with an ACCVIO error when there are many connections and disconnections. The FTP server also displays an error message that is similar to the following:

```
session connection from 127.124.172.114 at 11-JAN-2007 18:42:08.42
 %SYSTEM-F-NOSLOT, no PCB available
 %TCPIP-E-FTP_CREPRC, failed to create a child process
```

Solution:

This problem is corrected in this release.

4.6.12 DIRECTORY /FTP command fails to return failure status

Problem:

The `DIRECTORY /FTP` command fails to return a failure status, even when the target file does not exist.

Solution:

This problem is corrected in this release.

4.6.13 Entries made in TCPIP$ETC:IPNODES.DAT are not read

Problem:

Entries made in the TCPIP$ETC:IPNODES.DAT file are not read by the FTP client.

Solution:

This problem is corrected in this release.

4.6.14 FTP client echoes the keyboard input associated with ACCT

Problem:

The OpenVMS FTP client echoes the keyboard input associated with the Account (ACCT) command. Because, some FTP servers use the "account" as a secondary password, which raised security concerns.

Solution:

This problem is corrected in this release.

4.6.15 GET /FDL and COPY /FTP/FDL commands may fail

Problem:

Because of a non existent owner on the destination system, the `GET /FDL` and `COPY /FTP/FDL` commands may fail. The original owner must be omitted or ignored.

Solution:

This problem is corrected in this release.

4.6.16 Passive mode on a multihomed system

Problem:

When using passive mode on a multihomed system, the FTP client fails to ensure that the source IP address for the data connection matches the IP address used for the control connection. Many FTP servers reject such connections for security reasons.

Solution:

This problem is corrected in this release.

4.6.17 Sends the incorrect file version

Problem:

The FTP server sends the incorrect file version in the 150 info message to the FTP client.

Solution:

This problem is corrected in this release.

4.6.18 Display of files residing on second and subsequent disks

Problem:

When a `DIRECTORY` command is executed on a search list pointed to by a concealed logical, the list contains information about files only on the first disk and fails to display the files residing on second and subsequent disks.

Solution:

This problem is corrected in this release.

4.6.19 Transferring files greater than 2GB

Problem:

While transferring huge files, greater than 2GB, from a disk, all the other operations on this disk will hang until the transfer of file is accomplished.

Solution:

This problem is corrected in this release.

4.7 IMAP problems fixed in this release

The following sections describe IMAP problems fixed in this release.

4.7.1 IMAP server allows potential attackers

Problem:
IMAP server allows potential attackers with unlimited guess of username and password combinations.

Solution:

This problem is fixed in this release.

4.7.2 Listing of more than hundred empty folders fails

Problem:

The IMAP server crashes while listing more than hundred empty folders.

Solution:

This problem is corrected in this release.

4.7.3 IMAP server process hang in the exception handler

Problem:

An IMAP server process may hang in the exception handler.

Solution:

This problem is corrected in this release.

4.8 INETDRIVER problems fixed in this release

The following sections describe INETDRIVER problems fixed in this release.

4.8.1 System crash in the KVCI$$GENERATE_ASSOC_ID routine

Problem:

Users of the SRI QIO interface (INETDRIVER) experience a system crash with INVEXCEPTN in the KVCI$$GENERATE_ASSOC_ID routine.

Solution:

This problem is corrected in this release.

4.9 IPC (socket library) problems fixed in this release

The following sections describe IPC (socket library) problems fixed in this release.

4.9.1 TCPIP$INETACP process uses 100% CPU

Problem:
In a multithreaded customer application in which thousands of threads call select( ), TCPIP$INETACP process uses 100% CPU.

Solution:

This problem is fixed in this release.

4.9.2 Alignment faults in TCPIP$ACCESS_SHR.EXE image

Problem:
Alignment faults are observed in TCPIP$ACCESS_SHR.EXE image. The most common PC range is below:
TCPIP$ACCESS_SHR + 54230
TCPIP$ACCESS_SHR + 54264

Solution:

This problem is fixed in this release.

4.9.3 Definitions for TCP socket

Problem:

Some of the "definitions" are not available for certain TCP socket options in SYS$SHARE:TCPIP$INETDEF.*.

Solution:

The following definitions are added with this release of TCP/IP:

```
       #DEFINE INET$C_TCP_TSOPTENA 16  /* time stamp option */
#DEFINE INET$C_TCP_PAWS 32      /* PAWS option       */
#DEFINE INET$C_TCP_SACKENA 64   /* SACK enabled      */
```

Counterparts with the TCPIP$ prefix used instead of the INET$ prefix are also added.

4.9.4 getnameinfo( ) returns "unknown name or service" error

Problem:

The `getnameinfo( )` function returns an `unknown name or service` error if the specified address is not found. The RFC defines that `getnameinfo( )` must return the address. The routine also fails to honor the NI_NAMEREQD or NI_NOFQDN flags in all cases.

Solution:

This problem is corrected in this release.

4.9.5 freeaddrinfo( ) causes an ACCVIO

Problem:

`freeaddrinfo( )` causes an ACCVIO condition when a NULL pointer is passed for `freeaddrinfo( )`.

Solution:

This problem is corrected in this release.

4.9.6 IPv6 address queried before IPv4 address

Problem:

The BIND9 Resolver sends queries for IPv6 addresses before querying for IPv4 addresses, even when no local IPv6 addresses are configured.

Solution:

This problem is corrected in this release.

4.9.7 BIND9 Resolver flags for getaddrinfo are inadvertently shifted

Problem:

The BIND9 Resolver AI_ALL and AI_V4MAPPED flags for `getaddrinfo` are inadvertently shifted, preventing the IPv6 application build against the previous versions of TCPIP from working on TCPIP V5.6.

Solution:

Because the previous flag values are restored, some IPv6 applications built for the original TCPIP V5.6 release will no longer function correctly following the installation of this kit.

The relevant header file is `netdb.h`. Application developers having trouble with these flags must ensure that they are using a "netdb.h" file with the old (and recently restored) values.

4.9.8 Delay when communicating between socket pair

Problem:

The `socketpair( )` call returns a pair of TCP sockets, which are connected through a localhost ephemeral port numbers. When communicating between this socket pair, a 200ms delay is encountered while receiving and acknowledging the data.

Solution:

This problem is corrected in this release.

4.9.9 Alignment faults in gethostbyname( )

Problem:

Alignment faults are detected in the `gethostbyname( )` call and friends.

Solution:

This problem is corrected in this release.

4.9.10 Documentation for getaddrinfo() and gai_strerror() - EAI_BADHINTS

Problem:

Along with the other `getaddrinfo( )` error codes documented in the *HP TCP/IP Services for OpenVMS Sockets API and System Services Programming* guide, `getaddrinfo( )` may also return:

```
EAI_BADHINTS    "Invalid value for hints"
```

This error is returned if the `hints` parameter in the call to `getaddrinfo( )` is not correctly initialized.

Solution:

This problem is corrected in this release.

4.10 Load Broker problems fixed in this release

The following section describes Load Broker problems fixed in this release.

4.10.1 Load Broker memory leak

Problem:

If you are running several OpenVMS Clusters and using several dynamic cluster aliases for balancing the workload across the cluster members with each load broker maintaining 10 cluster aliases, after few days of operation the load broker dies with the %SYSTEM-F-OPCCUS error.

Solution:

This problem is corrected in this release.

4.11 LPD problems fixed in this release

The following sections describe LPD problems fixed in this release.

4.11.1 Incorrect job status in the mail message

Problem:

LPD printing with the `/PARAMETERS=MAIL` qualifier includes an incorrect job status in the resulting mail message.

Solution:

This problem is corrected in this release.

4.11.2 Printing to an LPD queue with a large setup module is inefficient

Problem:

Printing to an LPD queue with a large (over 1024 characters) setup module is inefficient. Although, correct output is printed, the logfile shows that for each job, there is a series of attempts to read the setup module into increasingly large buffers.

Solution:

A new configuration parameter, "Setup-Buffer-Size", in the TCPIP$LPD.CONF file allows the system manager to specify the initial setup module buffer size. The default value is 1024 bytes.

4.11.3 "TCPIP-E-LPD_REQREJECT" message displayed multiple times

Problem:

The `TCPIP-E-LPD_REQREJECT` message is displayed many times when attempting to deliver LPD jobs to a printer that is not in service.

Solution:

This problem is corrected in this release.

