HP DECnet-Plus for OpenVMS
Release Notes

March 2010

This manual describes installation notes for this release, new features not discussed in the current documentation, corrections included in this release, documentation errata, and operational notes.

Revision/Update Information:	This revised manual supersedes *HP DECnet-Plus for OpenVMS Integrity servers-Release Notes*, V8.3-1H1.
Operating System:	OpenVMS Version 8.4 for Integrity servers OpenVMS Alpha Version 8.4
Software Version:	HP DECnet-Plus for OpenVMS Version 8.4

Hewlett-Packard Company
Palo Alto, California

Contents

3 Corrections Included in this Release

4 Documentation Errata and Addenda

5 Operational Notes

Tables

Preface

Intended Audience

This manual is intended for all HP DECnet-Plus for OpenVMS Version 8.4 software users. Read this manual before you install, upgrade, or use DECnet-Plus for OpenVMS.

Structure of This Book

This manual contains the following chapters:

- Chapter 1 contains installation notes for this release.

- Chapter 2 describes new features not documented in the DECnet-Plus Version 8.4/8.3-1H1/8.3/8.2-1/8.2/7.1 documentation set.

- Chapter 3 lists corrections included in this release.

- Chapter 4 contains documentation errata and additions.

- Chapter 5 discusses operational notes, restrictions, and known problems with the current release.

This manual contains release notes introduced in the current release and notes from previous DECnet-Plus versions that still apply to the new release.

For a list of additional documents available that support this version of the DECnet-Plus for OpenVMS software, see the *DECnet-Plus for OpenVMS Introduction and User's Guide*.

Reader's Comments

HP welcomes your comments on this manual or any of the DECnet-Plus documents. Please send comments to **openvmsdoc@hp.com**

How To Order Additional Documentation

For information about how to order additional documentation and for online versions of most DECnet-Plus documentation, visit the following World Wide Web address:

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

Conventions

The following conventions are used in this book.

Convention	Meaning
`special type`	Indicates a literal example of system output or user input. In text, indicates command names, keywords, node names, file names, directories, utilities, and tools.
	You can abbreviate command keywords to the smallest number of characters that OpenVMS, NCL, DECdns, DECdts and the other utilities accept, usually three characters.
UPPERCASE	Indicates keywords that you enter. You can type the characters in uppercase or lowercase. You can abbreviate command keywords to the smallest number of characters that OpenVMS, NCL, DECdns, DECdts, or the other utilities accept, usually three characters.
	Uppercase also indicates the names of files, directories, utilities, tools, commands, parameters, and procedures.
italic type	Indicates a variable.
bold	Indicates a new term defined in the text or important information.
Return	Indicates that you press the Return key.
Ctrl/*c*	Indicates that you press the Control key while you press the key noted by *c*.
[YES]	Brackets indicate that the enclosed item is a default value in an installation prompt.
{ }	In command format descriptions, indicates you must enter at least one listed element.
$	Represents the OpenVMS DCL system prompt.

1
Installation

This chapter discusses installation information not found in the current documentation set.

1.1 Features Not Supported in This Release

X.25 synchronous data links are NOT supported by HP DECnet-Plus for OpenVMS Version 8.4 for OpenVMS Integrity server systems. They ARE supported by HP DECnet-Plus for OpenVMS Version 8.3 for OpenVMS Alpha systems.

1.2 License Requirements

1.2.1 License Requirements for OpenVMS Integrity Servers

HP DECnet-Plus for OpenVMS Version 8.4 for Integrity server systems requires the Base Operating Environment (BOE) license. This license includes the basic function license (DVNETEND). If you intend to configure your system as a DNS server or use host-based routing, you must obtain a separate DVNETEXT license.

_____ **Warning** _____

If you install the software without the DVNETEXT license and then attempt to configure your system as a DNS server, the DNS server will fail and the configuration utility (NET$CONFIGURE) will exit.

_____

1.2.2 License Requirements for OpenVMS Alpha Systems

HP DECnet-Plus for OpenVMS Version 8.4 for Alpha systems requires one of two licenses: the basic function license (DVNETEND) or the extended function license (DVNETEXT). If you intend to configure your system as a DNS server, you must use the DVNETEXT license.

_____ **Warning** _____

If you install the software without the DVNETEXT license and then attempt to configure your system as a DNS server, the DNS server will fail and the configuration utility (NET$CONFIGURE) will exit.

_____

_____ **Warning for Installations over DECnet-Plus V7.3-1** _____

When DECdns server support for Alpha systems was added to DECnet-Plus in Version 7.3-1, the DECdns software mistakenly verified the VAX extended function license (DVNETRTG) instead of the Alpha extended function license. This error has been corrected.

> If you have a DECnet-Plus V7.3-1 system currently configured as a
> DECdns server, do not install this software until you obtain and install
> the DVNETEXT license. If you fail to install the DVNETEXT license,
> your DECdns server will not start.

1.3 OpenVMS Software Version Requirement

HP DECnet-Plus for OpenVMS Version 8.4 for OpenVMS Integrity servers
requires Version 8.4 of the OpenVMS Integrity servers operating system. HP
DECnet-Plus for OpenVMS Version 8.4 for OpenVMS Alpha requires Version 8.4
of the OpenVMS Alpha operating system.

_____ **Note** _____

DECnet Phase IV and DECnet-Plus cannot be installed on the same
system. They are mutually exclusive. If either of the DECnet product is
present on the system, uninstall the product before installing the other.

_____

1.4 Other Software Version Requirements

If your network includes X.25 connectivity, HP DECnet-Plus for OpenVMS
Version 8.4 requires Version 2.0 of the X.25 for OpenVMS product. See the *HP
DECnet-Plus for OpenVMS Installation and Configuration* manual for important
information about when to install this software during the DECnet-Plus
installation and configuration process.

_____ **Important** _____

Version 2.0 of the X.25 for OpenVMS product does not support
synchronous devices on OpenVMS Integrity server systems at this
time. Therefore, synchronous X.25 data links are not supported by HP
DECnet-Plus for OpenVMS Version 8.4 on OpenVMS Integrity server
systems.