4.11.4 Latent coding defect within the LPD symbiont

Problem:

A latent coding defect within the LPD symbiont led the symbiont to exit with an ACCVIO error after the VMS83A_RMS V8.0 (or later) patch was installed on an OpenVMS 8.3 Alpha system.

Solution:

LPD users should install the latest TCP/IP kit along with the RMS V8.0 or V9.0 patch.

4.12 Management Utilities problems fixed in this release

The following sections describe Management Utilities problems fixed in this release.

4.12.1 TCPIP$CONFIG does not create an alias IP address

Problem:
TCPIP$CONFIG does not create an alias IP address, which is a substring of the primary address. For example, if the primary address is 10.1.1.100, then it is not possible to add an alias address 10.1.1.10.

Solution:

This problem is fixed in this release.

4.12.2 Large number of packets are sent when using the flood functionality

Problem:
In some instances, a large number of packets are sent, when using the flood functionality of the PING utility (-f) in combination with the option for sending fixed number of packets(-c).

Solution:

This problem is fixed in this release.

4.12.3 netstat -i fails to display the network names correctly

Problem:

`netstat -i` fails to display the network names correctly.

Solution:

This problem is corrected in this release.

4.12.4 Misleading and unsightly error message when the BIND resolver is not enabled

Problem:

Attempting to use the "dig" utility results in a misleading and unsightly error message when the BIND resolver is not enabled.

Solution:

This problem is corrected in this release.

4.12.5 TCPIP$CONFIG.COM fails to see devices

Problem:

TCPIP$CONFIG.COM fails to see devices when the controller letter does not begin with "A". For example, if EIB exists but EIA does not, then the EI controller does not appear in the Interface menu.

Solution:

This problem is corrected in this release.

4.12.6 Missing argument for the ip6hoplimit value

Problem:

Executing the `$ IFCONFIG WE0 INET6 IP6HOPLIMIT` command results in an ACCVIO because of the missing argument for the ip6hoplimit value.

Solution:

This problem is corrected in this release.

4.12.7 Errors when executing netstat -z

Problem:

When executing `netstat -z`, the following message is displayed:

```
netstat: -z is not implemented on this operating system
```

Solution:

Netstat will now zero the counters. In addition, if you attempt to use the `-z` option without privileges, netstat will no longer attempt to display the counters, but rather displays the following message:

```
netstat: must be root to zero counters
```

4.13 NET (Kernel) problems fixed in this release

The following sections describe NET (Kernel) problems fixed in this release.

4.13.1 TCP/IP routine that services I/O CANCEL and DEASSIGN requests does not restore the entry IPL

Problem:
Some processes, such as CIMSERVER, were found hanging in the RWINS state. This happened because the TCP/IP routine that services I/O CANCEL and DEASSIGN for the BG devices was not restoring the Interrupt Priority Level (IPL) to the entry IPL before returning.

Solution:

The entry IPL is now saved on the stack at the beginning and restored from the stack before returning.

4.13.2 Entering the username and password in binary mode

Problem:
When a user enters ((Ctrl+U) and username) followed by ((Ctrl+U) and password) to the telnet server in binary mode, the user authorization fails.

Note

A new logical TCPIP$TELNET_BINARY_IGNORE is defined, which when enabled on binary negotiation, will not set the TT$M_PASSALL bit in the terminal characteristics.

Solution:

This problem is fixed in this release.

4.13.3 TELNET server does not accept new connections

Problem:
Occasionally, the TELNET server does not accept new connections whereas other services such as FTP and SSH appear to accept new connections.

Solution:

This problem is fixed in this release.

4.13.4 RLogin fails

Problem:

Rlogin to a remote system crashes and displays the following message:

```
SSRVEXCEPT, Unexpected system service exception
```

Solution:

This problem is corrected in this release.

4.13.5 Corruption of non-paged pool

Problem:

Various system crashes are reported, involving corruption of non-paged pool.

Solution:

This problem is corrected in this release.

4.13.6 SACK retransmission transmits more data

Problem:

SACK retransmission resulted in too much data being retransmitted; that is, it retransmitted beyond the SACK Left Edge, SLE.

Solution:

This problem is corrected in this release.

4.13.7 Fail to sense SHARE and FULL_DUPLEX_CLOSE

Problem:

While it was possible to set the socket options, it is not possible to sense SHARE and FULL_DUPLEX_CLOSE.

Solution:

This problem is corrected in this release.

4.13.8 System crash after failing to start TCPIP

Problem:

The system crashes after a mysterious failure to start TCPIP, displaying the `SPLIPLHIGH` error.

Solution:

This problem is corrected in this release.

4.13.9 Setting the inet sysconfig parameter may cause a crash

Problem:

Setting the inet sysconfig parameter, `ovms_printf_to_opcom` may cause a crash at TCPIP start, on any version of the scaling kernel. The crash happens if the startup code attempts to print something, for example:

```
sysconfigtab: attribute sobacklog_hiwat in subsystem socket
can't be configured
```

Solution:

This problem is corrected in this release.

4.13.10 System crash because of coded bugcheck in m_copym( )

Problem:

A system crash occurs due to a coded bugcheck in the `m_copym( )`routine because an unexpected negative offset is calculated during selective acknowledgement (SACK) processing.

Solution:

This problem is corrected in this release.

4.13.11 System crash while processing select()

Problem:

A system crash within the TCPIP$INTERNET_SERVICES execlet occurs while processing a `select( )` call.

Solution:

This problem is corrected in this release.

4.13.12 System crash during Packet loss and SACK processing

Problem:

The system occasionally crashed or created an ACK storm during some circumstances involving packet loss and SACK processing.

Solution:

This problem is corrected in this release.

4.13.13 Impossible to disable error message display

Problem:

It is not possible to disable certain error messages displayed via OPCOM or directly to the operator console.

Solution:

Messages such as the following:

```
arp: local IP address nn.nn.nn.nn in use by
hardware address mm-mm-mm-mm-mm-mm
```

can now be displayed in the following ways:

```
$ sysconfig -r inet ovms_printf_to_opcom=1 ! On OPCOM
$ sysconfig -r inet ovms_printf_to_opcom=0 ! On OPA0:
$ sysconfig -r inet log_open=1   ! No display
```

In the future, the final setting may send messages to the SYSLOG facility if and when it is implemented.

4.13.14 System crash during a select() operation

Problem:

The system crashes during a `select( )` operation, or immediately after the operation is complete.

Solution:

This problem is corrected in this release.

4.13.15 Debug code to verify MBAG free list

Problem:

Add debug code to verify MBAG free list during `get` and `free`.

Solution:

This problem is corrected in this release.

4.13.16 Process in RWAST state during process rundown

Problem:

The Process goes into RWAST state during process rundown.

Solution:

This problem is corrected in this release.

4.13.17 use of select() results in a non-paged pool memory leak

Problem:

Under certain conditions, use of the `select( )` function results in a non-paged pool memory leak.

Solution:

This problem is corrected in this release.

4.13.18 Issuing process in the RWAST state

Problem:

A `select( )` operation with certain parameters can cause the issuing process to enter the RWAST state.

Solution:

This problem is corrected in this release.

4.13.19 Multicast traffic can be lost

Problem:

Multicast traffic can be lost when aggressive IGMP snooping is enabled on a switch. This is the result of OpenVMS delaying IGMP reports when the IGMP query specified a maximum response time less than 10 seconds.

Solution:

This problem is corrected in this release.

4.13.20 Extensive use of Out Of Band data can cause system crash

Problem:

Extensive use of Out Of Band data by applications can trigger a system crash at offset PANIC_C+00330 (On V5.6-9, Integrity servers).

Solution:

This problem is corrected in this release.

4.13.21 INETACP process experiences a deadlock

Problem:

The INETACP process experiences a deadlock, frequently stuck in the RWAST state. The internal AQB (work queue) would be non-empty, with perhaps hundreds of outstanding requests.

Solution:

This problem is corrected in this release.

4.13.22 TCPIP$INETACP process attempts to write an error message may result in hang

Problem:

When the TCPIP$INETACP process attempts to write an error message, when the socket send buffer is full, may result in hang.

Solution:

This problem is corrected in this release.

4.13.23 Processing of badly formed SACK packets

Problem:

A system crash with INCONSTATE status can occur during processing of badly formed SACK packets.

Solution:

This problem is corrected in this release.