_____

If your network includes TCP/IP connectivity and you plan to enable OSI over
TCP/IP or DECnet over TCP/IP, HP DECnet-Plus for OpenVMS Version 8.4
requires the latest version of the HP TCP/IP Services supported by the Operating
System.

1.5 Installing the New Release

Install this kit using the POLYCENTER Software Installation utility (PCSI) by
logging into the SYSTEM account. The following example is for the OpenVMS
Integrity servers platform.

Entering the following command at the DCL prompt (for OpenVMS Alpha
systems, use DECnet_OSI instead of DECNET_PLUS):

```
$ PRODUCT INSTALL DECNET_PLUS/SOURCE=file-location
```

For the new software to take effect, you must reboot the system. If the system is a member of a VMS cluster, you must reboot the entire cluster.

_____ **Note** _____

This kit contains a correction to the CDI$SHR executable (see CDI$SHR.EXE in the Corrections section). To ensure that this correction takes effect on a previously configured system, use the following command to clear the CDI cache after you install the kit:

```
$ MCR NCL FLUSH SESSION CONTROL NAMING CACHE ENTRY "*"
```
_____

1.6 AUTOGEN Errors During Installation (OpenVMS Alpha Only)

Version 7.3–2

The PCSI installation process now calls AUTOGEN near the end of the installation (with the parameters GETDATA, SETPARAMS, and CHECK_FEEDBACK). If AUTOGEN returns any error indication, the PCSI installation process displays the following informational text:

```
%PCSI-I-PRCOUTPUT, output from subprocess follows ...
%AUTOGEN-W-REPORT, please read AUTOGEN warnings in
SYS$SYSTEM:AGEN$PARAMS.REPORT
```

The AUTOGEN report may contain messages similar to the following:

```
** INFORMATIONAL ** - Removing CLU$PARAMS definition made by unknown product
    _UNKNOWN_$ADD_GBLPAGES = 55000    !Set by (unknown)
```

This message is related to the fact that previous versions of DECnet-Plus were incorrectly using the NEWPARAMS.DAT/CLU$PARAMS.DAT method to pass system parameter information to AUTOGEN. In previous versions, DECnet-Plus did not label its data in the NEWPARAMS.DAT file. The preceding message indicates that AUTOGEN has found an unlabeled system parameter in the existing CLU$PARAMS.DAT file and is removing it. If the system parameter was set by DECnet-Plus, the newly-created NEWPARAMS.DAT file contains the current system parameter requirements and these will be automatically included in CLU$PARAMS.DAT. Therefore, you can safely ignore these messages.

2

New Features and Enhancements

This chapter describes new functionality or enhancements provided by HP DECnet-Plus for OpenVMS. This section includes new functionality implemented in Versions 8.4, 8.3-1H1, 8.3, 8.2-1, 8.2, 7.3-2, 7.3-1, 7.3, 7.2-1, 7.2, and 7.1 which was not documented in the Version 8.2/Version 7.1 documentation set.

2.1 Network Management

This section describes new network management features.

2.1.1 DECnet/IP Communication Through SSH

Version 8.4   The following improvement has been made to NET$DRIVER.EXE, NET$OSDRIVER.EXE, NET$SESSION_CONTROL.EXE, NET$TRANSPORT_ OSI.EXE, and NET$TPCONS.EXE images:

This release of DECnet-Plus uses the port forwarding feature of Secure Shell (SSH). This enables you to transmit DECnet/IP data over a secure channel, thus providing data security. The DECnet transmitter side requires modification to support this feature; however the receiver side does not require any change.

This feature can be used Processwide or Systemwide by defining the logical with the /PROCESS or /SYSTEM qualifiers.

A new process or systemwide logical, DECNET_IP_PORT_FORWARD is introduced to provide the SSH functionality. The logical value should be unique and the port must be unused. The logical value must be same as that of the local port used to establish the secure channel. After setting the processwide logical in a particular process context, all DECnet/IP connections initiated by this process is secure.

If the systemwide logical is defined, all the DECnet/IP connections initiated by this system is secured.

Prerequisites: SSH client must be running on the local host and SSH server must be running on the remote host.

Note

For SSH related queries and support, contact the TCP/IP SSH Engineering team.

To enable the port forwarding feature of SSH, perform the following steps:

1. To establish a secure channel between a client and the server, execute the following SSH command

   ```
   Host1$ SSH -"L"port:host:hostport remotehost
   ```

   Where:

-L is the local port forwarding.

port is the local port on the client (local) system. The port value must be between 1 and 65535.

host is the server system.

hostport is the server's port.

remotehost is the remote system's IP address or name.

This command prompts you for the system password of the remotehost (Host2).

2. Enter the system password and an output similar to the following is displayed:

```
system's password:
Authentication successful.
Welcome to HP OpenVMS Industry Standard 64 Operating System, Version V8.4
```

3. Define the processwide or systemwide logical, DECNET_IP_PORT_FORWARD with the logical value. This logical value is same as that of the "Port" specified in Step 1.

Note

In a particular process context, if both the processwide and systemwide logicals are defined, the processwide logical gets the preference.

---

4. Execute the DECnet/IP commands such as directory, set host, and copy from the terminal on Host1 on which the logical is defined using the following syntax:

```
SET HOST LOCALHOST
```

The localhost is used instead of the IP address. Using localhost and port, an SSH channel is established between the transmitter and receiver system.

5. Deassign the logical after completing the task by executing the following command:

```
Host1$ DEASSIGN/PROCESS DECNET_IP_PORT_FORWARD
OR
Host1$ DEASSIGN/SYSTEM DECNET_IP_PORT_FORWARD
```

If the logical is not deassigned, all the connections still uses SSH.