4.13.24 TCPIP START ROUTING fails to start a dynamic routing process

Problem:

On OpenVMS Integrity systems, the `TCPIP START ROUTING` command fails to actually start a dynamic routing process (ROUTED or GATED).

Solution:

This problem is corrected in this release.

4.13.25 ICMP6 timeouts occurring frequently

Problem:

ICMP6 timeouts may occur more frequently than the required 500ms and 200ms.

Solution:

This problem is corrected in this release.

4.13.26 System crash with PGFIPLHI status

Problem:

A system crash occurs with PGFIPLHI status, with a PC of INET_SENSE_ SOCKET_COUNTERS_C+004A8 (on A56-ECO2).

Solution:

This problem is corrected in this release.

4.13.27 Service limits for NOLISTEN services

Problem:

Service limits for NOLISTEN services are not strictly enforced.

Solution:

This problem is corrected in this release.

4.13.28 MBUF leak (type MT_CONTROL)

Problem:

An MBUF leak (type MT_CONTROL) is observed within the kernel.

Solution:

This problem is corrected in this release.

4.13.29 IPv6 Logo testing

Problem:

The following ND6 test cases fail during IPv6 Logo testing:

- 11. Part A: Neighbor Solicitation Origination, Target Address Being Link-local
- 12. Part B: Neighbor Solicitation Origination, Target Address Being Global

4.13.30 INCONSTATE bugcheck

Problem:

An INCONSTATE bugcheck can occur when an application specified invalid parameters on an IO$_READVBLK QIO operation.

Solution:

This problem is corrected in this release.

4.13.31 System crash during restart of the INET driver

Problem:

System crashes during restart of the INET driver. This is because the INETDRIVER is sending a request to open a kernel VCI port after the kernel had shutdown.

Solution:

This problem is corrected in this release.

4.13.32 System crash when an application does a select() call

Problem:

Various identical system crashes are reported when an application does a `select( )` call.

Solution:

This problem is corrected in this release.

4.13.33 QIO based hostname lookup takes longer time

Problem:

QIO based hostname lookup takes longer than the intended 1 second when multiple pathnames or servers are configured on the bind resolver.

Solution:

This problem is corrected in this release.

4.14 NFS Client problems fixed in this release

The following sections describe NFS client problems fixed in this release.

4.14.1 TCPIP DISMOUNT/ALL command does not dismount DNFS devices

Problem:
TCPIP DISMOUNT/ALL command does not dismount DNFS devices with units greater than or equal to 32767.

In addition to this, these mounted DNFS devices are not displayed when you execute the TCPIP SHOW MOUNT command.

Solution:

This problem is fixed in this release.

4.14.2 Mounting NFS exported shares requires CMKRNL privileges

Problem:
Mounting NFS exported shares requires CMKRNL privileges.

Solution:

This problem is fixed in this release.

4.14.3 System crash with PGFIPLHI

Problem:

When using the NFS client, the system crashes with PGFIPLHI, Pagefault with IPL too high, or INVEXCEPTN, Exception while above ASTDEL.

Solution:

This problem is corrected in this release.

4.14.4 Mounting large disks

Problem:

NFS client can mount very large disks, but when `SHOW DEVICE/FULL` is executed on the NFS disk, it fails to show the total number of blocks and displays illegal logical block number error.

Solution:

This problem is corrected in this release.

4.15 NFS Server problems fixed in this release

The following sections describe NFS server problems fixed in this release.

4.15.1 INVEXCEPTN bugchecks occur at OPENVMS_BFS_GETATTR_VMS

Problem:
INVEXCEPTN bugchecks occur at OPENVMS_BFS_GETATTR_VMS when REMQUEQ operation was done. These bugchecks occur at different PCs.

Solution:

This problem is fixed in this release.

4.15.2 Creating and renaming directory names with special characters

Problem:
NFS Server cannot handle requests for creating and renaming directory names with special characters. The NFS server reports the following error:

```
File not found
```

Solution:

This problem is fixed in this release.

4.15.3 Access violation in the BFS filesystems

Problem:
The NFS server process fails to restart after access violation occurred in the BFS file systems.

Solution:

This problem is fixed in this release.

4.15.4 Creating a directory with special character

Problem:

When the NFS client requests the NFS server to create a directory with one or more special characters (For example, "New Folder", where, " ", space in the directory name is the special character) and requests the server to rename the new directory, NFS server fails to open the directory and displays `File not found`.

Solution:

This problem is corrected in this release.

4.15.5 INVEXCEPTN bugcheck in INSQUE and REMQUE PAL instruction

Problem:

An INVEXCEPTN bugcheck occurs in TCPIP$NFS_SERVICES:REMQUE and INSQUE PAL instruction called from different BFS routines, namely OPENVMS_BFS_READ_VMS, OPENVMS_BFS_CLOSE. This can also occur with other BFS routines.

Solution:

This problem is corrected in this release.

4.15.6 LOCKD temporary files are not removed

Problem:

LOCKD temporary files are not being removed from SYS$SYSDEVICE:[TCPIP$NFSLCK] after they are no longer needed. The files are named LOCKDxxxxPID.;1 where xxxx was a unique series of letters and PID is the pid for the process. The files are zero blocks in size.

Solution:

This problem is corrected in this release.

4.15.7 Unaligned reference fault

Problem:

While using the NFS server, system crashes with the following message: `INVEXCEPTN, Exception while above ASTDEL` Exception is an "Unaligned Reference Fault" for an address that is inside an NFS KPB thread stack. The exception address is inside the "EFI/PAL/SAL Memory" region (see the SDA CLUE SHOW MEMORY /LAYOUT command).

Solution:

This problem is corrected in this release.

4.15.8 Fails to trigger a defined exception handler

Problem:

The NFS server fails to trigger a defined exception handler.

Solution:

This problem is corrected in this release.

4.15.9 INVEXCEPTN bugcheck at the OPENVMS_BFS_GETATTR_VMS line

Problem:

An INVEXCEPTN bugcheck occurs at OPENVMS_BFS_GETATTR_VMS line 87591: REMQUEQ from PSPEC$A_NFS_USER_BLOCKS[0]. Other PC's are also possible.

Solution:

This problem is corrected in this release.

4.15.10 LOCKD process crashes with an ACCVIO error

Problem:

The LOCKD process crashes with an ACCVIO error.

Solution:

This problem is corrected in this release.

4.15.11 Files with names that contain an odd number of bytes are not created

Problem:

The NFS server fails to create files with names that contain an odd number of bytes. For example, "a.t", "aaa.t", and "aaaaa.t". The server returns ENOENT.

Solution:

This problem is corrected in this release.

4.16 NTP problems fixed in this release

The following sections describe NTP problems fixed in this release.

4.16.1 Stack buffer overflow in NTPQ

Problem:
A stack buffer overflow problem exists in the NTPQ program.

Solution:

This problem is fixed in this release.

4.16.2 Displays the "keyid" as optional

Problem:

NTPDC incorrectly displays the "keyid" as optional in the usage and help statements.

Solution:

A related correction applies to the *HP TCP/IP Services for OpenVMS Management Command Reference*, Section 13.8.3.3, NTPDC Request Commands: For the broadcast bullet only: change "[prefer]" to "[minpoll]".

4.16.3 NTP fails to synchronize during the repeated hour

Problem:

NTP does not synchronize during the repeated hour at the summer to winter time change.

Solution:

This problem is corrected in this release.

4.17 POP problems fixed in this release

The following section describes POP problems fixed in this release.

4.17.1 POP allows potential attackers

Problem:

POP allows potential attackers with unlimited username or password guesses.

Solution:

This problem is corrected in this release.

4.17.2 Version number on POP's "XTND STATS"

Problem:

On OpenVMS Integrity servers, the version number on POP's `XTND STATS` command was fixed at compile time, rather than being based upon the image ident of the POP server.

Solution:

This problem is corrected in this release.

4.18 PWIP problems fixed in this release

The following section describes PWIP problems fixed in this release.

4.18.1 System crash during PWIP shutdown

Problem:

A system crash occurs during PWIP shutdown and displays the following error message:

```
DECNET, DECnet detected a fatal error.
```

Solution:

This problem is corrected in this release.

4.18.2 Bulk data transfer performance

Problem:

Bulk data transfer (such as file copy) performance across a PWIP connection (such as DECnet over IP) is slow compared to FTP, over certain types of networks. There is no way to increase the TCP window size for such a connection.