Following is an example of how this implementation can be used:

In this example, the following names and numbers are used:

```
DECnet name: Host1              IP Number: 18.138.72.14
DECnet name: Host2              IP Number: 18.138.185.56
```

1. Set up a secure connection between local host (Host1) and remote host Host 2 using the following command:

```
Host1$ssh "-L" 512:localhost:399 18.138.185.56
system's password:

Authentication successful.

 Welcome to OpenVMS (TM) on Host2

Host2$
```

Where: 18.138.185.56 is the system IP address of the remotehost(Host2) to which you are transmitting data using the local port 512.

2. From a different terminal on the local host with a user login, a process or systemwide logical must be defined to use the DECnet/IP over SSH:

```
Host1$ DEFINE/PROCESS DECNET_IP_PORT_FORWARD 512
OR
Host1$ DEFINE/SYSTEM DECNET_IP_PORT_FORWARD 512
```

Where;

512 is the logical value, which is same as that of the "Port" specified in Step 1.

3. Execute a DECnet/IP command, such as SET HOST or COPY or DIRECTORY from the local host to remote host:

```
Host1$ DIRECTORY localhost"system welcome123"::sys$sysdevice:[000000]
```

An output of the DIRECTORY command from the 18.138.185.56 system is displayed.

4. After the communication is completed, you can deassign the logicals as follows, depending on whether a processwide or systemwide logical had been defined:

```
Host1$ DEASSIGN/PROCESS DECNET_IP_PORT_FORWARD
OR
Host1$ DEASSIGN/SYSTEM DECNET_IP_PORT_FORWARD
```

2.1.2 DECnet-Plus Support for Mixed Case Password

Version 8.3 The following improvements have been made to the NET$OSVCM.EXE and NET$SESSION_CONTROL.EXE images:

- OpenVMS version 7.3-2 and above allows you to use mixed-case and extended characters in passwords when PWDMIX is specified as login flags.

  DECnet has two different methods for user authentication. This is controlled by the sysgen parameter, NET_CALLOUT. If this parameter is set to 255, then the verification and proxy lookups are performed in LOGINOUT rather than DECnet.

  In earlier versions of DECnet, when DECnet performed the user verification there were restrictions on using mixed-case and extended characters in passwords. This version of DECnet supports mixed-case password for task to task communication and remote file access.

2.1.3 NET$CONFIGURE Improvements

The following changes have been made to NET$CONFIGURE.COM:

Version 8.3 • This release adds support for listening to selected interfaces for incoming DECnet over IP connections. DECnet-Plus, by default, would listen to inbound DECnet over IP connections on all IP-configured interfaces. With this new feature, you can select the interfaces on which DECnet over IP listens to the incoming connections. For example, if the system has five IP-configured interfaces and you want DECnet over IP to listen on only three interfaces, you can provide the list of IP addresses for those required interfaces.

To configure the system to listen to selective IP-configured interfaces using the ADVANCED configuration of DECnet-Plus:

- Type "ALL" if all the connections are required

  or

- Type comma separated list of the required IP addresses for the following question:

  * Interface(s) for DECnet/OSI over TCP/IP ? [ALL] :

  Also, refer to Section 2.1.3.1 for the new NCL commands.

Version 8.2
- The NET$CONFIGURE.COM procedure now informs you of the existence of the ISIS$CONFIGURE.COM procedure. You can use this procedure to configure a routing node that uses the link state routing protocol. Previously, there was no support for configuring a routing node using the link state routing protocol. For more information about using the ISIS$CONFIGURE.COM procedure, see the new appendix about configuring link state routing in the *HP DECnet-Plus for OpenVMS Installation and Configuration* manual.

2.1.4 NCL Updates

This section describes new features found in NCL.

2.1.4.1 Added information about Configuring the system to listen to DECnet/IP connections

Version 8.3
The following commands have been added to reflect the new feature described in Section 2.1.2 for V8.3

```
$MC NCL SET OSI TRANSPORT RFC1006 LISTENER IPADDRESSES {a.b.c.d, w.x.y.z}
$MC NCL ADD OSI TRANSPORT RFC1006 LISTENER IPADDRESSES {a.b.c.d, w.x.y.z}
$MC NCL REMOVE OSI TRANSPORT RFC1006 LISTENER IPADDRESSES {a.b.c.d,
w.x.y.z}
$MC NCL SHOW OSI TRANSPORT RFC1006 LISTENER IPADDRESSES
```

These commands will enable or disable DECnet-Plus to listen to inbound DECnet over IP connections on interfaces having local node IP addresses specified. However, these commands do not support DECnet-Plus to listen to remote node IP addresses. This is applicable for both RFC 1006 and RFC 1859.

---------------------------- **Note** ----------------------------

In this release, these commands are used to set/show/add/remove the OSI transport attributes on a local node only, but these commands cannot be used for a remote node.

2.1.5 NCL HELP Updates

Since Version 7.1, several changes have been made to NCL HELP. These changes represent new material about new functionality, new material about existing functionality, and corrections to existing material. The sections that follow describe help changes where some of the material discussed in the HELP updates is not present in the current documentation set or in these Release Notes.

2.1.5.1 Added New Material about Backtranslations and Towers

*Version
7.3–2*
Added significant explanatory material about managing `backtranslation softlink` and `tower maintenance` entities to the help text for the following commands:

`DELETE SESSION_CONTROL BACKTRANSLATION SOFTLINK SHOW SESSION_CONTROL BACKTRANSLATION SOFTLINK UPDATE SESSION_CONTROL BACKTRANSLATION SOFTLINK UPDATE SESSION_CONTROL TOWER MAINTENANCE`

For more information, see the help text (of particular interest is the help text for the two update commands).

2.1.5.2 Added Information about Support for IP Towers

*Version
7.3–2*
Added a description of an IP tower to the NCL_Introduction -> Syntax -> Data_Types -> TowerSet topic.

Added IP examples to the help text for commands used to manage `session control backtranslation softlink` and `session control tower maintenance` entities (see also Section 2.1.5.1).