Solution:

The following TCPIP logical names are included:

- TCPIP$PWIP_TCPRCVBUF - Receive socket buffer size
- TCPIP$PWIP_TCPSNDBUF - Send socket size

The logicals must be defined system-wide prior to starting PWIP. If not defined, the default behavior remains unchanged.

4.19 SMTP problems fixed in this release

The following section describes SMTP problems fixed in this release.

4.19.1 Anti spam for unresolvable-domains and unqualified-senders

Problem:
TCPIP SMTP antispam works correctly for:
- Accept-Unresolvable-Domains: FALSE
- Accept-Unqualified-Senders: FALSE

But, if on the BIND server, a MX wildcard record of type [*.ind.hp.com. IN MX 10 munar] with munar having a "A" record defined, anti spam for Unresolvable-Domains and Unqualified-Senders stops working.

Removing the *.ind.hp.com MX record makes the system to work as expected, that is, the system refuses the mail with unresolvable domain.

Solution:

This problem is fixed in this release.

4.19.2 SMTP fails to receive mails

Problem:

Although, the mails sent to the local or remote host (not running TCPIP 5.7) work, SMTP fails to receive mails sent from a remote host. On replying back to a mail sent from a TCPIP 5.7 system, the mail bounces.

Solution:

This problem is corrected in this release.

4.19.3 Large number of recipients in the TO field

Problem:

Having a large number of recipients in the TO field of an arriving SMTP message could lead to corrupt header lines.

Solution:

This problem is corrected in this release.

4.19.4 VMS MAIL does not support lines longer than 255 characters and mixed case headers

Problem:

- VMS MAIL does not support lines longer than 255 characters. Long header lines are becoming increasingly common in the modern Internet. While fetching such messages, the IMAP server may return some headers in the body part of the mail, causing it to appear corrupted to the client.
- IMAP has trouble fetching mails with lowercase or mixed case RFC headers.

Solution:

This problem is corrected in this release.

4.19.5 SMTP server fails to deliver mail

Problem:

The SMTP server fails to deliver mail when the domain name is a combination of letters and numbers. As per RFC, the domain name can be any combination of numbers and letters.

Solution:

This problem is corrected in this release.

4.19.6 SMTP distribution list filenames fails to form properly

Problem:

SMTP distribution list filenames are not always formed properly, and it is not possible to specify a location other than TCPIP$SMTP_COMMON: to contain *.DIS files.

Solution:

This problem is corrected in this release.

4.19.7 TCPIP$SMTP_FROM logical affects the SMTP Return-Path header

Problem:

The TCPIP$SMTP_FROM logical affects the SMTP Return-Path header when defined. The Return-Path must reflect the contents of the logical name, as it did prior to TCPIP V5.6, with no need to encapsulate the value within angle brackets.

Solution:

This problem is corrected in this release.

4.19.8 Adding Persistent-Server displays an error message

Problem:

When you add the "Persistent-Server" field in the TCPIP$SMTP.CONF file and restart SMTP, TCP/IP displays the following error:

```
unknown configuration field; Persistent-Server has been ignored.
```

Solution:

This problem is corrected in this release.

4.20 SNMP problems fixed in this release

The following section describes SNMP problems fixed in this release.

4.20.1 SNMP displays "HrProcessorLoad" as always zero

Problem:
For OpenVMS systems having one CPU, SNMP displays "HrProcessorLoad" as always zero.

Solution:

This problem is fixed in this release.

4.20.2 TCPIP$HR_MIB.EXE memory leaks

Problem:
TCPIP$HR_MIB.EXE has two memory leaks for OIDs hrProcessorFrwID and hrProcessorLoad.

Solution:

This problem is fixed in this release.

4.20.3 Error message not displayed when the specified hostname is invalid

Problem:

An SNMP request, `tcpip$snmp_request` command does not return the error message when the specified hostname is invalid.

Solution:

This problem is corrected in this release.

4.20.4 TCPIP$HR_MIB process dies with an ACCVIO error

Problem:

The TCPIP$HR_MIB process dies with an ACCVIO error.

Solution:

This problem is corrected in this release.

4.20.5 SNMP fails to start with IPv6 disabled

Problem:

SNMP fails to start on a system with IPv6 disabled.

Solution:

This problem is corrected in this release.

4.20.6 TCPIP$HR_MIB process consumes excessive CPU time

Problem:

If the total number of BG or MBA devices exceeds 5000, TCPIP$HR_MIB process consumes excessive CPU time and leads to sluggish performance.

Solution:

A new logical, TCPIP$SNMP_SCAN_ALLDEV, is included. If TCPIP$SNMP_ SCAN_ALLDEV is defined, the entire set of devices will be scanned. If the logical is not defined then only the following devices will be scanned:

- Disk
- Tape
- Communication device
- Terminal
- Line printer
- Work stations
- General audio
- Bus
- General video
- DEC voice products

4.21 SSH, SCP and SFTP problems fixed in this release

The following section describes SSH, SCP and SFTP problems fixed in this release.

4.21.1 Error message is overwritten for "illegal options" provided with ls

Problem:
For illlegal options provided with ls, such as `ls a`, SFTP displays an error message: `Illegal option---a`. The error message is partially overwritten by blank lines and by the next sftp> prompt.

Solution:

This problem is fixed in this release.

4.21.2 SSH server crashes when non-existent username is specified

Problem:
SSH server crashes on login when a non-existent user name is specified at the login prompt.

Solution:

This problem is fixed in this release.

4.21.3 MGET *.<file extension> does not work

Problem:
A MGET *.<file extension> does not work with SFTP server.

Solution:

This problem is fixed in this release.

4.21.4 SCP Copy does not work with filenames with wildcards

Problem:
SCP copy does not work with filenames with wildcards.

Solution:

This problem is fixed in this release.

4.21.5 LS *.TXT fails to display files

Problem:
LS *.TXT fails to display files on SFTP client.

Solution:

This problem is fixed in this release.

4.21.6 SSH idle-timeout counter fails to reset

Problem:
Although the SSH server sends messages to the client within the configured idle-timeout period, the SSH client would still timeout. Hence, the SSH idle-timeout counter would fail to reset if a message was received from the server.

Solution:

This problem is fixed in this release.

4.21.7 SFTP client converts filenames to uppercase

Problem:

On ODS-5 disks, when connecting to a UNIX system using the get command, the SFTP client converts filenames to uppercase.

Solution:

This problem is corrected in this release.

4.21.8 SFTP "PUT" command fails on Windows server

Problem:

When copying a file using the PUT command from an OpenVMS to a Windows 2003 PC using WS_FTP Server 7.1 from IPSWITCH.COM, SSH_FILEXFER_ATTR_PERMISSIONS error is returned. A file header is created, but no data is placed in the file. Both binary transfers and ascii stream_lf transfers fail.

Solution:

This problem is corrected in this release.

4.21.9 SFTP "CD SYS$LOGIN" fails

Problem:

In an SFTP from an OpenVMS system, the user cannot navigate to the home directory using "cd sys$login" or "cd /" or "cd ~". When such an operation is attempted, the user is either directed to a wrong directory (which in most cases is the ssh's home directory) in case of a privileged user or gets a "CD FAILED" error in case of an unprivileged user.

Solution:

This problem is corrected in this release.

4.21.10 SFTP process becomes CPU-bound when using CHROOT

Problem:

SFTP process becomes CPU bound when using CHROOT. If most of the SFTP processes become CPU-bound, it can render the OpenVMS system unusable with Denial of Service.

Solution:

This problem is corrected in this release.

4.21.11 ls * .txt does not display the list of files

Problem:

The `ls * .txt` command in SFTP command fails to display the list of files in the current working directory and exits with an ACCVIO.

Solution:

This problem is corrected in this release.

4.21.12 Copy fails with wildcard (*) character

Problem:

SCP copy fails when the command is entered with wildcard (*) character. The copy command also fails when entered with percentage sign (%).

Solution:

This problem is corrected in this release.

4.21.13 ACCVIO on non-existent user

Problem:

The SSH server fails with an ACCVIO on non-existent user.

Solution:

This problem is corrected in this release.

4.21.14 mget *.lis does not work

Problem:

In an SFTP session, the `mget *.lis` command fails to work.

Solution:

This problem is corrected in this release.

4.21.15 ls -l fails to work

Problem:

The `ls -l` command in SFTP does not work.

Solution:

This problem is corrected in this release.

4.21.16 ACCVIO if identifier not the same as the username

Problem:

An ACCVIO error occurs in the SSH client if the identifier name for the current UIC is not the same as the username.

Solution:

To keep compatibility with older versions, the logical name, TCPIP$SSH_ALLOW_IDENT_MISMATCH must be assigned in the system table to enable the new behavior. If not assigned, or if assigned with numeric value 0, the code behaves as in previous versions.

4.21.17 Wildcard ("*") processing on "ls"

Problem:

Within SFTP, wildcard ("*") processing does not work properly on `ls` or, if the target file already exists, on `mget`.

Solution:

This problem is corrected in this release.

4.21.18 Entering an extra <CR>

Problem:

Within SFTP, it is necessary to enter an extra <CR> after pressing <CTRL/Z>, <CTRL/Y>, or <CTRL/C>. Also, display of the resulting messages such as "** Interrupt **" is not consistent with other TCPIP components, nor with longstanding VMS usage.

Solution:

A new logical name, TCPIP$SSH_SFTP_SUPPRESS_EXIT_MESSAGES, is available to suppress display of the following messages:

```
- CTRL/Z -> ** Exit **
- CTRL/Y -> ** Interrupt **
- CTRL/C -> ** Cancel **
```

It is effective if the logical name is defined at the system level (/SYSTEM) with any value except 0.

4.21.19 SSH access to an account with an expired password and a PWDLIFETIME of 0

Problem:

SSH access to an account with an expired password and a PWDLIFETIME of 0 still requires a password change, unlike TELNET or SET HOST.

Solution:

This problem is corrected in this release.

4.21.20 put *.*;* may not work

Problem:

The SFTP command, `put *.*;*` fails with an ACCVIO error.

Solution:

This problem is corrected in this release.

4.21.21 Ability to navigate to subdirectories has regressed

Problem:

From a PC SFTP client, specifically the one from SSH Inc., the ability to navigate to subdirectories has regressed from a previous fix.

Solution:

This problem is corrected in this release.

4.21.22 ls -r fails with an error

Problem:

In SFTP, an `ls -r` command fails with an error and does not display any files in the subdirectories.

Solution:

This problem is corrected in this release.

4.21.23 Transferring larger files

Problem:

Using SCP or SFTP to transfer a file larger than 2 GB results in a corrupt file.

Solution:

This problem is corrected in this release.

4.21.24 ls command fails to list ODS-5 extended filenames

Problem:

In SFTP, output from an `ls` command fails to list ODS-5 extended filenames.

Solution:

This problem is corrected in this release.

4.21.25 Error returned by the stat() function during a "get" operation

Problem:

Although, the files are in a subdirectory of the current source with recursion disabled, SFTP complains about an error returned by the `stat()` function during a `get` operation.

Solution:

This problem is corrected in this release.

4.21.26 SSH server enforces an idle session timeout value

Problem:

The SSH server enforces an idle session timeout value because of the following issues:

- The actual idle timeout is about 10% greater than the configured IdleTimeOut value.
- Activity from the client after approximately 90% of the IdleTimeOut duration is not counted; the session is cut off anyway.

Solution:

A new logical name, TCPIP$SSH_SHIFT_IDLE_TIMEOUT, when defined with anything other than "0" causes a shifting of the window of actual enforced timeout values. Rather than allowing an idle user a grace period of up to 10% of the configured IdleTimeOut, the timeout will actually be enforced at some time between 95% and 105% of that value.

4.21.27 ACCVIO error during password validation

Problem:

An ACCVIO error occurs in SSH during password validation.

Solution:

This problem is corrected in this release.

4.21.28 Issues related to the password change

Problem:

Following are the issues related to the password change feature in SSH:

- The old password sent by a client is ignored by the OpenVMS SSH server.
- The OpenVMS client never prompts the user for an old password.

Solution:

On the SSH server, if the value for pwdlifetime for a user account in the SYSUAF is 0 (none), the user at the client is not prompted to update his password even if it has expired. This is an OpenVMS feature, not specific to SSH.

For the password update feature to work, the appropriate value in SSHD2_ CONFIG. must be set to "yes" (without the quotation marks).

```
Client is VMS:
AllowVmsLoginWithExpiredPw (default is yes)
       Client is not VMS:
       AllowNonvmsLoginWithExpiredPw (default is no)
```

For some clients, if the value of AllowedAuthentications in SSHD2_CONFIG. is set to password only, the following situation may occur for the user at the client:

- Client prompts for the account password.
- User enters the correct password.
- The password has expired; client prompts user to re-enter the old and new passwords.
- The user enters an incorrect old password.
- Client now re-prompts the user to enter a password, as described in step a. However, when the user enters the correct password, step c does not occur. Instead, step e is repeated.
- Eventually, the login attempt fails.

This behavior does not occur with the OpenVMS client.

There is a new logical name: To enable prompting for old password in the OpenVMS SSH client when updating an expired password, use the following command:

```
$ DEFINE /SYSTEM TCPIP$SSH_NUM_OLD_PASSWORD_CHECKS n
```

Where; "n" is the number of guesses that the client is to be allowed for the old password. You should make this value less than or equal to the value of the variable PasswordGuesses in the server configuration file SSHD2_CONFIG. A separate mechanism is required to define the value for the client since it does not have access to SSHD2_CONFIG., but only to SSH2_CONFIG.
To make this value permanent across reboots, include the command in the system startup procedure.
Note that if n = 0 or "0", or if the logical is not defined, the SSH client will not prompt for the old password.

4.21.29 Error message appears at the conclusion of a copy operation

Problem:

When using SCP to copy a file to a remote non-OpenVMS server, the error message, `got EOF reading file` sometimes appears at the conclusion of copy operation, which is otherwise a successful operation.

Solution:

This problem is corrected in this release.

4.21.30 -r command does not work as expected

Problem:

The `scp -r` command does not work as expected.

Solution:

The -r option is intended to be used when the source path specifies a directory, not including filename(s). Copy of files where filename is specified does not require use of the -r option.

Note, however, that when a filename is specified, even if it is in a subdirectory of the current default, the file is copied to the target default. When a directory name is used as the source and -r is specified, the directory tree is reproduced on the target system.

The fix for this case enables the OpenVMS SCP client to handle directory levels more than one deep when the -r option is used. As before, recursive copy is not supported for the SFTP client.

Also, recursive copy with filenames not specified preserves the version number of the source file. This behavior means that when the target of a put command is also an OpenVMS system, the file will not be copied if that version already exists. An error message, similar to the following is displayed:

```
        tcpip$ssh_scp2.exe:
warning: open: ./testroot/AFILE.TXT;1 (dst):
unspecified failure (server msg: 'syserr: bad file
number, file: ./testroot/AFILE.TXT;1')
```

4.21.31 Directory logical names gets translated on the client

Problem:

In SFTP and SCP, directory logical names gets translated on the client system instead of being passed to the server.

Solution:

Logical names entered through the SCP and SFTP clients should be translated on the server system. For example, if the client and server systems have a different translation for the same system-wide logical name, the one on the server should be used. Note that because the SFTP server does not execute the SYS$SYLOGIN command procedure, some logical names available in interactive sessions are not available, e.g., SYS$LOGIN.

If a user does not have access to the directory referenced by a logical name (e.g., TCPIP$SSH_HOME for a non-privileged account), a cdin SFTP will fail, as expected.

Also note that from a non-OpenVMS client, no attempt is made to translate a string as a logical name; behavior depends on the client. For example, from a Red Hat Linux system:

```
sftp> cd name
(no leading slash before "name") results in an attempt to move
to the [.name] subdirectory of the current default location.
sftp> cd /name
results in an attempt to go to a device "name", with no
directory specified, which fails.

Current default: dev1:[user1]; dev1:[user2] does not exist:

sftp> cd dirname
sftp> pwd
Remote working directory: /DEV1/user1/dirname

sftp> cd /dev1
Couldn't canonicalise: No such file or directory
```

```
sftp> cd /dev1/user1
sftp> pwd
Remote working directory: /dev1/000000/user1

sftp> cd /dev1/user2
Couldn't stat remote file: No such file or directory
```

4.21.32 Miscellaneous Problems

Problem:

- Within SFTP, the `cd ..` command does not work, and `ls *.*;` does not work for directories.
- SFTP behavior is inconsistent for `cd` and `ls` when the target directory did not allow full user access.
- For directories allowing READ+EXECUTE access, the `ls` command sometimes results in an error message along with a display of the appropriate filenames.
- For directories allowing EXECUTE access only, `ls` should not list files, but it did list them (along with an error message). It must list a file only if that specific name is specified by the user.