Added an example of registering an IP tower using the `decnet_register` node registration tool to the Network_Management -> Tools -> Decnet_Register topic.

2.1.5.3 Added Help for register and modify decnet_register Commands

*Version
7.3–2*
Added new material about the `modify` and `register` commands used to set the session control version.
For more information about why these command examples may be useful, see the help text.

2.1.5.4 Added Information about Flushing the CDI Cache

*Version
7.3–2*
Added material to the help text for the Flush_(OpenVMS) topic. This topic discusses flushing an entry from the Session Control Naming Cache (known as the CDI cache). Also added an example of flushing an IP cache entry.

2.1.5.5 Modified Description of the Session Control Naming Search Path Characteristic

*Version
7.3–2*
Modified the description of the `naming search path` characteristic in the help text for the `show session control` command to reflect relaxed restrictions in both the content of and the order of the naming search path for DECdns servers. For more information about this topic, see Chapter 7 of the *HP DECnet-Plus for OpenVMS Installation and Configuration* manual (in particular, the section entitled "Using the DECdns Namespace as Secondary on a DECdns Server.")

2.1.5.6 Directory System Agent (DSA) Entity Help Updated

*Version
7.3–2*
Replaced the Directory_Module help topic with new help information for the HP OpenVMS Enterprise Directory product (HP's implementation of the ITU-T X.500 Recommendations for OpenVMS).

2.1.5.7 Added DNS/BIND Namespace Examples for LOOP Help

*Version
7.3–1*
Added DNS/BIND namespace examples to the help for the `loop loopback` application command. For example, the example section now includes the following DNS/BIND example:

`loop loopback application name DOMAIN:LAMCHP.SCH.DEC.COM`

2.1.5.8 Updated Help for FDDI Station Link Event Reporting

Version 7.3   Updated the Event_Messages -> FDDI_Station -> Link topic to reflect restrictions in FDDI Station Link event reporting which are imposed by the OpenVMS device drivers.

The following events are not logged, but their respective counters are incremented when these events occur:

    block check error
    directed beacon received
    duplicate address test failure
    duplicate token detected
    fci strip error
    frame status error
    link buffer unavailable
    pdu length error
    receive data overrun
    ring beacon initiated
    ring purge error
    trace initiated
    transmit failure
    transmit underrun

The "unrecognized individual pdu destination", "unrecognized multicast pdu destination", and "user buffer unavailable" events can be reported, and their respective counters can increase accordingly. However, DECnet blocks "unrecognized multicast pdu destination" by default. Refer to the `SYS$MANAGER:NET$EVENT_LOCAL.TEMPLATE` file if you wish to pass this event.

The "ring initialization initiated" and "ring initialization received" events are now logged by certain OpenVMS device drivers. If an OpenVMS device driver supports these events, they are not logged on a one-to-one basis with increases in their corresponding counters. Instead, only one error report is issued for any number of these events that occur within a sampling period. This is intended to decrease any possibility of flooding OPCOM.

2.2 New Devices Supported by MOP

Version 7.3   Modified NET$NISCS_LAA.EXE to recognize new style device names returned by $GETDVI. This permits loads over SCSI PAC devices. Prior to this release, the satellite load failed with the following messages displayed at the satellite:

```
%VMScluster-I-MSCPCONN, Connected to a MSCP server for the system disk,
  node nnnnnn
%VMScluster-E-NOT_SERVED, Configuration change, the system disk is no
  longer served by node nnnnnn
```

2.3 DECnet-Plus and DECnet Phase IV support VLAN

Version 8.3   The following improvements have been made to the NET$CONFIGURE.COM and NET$CONVERT_DATABASE.EXE:

• DECnet-Plus and DECnet phase IV can be configured to run over VLAN.

2.4 Transport Improvements

The following improvements have been made to NET$TPCONS.EXE and NET$TRANSPORT_OSI.EXE:

Version 8.3
- This release adds support for listening to selected interfaces for incoming DECnet over IP connections. For more information, see Section 2.1.2 for V8.3 and Section 2.1.3.1.

Version 7.3–1
- The DECnet-Plus interface has been redesigned to allow independent restarts between the DECnet OSI Transport module and the HP TCP/IP Services for OpenVMS product. Previously, the entire system had to be rebooted if the TCP/IP PATHWORKS Internet Protocol (PWIP) interface was restarted. Now, if the TCP/IP PWIP interface is disabled and then reenabled, DECnet-Plus starts new transport connections. Similarly, if the DECnet OSI Transport module is disabled and then reenabled, the TCP/IP PWIP interface receives new DECnet transport connections through the new TPCONS ports.

2.5 Host-Based Routing Improvements

Version 8.2
This release supports the configuration of host-based routers that use the link state routing algorithm. The NET$CONFIGURE procedure always creates routers that use the routing vector algorithm. However, a new command procedure (ISIS$CONFIGURE.COM) can be used to modify the router configuration to use the link state routing algorithm. This procedure also allows more control of the routing configuration than is found in NET$CONFIGURE.COM. For more information, see the "Host-Based Routing" section in Chapter 8 of the *HP DECnet-Plus for OpenVMS Network Management* manual and the new ISIS$CONFIGURE appendix in the *HP DECnet-Plus for OpenVMS Installation and Configuration* manual.

This release of the NET$ROUTING_IS.EXE module contains the following improvements:

Version 8.2
- Raised the maximum allowed routing circuits from 16 to 32.

Version 7.3
- Modified logic used to set maximum circuit segment size for FDDI circuits. Previously, the calculation could sometimes use the Phase IV default of 576. This has been changed to always use the FDDI default of 4352.

2.6 Session Control Improvements

This release of the NET$SESSION_CONTROL.EXE module contains the following improvement:

Version 7.3
- On Integrity servers and Alpha systems, the NET$SESSION_CONTROL.EXE module now uses the name string from the PSB instead of GETJPI.

2.7 Distributed Naming Service (DECdns)

The following sections describe new features of DECdns.