Solution:

The following are some differences from DCL or FTP behavior and messages:

When an "ls" encounters a file for which attributes are not accessible to the user on the SFTP server, the following text is included in any message displayed: `no privilege for attempted operation`. For example:

```
fcr_readdir_lstat: G-R.TXT;1 (src): no such file
(server msg: 'platform cannot stat() filename: file
does not exist or no privilege for attempted
operation.')
```

Like FTP and DCL, SFTP does not allow a general `ls` (with no filename specified) for a directory on the server to which the user has E (Execute) access only. However, unlike FTP or DCL, SFTP does not work for an `ls` followed by a specific filename in an E access directory.

For certain files, mainly those that do not exist on the server, the following new client-based message is displayed instead of the standard message sent by the server:

```
no such file (client msg: no such file or directory,
or no privilege for attempted operation)
```

4.21.33 SSH server may not complete authentication

Problem:

If the TCPIP$SOCKET_TRACE logical name is defined, the SSH server may not complete authentication and all logins fail.

Solution:

This problem is corrected in this release.

4.21.34 SSH client uses an existing SSH connection for a new SFTP session

Problem:

The SSH server may fail to generate an ACCVIO error when the SSH client uses an existing SSH connection for a new SFTP session.

Solution:

This problem is corrected in this release.

4.21.35 Messages displaying the last interactive and last non-interactive login times are not displayed

Problem:

When logging into OpenVMS with SSH, messages displaying the last interactive and last non-interactive login times are not displayed. Neither a message flags the number of login failures since the last successful login.

Solution:

This problem is corrected in this release.

4.21.36 X application fails authentication

Problem:

X11 chaining with a TCP/IP Services host in the middle of the chain causes the X application to fail authentication. For example, if host1 through host3 are OpenVMS systems:

```
host1> SSH "+X" host2
...snip...
host2> SSH "+X" host3
...snip...
host3> RUN SYS$SYSTEM:DECW$CLOCK
warning: X11 auth data does not match fake data.
XIO: fatal IO error 65535 (network partner disconnected logical
link) on X server "_WSA12:"
```

Solution:

Some clients may attempt keyboard interactive client authentication, which may send a null username string. The new code should handle this situation; in case of errors, the workaround is to change or add the following line in the TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]SSHD2_CONFIG. file:

```
PreserveUserKeyCase no
```

4.21.37 PUT command to Sterling or Tumbleweed software failed with errors

Problem:

SFTP put to servers running Sterling or Tumbleweed software failed with errors such as Operation unsupported or The requested operation cannot be performed because there is a file transfer in progress.

Solution:

This problem is corrected in this release.

4.21.38 Fails to set the last non-interactive login time

Problem:

SFTP sessions does not set the last non-interactive login time in the user's UAF record, which is inconsistent with FTP.

Neither SFTP sessions nor single command mode SSH logins get an SSH-generated USER type accounting record, as do other interactive terminal logins.

Solution:

This problem is corrected in this release.

4.21.39 SSH server could be sent into a tight loop

Problem:

When the Tectia SSH client is used and multiple file transfer windows are open, the SSH server could be sent into a tight loop.

When using a client that multiplexed SFTP sessions over existing SSH connections, each time an SFTP session ended, the SSH server parent process (the process running TCPIP$SSH_SSHD2.EXE) is left with a link to a BG device that no longer exists, a waste of resources for the server process.

Solution:

This problem is corrected in this release.

4.21.40 ListenAddress SSH server configuration field is not supported

Problem:

The ListenAddress SSH server configuration field is not supported on TCP/IP Services for OpenVMS. Instead, the same effect can be achieved by using the command `TCPIP SET SERVICE /ADDRESS`. However, this difference is not obvious to users.

Solution:

A warning message, generated by the SSH server, is added to point the user to that command.

4.21.41 Protections on key files created by SSH_KEYGEN

Problem:

Protections on key files created by the SSH_KEYGEN utility are UNIX-style, not OpenVMS-style. Specifically, they allowed only READ and not EXECUTE access. For example:

```
KEYFILE.;   -- (RWD,RWD,,)
KEYFILE.PUB -- (RWD,RWD,R,R)
```

Solution:

This problem is corrected in this release.

4.21.42 "-e" switch on SSH_KEYGEN does not work

Problem:

The -e switch on the SSH_KEYGEN utility does not work.

Solution:

This problem is corrected in this release.

4.21.43 Password expiry

Problem:

When a password expires and the UAF DisForce_Pwd_Change flag is set, the SSH server does not set the PWD_EXPIRED or PWD2_EXPIRED UAF flag to prevent subsequent user logins not to change their password with SET PASSWORD. This allows circumvention of password expiration as users with expired passwords may not continue to log in.

When logging in with the PWD_EXPIRED or PWD2_EXPIRED UAF flag set, the SSH server does not issue a text warning to the client as they expected from using TELNET and other login methods:

```
Your password has expired; contact your system manager
```

Instead, the SSH server cues three times for password, even if the password is entered correctly, and then disconnects.

Solution:

If a user's account has the DisForce_Pwd_Change UAF flag set, and the user does not change their expired password during password-based login, any subsequent login (including SSH public key) will be rejected until the user's PWD_EXPIRED (or PWD2_EXPIRED) flag is reset by the system administrator.

When logging in with the PWD_EXPIRED or PWD2_EXPIRED UAF flag set, the SSH server now correctly returns the text:

```
Your password has expired; contact your system manager
```

However, some clients do not display the message.

4.21.44 SSH access to Integrity ILO console

Problem:

SSH access to Integrity ILO console results in the following error:

```
warning: Authentication failed.
Disconnected; key exchange or algorithm negotiation
failed (Key exchange failed.)
```

Solution:

This problem is corrected in this release.

4.21.45 Explanatory message back to the client during an attempted password change

Problem:

The SSH server fails to send an explanatory message back to the client during an attempted password change if the chosen password is too short.

Solution:

After a password is entered, a message about the password being too short or in the history list is returned, or if the new password is good, the user is logged in. The value of PasswordGuesses in sshd2_config is not checked for new password entry guesses.

4.21.46 Connecting to AIX OpenSSH server results in an error

Problem:

Connecting from an OpenVMS SSH client to AIX OpenSSH server results in the following error message:

```
Did not receive identification string from n.n.n.n
```

Solution:

The SSH client's modified behavior (sending an SSH protocol version string of "SSH-2.0" rather than "SSH-1.99") applies only when the new TCPIP$SSH_AIX_PATCH logical is defined in the SYSTEM table with a non-zero value.

4.21.47 Log into a non-existent account via SSH may fail

Problem:

An attempt to log into a non-existent account via SSH with password authentication may cause an SSH server ACCVIO.

Solution:

This problem is corrected in this release.

4.21.48 UserLoginLimit is ignored

Problem:

The SSH server configuration parameter UserLoginLimit is ignored.

Solution:

This problem is corrected in this release.

4.21.49 Using X11 forwarding frequently fails

Problem:

When using SSH in single command mode with the TCP/IP Services for OpenVMS SSH server, where the command being issued used X11 forwarding (such as CREATE/TERMINAL/DETACH), the command frequently fails with an error such as `X Toolkit Error: Can't Open display`. A call to WAIT in TCPIP$SSH_RCMD.COM worked around the problem but introduces additional delay.

When interactively logging into the TCP/IP Services for OpenVMS SSH server, every login incurred an unnecessary one second delay.

Solution:

This problem is corrected in this release.

4.21.50 RIGHTSLIST identifier missing displays an ACCVIO error

Problem:

If SSH_KEYGEN is used from an account whose RIGHTSLIST identifier is missing, an ACCVIO is displayed rather than a more graceful error message.

Solution:

This problem is corrected in this release.

4.21.51 Opening multiple interactive login sessions over one SSH TCP connection

Problem:

When an SSH client tries to open multiple interactive login sessions over one SSH TCP connection, the TCP/IP Services for OpenVMS SSH server loops or exits with an error, rather than gracefully rejecting the additional sessions.

Solution:

This problem is corrected in this release.