2.7.1 DECdns Now Supports Dynamic Device Recognition

Version 8.2   The static device tables formerly used to determine the devices used by DECdns have been removed. Now, DECdns uses the $DEVSCAN and $GETDVI system services to build a list of devices that have the following characteristics:

- a device class of DC$SCOM (synchronous communication device)
- a device characteristic of DEV$V_NET
- a device status of UCB$V_ONLINE and UCB$V_TEMPLATE
- a device name in the form _xxy0:

You can use the logical name DNS$ETHERNET_DEVICE to provide a list of devices that DECdns should NOT use. All devices must be in the form _xxy0:. The string can contain spaces and other text which is ignored by DTSS. For example, the following command tells DECdns not to use the _EIA0: and _FWA0: devices.

```
$ DEFINE/SYSTEM DNS$ETHERNET_DEVICE "Don't use _EIA0: and _FWA0: "
```

Note

Unterminated network adapters can cause the dynamic device recognition process to hang. Either terminate all network adapters or include any unterminated devices in the DNS$ETHERNET_DEVICE logical definition.

2.7.2 DECdns Now Supports DECnet over TCP/IP Links

Version 7.3–2   DECdns has been enhanced to support the DECnet over TCP/IP transport. The sections that follow discuss various topics related to this new feature. For more information, see the *HP DECnet-Plus for OpenVMS DECdns Management* manual.

2.7.2.1 Protocol Towers

The DNA$Towers attribute of the object entry for a Phase V node can now include a protocol tower with an IP address. The third tower in the following example is an IP protocol tower.

```
DNS>show obj .xpr.wzbang dna$towers
                              SHOW
                            OBJECT  WINTER:.xpr.wzbang
                               AT  09-MAR-2004:14:55:02
                DNA$Towers (set) = :
                Tower  1 Floor 1  = 01 13    (null)
                Tower  1 Floor 2  = 03       00 13
                Tower  1 Floor 3  = 04       (null)
                Tower  1 Floor 4  = 06       49 00 18 aa 00 04 00 2a 60 20
                DNA$Towers (set) = :
                Tower  2 Floor 1  = 01 13    (null)
                Tower  2 Floor 2  = 03       00 13
                Tower  2 Floor 3  = 05       de c0
                Tower  2 Floor 4  = 06       49 00 18 aa 00 04 00 2a 60 21
                DNA$Towers (set) = :
                Tower  3 Floor 1  = 01 13    (null)
                Tower  3 Floor 2  = 02       00 13
                Tower  3 Floor 3  = 05       de c0
                Tower  3 Floor 4  = 09       a1 72 5e 45
DNS>
```

2.7.3 decnet_register Now Supports IP Towers in the DECdns Namespace

Version 7.3–2

Normally, the IP towers and IP backtranslation softlinks for all nodes are now automatically updated in the DECdns namespace during regular tower and softlink maintenance operations. Occasionally, it may be necessary to perform manual updates or to verify that the current information is correct. For this reason, the decnet_register tool has been enhanced to show and register IP towers and backtranslation softlinks for nodes within the DECdns namespace. The following example illustrates how to use menu Option 1 to display information about the node WINTER:.XPR.CASE:

```
$  run decnet_register

DECNET_REGISTER - Manage node registrations in network directory services
  Use Return, CTRL/N, and CTRL/P to move between input fields
  Use "?" to obtain help, CTRL/Z to cancel

  1 - Show information about registered node names
  2 - Register or modify node names
  3 - Update registered node towers using information from the nodes
  4 - Rename a registered node name
  5 - Repair the synonym and address links for registered node names
  6 - Deregister node names

  7 - Export node names to a data file
  8 - Import node names from a data file

  9 - Set preferences and network values

 10 - Manage the directory service
 11 - Spawn to DCL

  * Option (use CTRL/Z to exit):  1

Show registered node information
  Use Return, CTRL/N, and CTRL/P to move between input fields
  Use "?" to obtain help, CTRL/Z to cancel

Specify the directory service as LocalFile, DECdns, or PhaseIV.

* Directory service:  DECdns

Specify the node to show using an explicit or wildcard name, an NSAP,
```

```
                  or a Phase IV synonym or address.

                  * Node name or address:  WINTER:.XPR.CASE

                  Specify the information to display as either brief, full, or names.
                  Specify the output file name (a blank line indicates the terminal).

                  * Display format:  full
                  * Output file:

                  Press Return to show the node values, CTRL/Z to cancel

                  Directory Service: DECdns

                  Node name:     WINTER:.XPR.CASE
                  Phase IV synonym:  CASE

                  Address tower protocol and selector values:
                    Session:   DNA_SessionControlV3 (SC3)
                               00 13
                    Transport: DNA_OSItransportV1 (TP4)
                               DE C0
                    Routing:   DNA_OSInetwork (CLNS)
                               49::00-18:AA-00-04-00-24-60:21 (24.36)

                    Session:   DNA_SessionControlV3 (SC3)
                               00 13
                    Transport: DNA_NSP (NSP)
                               (no selector value)
                    Routing:   DNA_OSInetwork (CLNS)
                               49::00-18:AA-00-04-00-24-60:20 (24.36)

                    Session:   DNA_SessionControlV2 (SC2)
                               00 13
                    Transport: DNA_OSItransportV1 (TP2 or TP0)
                               DE C0
                    Routing:   DNA_IP (IP)
                               161.114.94.62

                  Synonym softlink name:
                      WINTER:.DNA_NodeSynonym.CASE

                  Reverse address mapping (backtranslation) softlink names:
                      WINTER:.DNA_BackTranslation.%X49.%X0018.%XAA0004002460
                      WINTER:.DNA_BackTranslation.%XA1725E3E

                  Number of nodes reported on:  1
```

2.8 Distributed Time Service (DECdts)

The following sections describe new features of DECdts.