4.21.52 Rename command for a file with an OpenVMS version number returns an error

Problem:

When an SFTP client user issues a rename command for a file with an OpenVMS version number, an error is returned. The file is not renamed.

Solution:

This problem is corrected in this release.

4.21.53 "password aging" message is not displayed

Problem:

The SSH server does not provide a `password aging` message when the user logs into the system with a nearly expired password.

Solution:

This problem is corrected in this release.

4.21.54 Re-entering the old password as the new password

Problem:

During a forced password change, if the user tries to re-enter the old password as the new one, the SSH server may simply close the connection rather than displaying an error message and allows the user to choose a different password.

Solution:

This problem is corrected in this release.

4.21.55 ACCVIO when the batch mode is used

Problem:

An ACCVIO occurs in the SCP or SFTP client when the batch mode option, `-b` is used from a DCL procedure in a subprocess where SYS$OUTPUT or SYS$INPUT has been re-defined to point to a file.

Solution:

This problem is corrected in this release.

4.21.56 Weak password and system-dictionary checking does not happen

Problem:

During a forced password change, the SSH server does not perform weak password checking or system-dictionary checking on the proposed new password.

Solution:

This problem is corrected in this release.

4.21.57 SSH login via public key authentication may fail

Problem:

Although the expired password is not used, an SSH login via public key authentication may fail, if the target user has the DISFORCE_PWD_CHANGE flag set or improperly set the PWD_EXPIRED or PWD_EXPIRED2 flag.

Solution:

This problem is corrected in this release.

4.21.58 LCD command in SFTP fails with "CD failed"

Problem:

The LCD command in SFTP fails with a `CD failed` error if not connected to a remote SFTP server, although it should have been possible to change the local directory. Also, the CD command returns the same error when an OpenVMS-style directory specification is used while connecting to a non-OpenVMS server.

Solution:

This problem is corrected in this release.

4.21.59 error and command messages to stderr (SYS$ERROR) and stdout (SYS$OUTPUT)

Problem:

The SFTP client fails to properly direct error and command messages to stderr (SYS$ERROR) and stdout (SYS$OUTPUT) as appropriate.

Solution:

This problem is corrected in this release.

4.21.60 Data appears to be truncated on the remote end

Problem:

The SFTP and SCP utilities are not properly "put"ing fixed record format files to non-VMS systems. The data appears to be truncated on the remote end.

Solution:

This problem is corrected in this release.

4.21.61 Spurious debug messages at the end of an SFTP log file

Problem:

Spurious debug messages appear at the end of an SFTP log file.

Solution:

This problem is corrected in this release.

4.21.62 Authentication failure when trying to connect to HP ProLiant iLO mpSSH Server

Problem:

Authentication fails when attempting to use the OpenVMS SSH client to connect to an HP ProLiant iLO mpSSH Server.

Solution:

This problem is corrected in this release.

4.21.63 Only the first 3 IdKeys are processed

Problem:

When using SSH with public key authentication, only the first 3 IdKeys are processed from the IDENTIFICATION file.

Solution:

This problem is corrected in this release.

4.21.64 lcd to logical name specification restrictions

Problem:

- When SFTPed to a UNIX system, lcd to a logical name specification works for the first time, but subsequent attempts to lcd to any logical name may fail.
- When SFTPed to an OpenVMS or UNIX system, lcd to a logical name specification followed by an lcd to a directory specification in OpenVMS syntax (For example, [.tmp]) may fail with the following error:

```
Warning: chdir(/sys$login/./tmp) errno = 2  PWD failed.
```

Solution:

This problem is corrected in this release.

4.21.65 Port forwarding fails if ResolveClientHostName is set to "no"

Problem:

SSH port forwarding fails if the SSHD2_CONFIG. option ResolveClientHostName is set to "no".

Solution:

This problem is corrected in this release.

4.21.66 Transferring large number of files using SFTP

Problem:

Transferring a very large number of files using SFTP can result in a memory allocation error and displays the following error:

```
"Not enough memory"
or
TCPIP-F-SSH_ALLOC_ERROR
```

due to a memory leak.

Solution:

This problem is corrected in this release.

4.21.67 SSH connection requests are handled as NETWORK access

Problem:

All the various types of SSH connection requests (For example, SSH interactive sessions, single command mode, SFTP) are handled as NETWORK access, instead of differentiating by session type.

Solution:

This problem is corrected in this release.

4.21.68 UAF account expiry is not notified

Problem:

If an UAF account has "expired", SSH does not properly notify the user. It also logs an inappropriate intrusion record when a valid but expired password is presented.

Solution:

This problem is corrected in this release.

4.21.69 Characters from extended character set are allowed

Problem:

Although the UAF flag PWDMIX is not set, SSH allows characters from the extended character set to be used when creating a password during an expired password change event.

Solution:

This problem is corrected in this release.

4.21.70 Accessing files via SFTP causes excessive Security alarms

Problem:

Accessing files via SFTP causes excessive Security alarms in the Audit log complaining that EXECUTE access is required for the SYSUAF.DAT file.

Solution:

This problem is corrected in this release.

4.21.71 SYS$ANNOUNCE message displayed after login

Problem:

The SYS$ANNOUNCE message is displayed after login, and display of the SYS$WELCOME message is not implemented.

Solution:

This problem is corrected in this release.

4.21.72 "ls -l" and the "rename" command with wildcards fails

Problem:

Using the SFTP `ls -l` and the `rename` command with wildcards `(*)` fails when the specified name was a directory.

Solution:

This problem is corrected in this release.

4.21.73 Opening a second Tectia SSH client

Problem:

Attempts to open a second Tectia SSH client session may result in both sessions getting disconnected.

Solution:

This problem is corrected in this release.

4.21.74 Server process crashes while listing files

Problem:

The SFTP Server process crashes while listing files, if any one the listed file owner name is equal to greater than the OpenVMS maximum allowable length, that is, 12 characters.

Solution:

This problem is corrected in this release.

4.22 SYSCONFIG problems fixed in this release

The following section describes SYSCONFIG problems fixed in this release.

4.22.1 Sysconfigdb generates incorrect error message

Problem:

The sysconfigdb command generates a `%SYSTEM-F-SSFAIL, system service failure` exception instead of exiting gracefully upon detecting an error.

Solution:

This problem is corrected in this release.

4.23 TCPDUMP problems fixed in this release

The following section describes TCPDUMP problems fixed in this release.

4.23.1 TCPDUMP exits with a success status when invalid arguments are passed

Problem:

Although, invalid command line arguments are passed, TCPDUMP may exit with a success status. It must exit with something more descriptive, such as %SYSTEM-E-ABORT (condition code 42).

Solution:

This problem is corrected in this release.

4.24 TELNET problems fixed in this release

The following section describes TELNET problems fixed in this release.

4.24.1 Arbitrary characters received on the TELNET server

Problem:
Arbitrary characters are received on TELNET server when used in binary mode.

Solution:

This problem is fixed in this release.

4.24.2 Quoted character gets dropped

Problem:

Binary telnet session occasionally drops quoted character.

Solution:

This problem is corrected in this release.

4.24.3 User authorization failure

Problem:

When you establish a telnet session in a binary mode to an OpenVMS vms host by entering Ctrl-U+Username followed by Ctrl-U+password, it results in a user authorization failure.

Solution:

This problem is corrected in this release.

4.24.4 Destination address is not set correctly

Problem:

The destination address associated with an outbound TN device is not always set correctly.

Solution:

This problem is corrected in this release.

4.24.5 Allocating a freshly-created outbound TN device

Problem:

Allocating a freshly-created outbound TN device is not possible because the device is initially marked as mounted. The message `SYSTEM-F-DEVMOUNT, device is already mounted` may result from an attempt to use the DCL ALLOCATE command.

Solution:

This problem is corrected in this release.

4.24.6 "INVEXCEPTN @SMP$ACQUIRE_C + 00034" error displayed

Problem:

The system crashes with the following message:

```
INVEXCEPTN @SMP$ACQUIRE_C + 00034.
```

Solution:

This problem is corrected in this release.

4.24.7 Logins blocked after the seed for TN devices exceeding 9999

Problem:

Further logins are blocked after the seed for TN devices exceeds 9999.

Solution:

This problem is corrected in this release.

4.24.8 TN3270 users receive an error message

Problem:

TN3270 users receive an error message while attempting to load the translation table file.

Solution:

This problem is corrected in this release.