2.8.1 DECdts Now Supports Dynamic Device Recognition

Version 8.2   The static device tables formerly used to determine the devices used by DECdts have been removed. Now, DECdts uses the $DEVSCAN and $GETDVI system services to build a list of devices that have the following characteristics:

- a device class of DC$SCOM (synchronous communication device)

- a device characteristic of DEV$V_NET

- a device status of UCB$V_ONLINE and UCB$V_TEMPLATE

- a device name in the form _xxy0:

You can use the logical name DTSS$ETHERNET_DEVICE to provide a list of devices that DECdts should NOT use. All devices must be in the form _xxy0:. The string can contain spaces and other text which is ignored by DTSS. For example, the following command tells DECdts not to use the _EIA0: and _FWA0: devices.

```
$ DEFINE/SYSTEM DTSS$ETHERNET_DEVICE "Don't use _EIA0: and _FWA0: "
```

Note

Unterminated network adapters can cause the dynamic device recognition process to hang. Either terminate all network adapters or include any unterminated devices in the DTSS$ETHERNET_DEVICE logical definition.

2.8.2 DECdts Now Supports DECnet over TCP/IP Links

Version 7.3–2

DECdts now supports operation in the DECnet over TCP/IP environment without requiring the use of a configuration file. This requires the use of the DECdns version that supports DECnet over TCP/IP. From the management standpoint, global DECdts servers work much the same as they do in the DECnet-only environment. You still use the `advertise` command to add a global server to the global set. For more information, see the *HP DECnet-Plus for OpenVMS DECdts Management* manual.

3

Corrections Included in this Release

This chapter discusses corrections included in HP DECnet-Plus for OpenVMS Version 8.4. The chapter contains an abbreviated list of the updates included in this release. If a specific update you are looking for is not listed, this does not mean that it is not included in this release. For further information on specific updates, contact your HP support representative.

3.1 DNS$ADVER.EXE

The following correction has been made to DNS$ADVER.EXE:

- This release fixes the DECnet hang during start-up when the DNS$ADVER process is in the RWAST state. This happens when the PQL_MBYTLM/BUFFER_LIMIT parameter is set to a high value or when the number of network interfaces are more than 10.

  In addition to the messages that are logged in DNS$ADVER_ERROR.LOG logfile, a message will be logged on the operator console when the DNS$ADVER process is unable to start its protocol on any of the ethernet interfaces.

3.2 DTSS Changes

The following correction has been made to the DTSS$SERVICE image:

- This fix prevents the access violation error found during DTSS server startup with global server configured.

3.3 Network Management Changes

The following corrections are made to the network layer.

- This release fixes the INVEXCEPTION crash in the routing layer caused because of accessing the corrupted end system cache database. When the $ MC NCL DISABLE ROUTING command is executed, apart from disabling the routing entity it clears the base address of the end system cache table while processing the incoming data PDU.

- This release fixes the BADQHDR crash while trying to resume the network task, which is the "SUSPENDED QUEUE" task at the session layer. Failure to acquire the secondary interlock on the header of the suspended queue at the session layer causes the system to crash.

3.3.1 End System Routing

The following correction has been made to the NET$ROUTING_ES.EXE image:

- This release fixes some of the alignment faults in NET$ROUTING by aligning the unaligned variables found during DTSEND tests.

The following correction has been made to NET$ROUTING_ES.EXE and NET$ALIAS.EXE images:

- This fix sets the ES hello packet with a holding time of zero so as to clear the adjacencies immediately when the "SHUT ALIAS port" command is used.

The following correction has been made to NET$ROUTING_VCM.EXE and SYS$NAME_SERVICES.EXE images:

- This release fixes the alignment faults observed in SYS$NAME_SERVICES and NET$ROUTING_VCM on Integrity server systems.

The following correction has been made to the NET$ROUTING_IS.EXE image:

- This release fixes the system crash while creating a new manual adjacency with the same Adjacency name, LAN address, and ENDnode id on two different CSMA-CD circuits.

3.3.2 NET$CONFIGURE Command Procedure

The following corrections have been made to the NET$CONFIGURE.COM command procedure:

- This fix validates the IP address and prompts until a valid IP address is entered for the "Interface(s) for DECnet/OSI over TCP/IP" option while running NET$CONFIGURE in an advanced mode.

- This release enables SYS$NODE* logicals to be read from the NET$CONFIG.DAT file with the correct set of privileges on an Integrity server satellite node. The following warning message is no longer displayed while booting the satellite system:

```
%DECnet-W-NOOPEN, could not open SYS$SYSROOT:[SYSEXE]NET$CONFIG.DAT
```

3.3.3 NET$STARTUP Command Procedure

The following correction has been made to the NET$STARTUP.COM command procedure:

- The default protection of the OSIT$NAMES logical name table has been modified such that only the privileged user, such as SYSTEM will be able to modify the table.

  As described in Section 6.4.6.1 of *DECnet-Plus for OpenVMS Programming Manual*, the SYSNAM privilege to define a logical name in OSIT$NAMES is not applicable.

3.3.4 NCL$GLOBALSECTION.DAT

The following change has been made to NCL$GLOBALSECTION.DAT:

- In this release, the naming format of "rfc1006 Duplicate Connection" is changed to "RFC1006 Duplicate Connection". The following commands enable OSITP to accept the RFC1006 CLASS-0 duplicate connections without affecting the original connections:

```
$ mc ncl show osi transport RFC1006 Duplicate Connection
$ mc ncl set osi transport RFC1006 Duplicate Connection = TRUE or FALSE
```

3.4 OSAK Changes

The following corrections have been made to the OSAK$OSAKSHR.EXE image:

- This release fixes the problem of OSAK ports not being closed properly even when the Directory System Agent (DSA) timer is set to 300. As a result, the DSA-server would hang.

- This fix avoids an access violation in OSAK$OSAKSHR.EXE when the OSAK library function, osak_close_port tries to access a memory that is already freed-up.

- When the OSI Transport connection is already established, remote NSAP address is not populated if a disruptive event occurs. This problem is fixed.

3.5 Session Control

The following corrections have been made to the NET$SESSION_CONTROL.EXE image:

- This release suppresses the display of the `Failure on the back translate address request` message when a node is connected to another node using the SET HOST command. This happens when:

  - A node with fullnodename, that is, with the first octet (from left side) with greater than 8 alpha numeric characters and without the alias in the TCP/IP local host database.

    OR

  - A node is registered in the DECnet local database without a synonym.

- This releases fixes the crash in Session layer while processing an Expedited data event, which came from Transport layer for a non-existent Session port.

3.6 Transport Layer

The following corrections have been made to the NET$TRANSPORT_OSI.EXE image:

- When there is a duplicate CONS connection at the OSI transport, with the same source reference, this release is fixed to reject the new connection without affecting the existing connection.

- This release fixes the INVEXCEPTION crash in the OSITP port management routine while trying to access an already deallocated network connection control block (NCCB).

- This release fixes the INVEXCEPTION crash in OSITP$CLNS_CLOSEASSOCIATION because of an invalid VCRP address passed to this routine. The system crash occurs while trying to access this invalid virtual address.

- This release fixes the system crash with NAT Consumption fault error in the NET$OSI_TRANSPORT module. This fix is applicable only on Integrity server systems.

- This release fixes the leaking BG devices which is caused when an illegal packet is received and when the transport connection between the TPCONS and the OSI layer is not yet opened.

The following change has been made to CTF$OSITP_ANALYZE.EXE and NET$TRANSPORT_OSI.EXE:

- This release is enhanced to display the Local and Remote Transport Selector (Tsel) information as part of the Remote Transport Disconnect OPCOM Event and Local Transport OPCOM Event on both Integrity servers and Alpha systems. This will help you to debug or trace the faulty applications.

The following corrections have been made to the NET$TRANSPORT_NSP.EXE image:

- This release enhances the performance between DECnet Alpha Phase IV and DECnet Integrity servers Phase V (DECnet-Plus) system by transmitting less number of data acknowledgements.

  The transmitter now processes less number of data acknowledgements while transferring data.

- This release fixes the crash in NET$TRANSPORT_NSP caused because of the NAT consumption fault.

4

Documentation Errata and Addenda

This chapter contains corrections and additions to the current documentation set for HP DECnet-Plus for OpenVMS.

4.1 Current Product Documentation

Version 8.4   The current documentation set for DECnet-Plus is shown in the following list:

- *DECnet-Plus for OpenVMS Introduction and User's Guide*
  Version 7.1
  (Order number: AA-Q191F-TE)

- *DECnet-Plus Planning Guide*
  Version 7.1
  (Order number: AA-QBTHE-TE)

- *HP DECnet-Plus for OpenVMS Installation and Configuration*
  Version 8.3
  (Order number: BA406-90007)

- *HP DECnet-Plus for OpenVMS Network Management*
  Version 8.2
  (Order number: BA406-90006)

- *HP DECnet-Plus for OpenVMS Network Control Language Reference*
  Version 8.2
  (Order number: BA406-90004)

- *DECnet-Plus Problem Solving*
  Version 7.1
  (Order number: AA-Q18ZE-TE)

- *HP DECnet-Plus for OpenVMS DECdns Management*
  Version 8.2/DECdns Version 2.0
  (Order number: BA406-90002)

- *HP DECnet-Plus for OpenVMS DECdts Management*
  Version 8.2/DECdts Version 2.0
  (Order number: BA406-90003)

- *DECnet-Plus FTAM and Virtual Terminal Use and Management*
  Version 7.1/FTAM Version 3.2
  (Order number: AA-Q78TD-TE)

- *DECnet-Plus for OpenVMS Programming*
  Version 7.1
  (Order number: AA-Q195E-TE)

- *DECnet-Plus DECdts Programming*
  Version 7.1/DECdts Version 1.1
  (Order number: AA-PHEQC-TE)

- *DECnet-Plus OSAK Programming*
  Version 7.1/OSAK Version 3.0
  (Order number: AA-PJ1CE-TE)

- *DECnet-Plus OSAK Programming Reference*
  Version 7.1/OSAK Version 3.0
  (Order number: AA-PJ1DD-TE)

- *DECnet-Plus OSAK SPI Programming Reference*
  Version 7.1/OSAK Version 3.0
  (Order number: AA-QRAYB-TE)

- *DECnet-Plus FTAM Programming*
  Version 7.1/FTAM Version 3.2
  (Order number: AA-PJ1EF-TE)

- *DECnet/OSI for VMS CTF Use*
  Version 5.5
  (Order number: AA-PHEBB-TE)

4.2 Documentation Update for Version 8.2

Several manuals have been updated for HP DECnet-Plus for OpenVMS Version
8.2. See the list in Section 4.1 for the version numbers associated with each
manual in the documentation set. Much of the updated material came from
entries in the Release Notes for several previous versions of DECnet-Plus.
Table 4–1 provides a cross-reference between former Release Note topics and
their locations in the new manuals. The manual references are given in the form
manual-chapter or appendix where *manual* is the following:

INS - *HP DECnet-Plus for OpenVMS Installation and Configuration*
MNG - *HP DECnet-Plus for OpenVMS Network Management*
NCL - *HP DECnet-Plus for OpenVMS Network Control Language Reference*
DNS - *HP DECnet-Plus for OpenVMS DECdns Management*
DTS - *HP DECnet-Plus for OpenVMS DECdts Management*

In many cases, the information in the Release Notes was interleaved with existing
information. Therefore, references to specific sections in the new manuals is not
feasible.