4.24.9 OpenVMS telnet client echoes the password

Problem:

OpenVMS telnet client echoes the password, when you try to login to a Linux busybox telnet server from an OpenVMS system.

Solution:

This problem is corrected in this release.

4.25 TFTP problems fixed in this release

The following section describes TFTP problems fixed in this release.

4.25.1 TFTP server randomly exits in between a file transfer

Problem:

To boot diskless systems, the TFTP server is used to fetch the boot files from the server. When an OpenVMS system tries to boot by first fetching the files from the TFTP server, it works as expected. But when this same operation is performed by multiple systems, random failures are observed in the file transfer.

Solution:

This problem is corrected in this release.

4.26 User Control Program problems fixed in this release

The following section describes User Control Program problems fixed in this release.

4.26.1 Enabling the 128th service using CONFIG ENABLE SERVICE

Problem:
A maximum of 127 new services can be created using `TCPIP> CONFIG ENABLE SERVICE` On enabling the 128th service, the following error message is displayed:

```
%TCPIP-E-CONFIGERROR,   error processing configuration request
%TCPIP-E-TOOMANYSERV, database already has maximum number of
```

Solution:

This problem is fixed in this release.

4.26.2 Entering a long domain name may trigger a failure while configuring TCPIP

Problem:

While executing TCPIP$CONFIG.COM in an attempt to initially configure TCPIP, entering a very long domain name may trigger a failure, making it impossible to configure the system. The underlying cause was a failing `TCPIP SHOW CONFIGURATION COMMUNICATION /OUTPUT=`*`filename`* command, which had an 80-character line length limitation.

Solution:

This problem is corrected in this release.

4.26.3 TCPIP SHOW COMMUNICATION truncates its output

Problem:

The `TCPIP SHOW COMMUNICATION` command truncates its output when the domain name is more than 29 characters long.

Solution:

This problem is corrected in this release.

4.26.4 SET NAME_SERVICE /INITIALIZE /CLUSTER fails to find TCPIP$BIND_RUNNING_*.DAT;*

Problem:

The `SET NAME_SERVICE /INITIALIZE /CLUSTER` command attempts to find the file TCPIP$BIND_RUNNING_*.DAT;* but fails because the semantics of the TCPIP$BIND_COMMON logical name have changed.

Solution:

This problem is corrected in this release.

4.26.5 TCPIP SHOW DEVICE_SOCKET output is not properly formatted

Problem:

When used with the DCL command `PIPE`, the output from a `TCPIP SHOW DEVICE_SOCKET` command is not properly formatted.

Solution:

This problem is corrected in this release.

5
Documentation Update

This chapter describes updates to the information in the TCP/IP Services product documentation.

This information will be supplied in the final release of TCP/IP Services.

5.1 Documentation Not Being Updated for This Release

The following manuals are not updated for TCP/IP Services Version 5.7. Documentation changes planned for these manuals are indicated:

- *TCP/IP Services for OpenVMS Installation and Configuration*
- *TCP/IP Services for OpenVMS Management Guide*
- *TCP/IP Services for OpenVMS Guide to SSH*
- *TCP/IP Services for OpenVMS Concepts and Planning*
- *TCP/IP Services for OpenVMS Management Command Reference*
- *TCP/IP Services for OpenVMS Management Command Quick Reference Card*
- *TCP/IP Services for OpenVMS ONC RPC Programming*
- *TCP/IP Services for OpenVMS Sockets API and System Services Programming*
- *TCP/IP Services for OpenVMS Tuning and Troubleshooting*
- *TCP/IP Services for OpenVMS User's Guide*

5.2 Documentation Errata

The following section describes the documentation updates and errata for TCP/IP documentation set:

- **Point-to-Point Protocol Support**

  The *HP TCP/IP Services for OpenVMS Management* manual specifies that Point-to-Point Protocol (PPP) is supported only on Alpha systems. This feature is now supported on both OpenVMS Integrity servers and Alpha systems.

- **REPLY /ENABLE=NETWORK command**

  In the *HP TCP/IP Services for OpenVMS Management* manual (page 24-13), Section 24.10, Receiving LPR/LPD OPCOM Messages, the following command used to receive the notifications:

```
$ TCPIP SET SERVICE LPD /LOG=option
$ REPLY /ENABLE=OPCOM
```

stands corrected as

```
$ TCPIP SET SERVICE LPD /LOG=option
$ REPLY /ENABLE=NETWORK
```

- **Default value for TCP_KEEPIDLE**

  In the *HP TCP/IP Services for OpenVMS Sockets API and System Services Programming* manual (page A-3) and TCP/IP Help, the /PROBE_IDLE setting corresponds to three different sysconfig parameters: TCP_KEEPINIT, TCP_KEEPINTVL, and TCP_KEEPIDLE. The default value for TCP_KEEPIDLE was mentioned as 75 seconds. The default value for TCP_KEEPIDLE is now increased to 2 hrs, which is on par with the RFC requirement, and the default value for TCP_KEEPINIT and TCP_KEEPINTVL remains same, which is 75 seconds.

- **SSH_KEYGEN -e Command Option Converts OpenSSH-based Public Key to OpenVMS Format**

  If you want to enable public-key authentication on an OpenVMS system by copying the public key generated from a Linux (or other OpenSSH-based) system instead of generating the pair of keys using the OpenVMS ssh-keygen utility, use the `-e` qualifier to convert the public key before you transfer it to the OpenVMS system. OpenSSH-based systems, such as the typical Linux system, use their own file format for SSH keys.

  For example:

  ```
  % ssh_keygen -e -f public-key > openvms-format-public-key
  ```

  The `-e` qualifier has been inadvertently omitted from the *HP TCP/IP Services for OpenVMS Guide to SSH* Section, Using the SSH_KEYGEN Utility (page 46).

A

LPD/LPR Configuration

This appendix illustrates how to configure LPD/LPR jobs from a local host to a remote system.

A.1 Configuring LPD job from local host to the remote system

The print jobs must be submitted from local host, "HOSTA", to the remote system, "HOSTB".

To configure the LPD jobs from a local host to the remote system, where the LPD server is not listening on default port (515), complete the following steps:

1. On "HOSTA", setup the printcap entry for the printer in the TCPIP$PRINTCAP.DAT file as follows:

```
LOOP_BOGUS_P_1|loop_bogus_p_1:\
        :lf=/TCPIP$LPD_ROOT/000000/LOOP_BOGUS_P_1.LOG:\
        :lp=LOOP_BOGUS_P_1:\
        :rm=hostb.hp.com:\
        :rp=bogus_p_1:\
        :rt=1234:\
        :sd=/TCPIP$LPD_ROOT/LOOP_BOGUS_P_1:
```

2. On "HOSTB", configure the LPD receiver to listen on port 1234. Manually define another service database entry that is same as LPD. Use the standard procedure to set and enable the service.

A.2 Configuring LPD job from local host to the remote system over the SSH tunnel

The print jobs are submitted from "HOSTA" to the remote system, "HOSTB". The LPD receiver is running on HOSTB listening to default port or any other configured port. The encrypting SSH tunnel is established between HOSTA's port (`rt`) and HOSTB's port on which the LPD receiver is listening.

To configure LPD jobs from a local host to a remote system over the SSH tunnel, complete the following steps:

1. On "HOSTA", setup the printcap entry for the printer in the TCPIP$PRINTCAP.DAT file as follows:

```
LOOP_BOGUS_P_1|loop_bogus_p_1:\
        :lf=/TCPIP$LPD_ROOT/000000/LOOP_BOGUS_P_1.LOG:\
        :lp=LOOP_BOGUS_P_1:\
        :rm=localhost:\
        :rp=bogus_p_1:\
        :rt=1234:\
        :sd=/TCPIP$LPD_ROOT/LOOP_BOGUS_P_1:
```

   Note that the `rm` field is set to "localhost".

2. On "HOSTB", using the standard LPD configuration procedure, configure the LPD receiver listening on port 515.

   Or

   If the you want to configure LPD on a port other than the default port, manually define another service database entry that is the same as LPD.

3. Run the SSH command on "HOSTA" to establish the SSH tunnel between the local port and remote port. For example, if the `rt` is 1234 on the local host and the remote port is "515" on which the LPD server is listening, use the following command to establish the SSH tunnel:

   ```
   SSH -"L"1234:localhost:515 hostb.hp.com
   ```