Table 4–1   Documentation Update/Release Notes Cross-Reference

Release Note Topic	Refer to ...
New Features	
NET$CONFIGURE	
New option to configure DNS servers	INS-7
DNS server node can have other name service as primary	INS-7
Phase IV migration improvements	INS-6
New Support for DNS/BIND as Primary Name Service	INS-6
NET$STARTUP Procedure	

Table 4–1 (Cont.)   Documentation Update/Release Notes Cross-Reference

Release Note Topic	Refer to ...
NET$STARTUP supports STARTUP_P2 SYSGEN procedure	MNG-8
NET$LOGICALS File	
New logicals	MNG-6
NET$SHUTDOWN	
New NET$APPLICATION_SHUTDOWN logical	MNG-6, MNG-8
NCL	
Explanation of IP address backtranslations	NCL-1
New management topics in NCL Help	NCL-1
Improved explanation of access control	NCL-1
Improved explanation of wildcard proxies	NCL-1
New SHUT ALIAS PORT command	NCL-3
Host Based Routing	
Routing Originating Queue Limit characteristic modified	NCL-21
Session Control/CDI Cache	
CDI cache improvement	MNG-5
CDI$SYSTEM_TABLE logical name table	MNG-5
Resolution of IP fully-qualified names	MNG-5
DECdns	
Establishing clerk connections to WAN TCP/IP Servers	INS-7
New logicals for the DNS$ADVER process	DNS-12
Controlling the LAN devices used by DECdts	DNS-6
DECdts	
New procedures for Changing Time	INS-7[1]
New DECdts NTP provider sample program	DTS-C
Designating Global Servers Using the BIND Database	DTS-2
Option to Disable DECdts at System Boot	DTS-2
Controlling the LAN devices used by DECdts	DTS-2
OSAK	
OSAK new features moved to Documentation Errata chapter.	
Documentation Corrections	
NCL	
Syntax corrections	NCL-(throughout command descriptions)

---

[1]See also the "Setting System Time" chapter in the *HP OpenVMS System Manager's Utility Guide*, the "Creating Time Zone Conversion Information" in the "Overview" chapter of the *Compaq C Run-Time Library Utilities Reference Manual*, and the "Date/Time Functions" chapter and tzset function description in the *HP C Run-Time Library Reference Manual for OpenVMS Systems* manual.

Table 4–1 (Cont.)   Documentation Update/Release Notes Cross-Reference

Release Note Topic	Refer to ...
Alias Port Outgoing Default characteristic added	NCL-3
Routing Entity Maximum Buffers characteristic modified	NCL-21
Removed restriction on modifying OSI Transport Cons Filters characteristic	NCL-20
Added material about using SET NCL DEFAULT commands	NCL-1
Added material about using NCL SNAPSHOT command	NCL-1
Network Management	
New DECNET_VERSION values	MNG-3
Added material about using SNAPSHOT command	MNG-11, NCL-1
Operational Notes	
Network Management	
Startup procedure changed: NCL information minimized	MNG-6, MNG-8
decnet_register option 3 - updating registered node towers	MNG-5, MNG-E
DECdns	
Modifying a Clerk to use the Cluster Alias	DNS-6
Providing adequate resources for DNS clerk	DNS-12
Providing adequate resources for DNS server	DNS-12
Using the DNS.CONF file	DNS-12
Adjusting null_port_timeout in DNS.CONF file	DNS-12
Note on using the NEW EPOCH command	DNS-11
Default parameters for process limits on DNS servers	DNS-12
Removing Obsolete DNS$CACHE files	DNS-12

4.3 Network Management and NCL

The following sections describe documentation errata and addenda for the *HP DECnet-Plus for OpenVMS Network Management*, *HP DECnet-Plus for OpenVMS Network Control Language Reference*, and *DECnet-Plus Problem Solving* manuals.

4.3.1 Devices and OpenVMS Device Names

Version 8.2   The sections that follow list the devices that can be configured using DECnet-Plus software. The last column lists the device name to use for the `communication port` characteristic when creating entities that reference these devices.

_____ **Note** _____

DECnet-Plus supports a subset of the communication devices supported by OpenVMS. Some of the devices shown in these tables may be configurable (either by NET$CONFIGURE or directly by NCL) but

are no longer supported by DECnet-Plus. See the *Software Product Descriptions* (SPDs) for HP DECnet-Plus for OpenVMS and HP OpenVMS for a list of devices supported by the current release.

4.3.1.1 CSMA-CD Devices

The circuit devices listed in Table 4–2 can be configured using DECnet-Plus software. They provide multi-access connections among many nodes on the same CSMA-CD circuit.

Table 4–2 CSMA-CD Devices

Device Name	Type	OS	I/O Bus	OpenVMS Name	DECnet Comm Port
82559 (Intel)	100BaseTX	Integrity servers	PCI(embedded)	EI	EI*c*
A5230A	100BaseTX	Integrity servers	PCI	EW	EW*c*
A5506B	100BaseTX (4-port)	Integrity servers	PCI	EW	EW*c*
A6825A	1000BaseTX	Integrity servers	PCI	EW	EW*c*
A6847A	1000BaseSX	Integrity servers	PCI	EW	EW*c*
A7011A	1000BaseSX (2-port)	Integrity servers	PCI-X	EI	EI*c*
A7012A	1000BaseTX (2-port)	Integrity servers	PCI-X	EI	EI*c*
A9782A	1000BaseSX	Integrity servers	PCI-X	EW	EW*c*
A9784A	1000BaseTX	Integrity servers	PCI-X	EW	EW*c*
BCM5701	1000BaseTX	Integrity servers, Alpha	PCI(embedded)	EW	EW*c*
BCM5703	1000BaseTX	Integrity servers, Alpha	PCI(embedded)	EW	EW*c*
COREIO	10Base5	Alpha	TURBOchannel	ES	ES*c*
DEBNA	10Base5	VAX	BI-bus	ET	ET*c*
DEBNI	10Base5	VAX	BI-bus	ET	ET*c*
DEBNK	10Base5	VAX	BI-bus	ET	ET*c*
DEBNT	10Base5	VAX	BI-bus	ET	ET*c*
DEGPA-*xx*	1000BaseTX,SX	Alpha	PCI	EW	EW*c*
DEGXA-*xx*	1000BaseTX,SX	Alpha	PCI,PCI-X	EW	EW*c*
DELQA	10Base5	VAX	Q-bus	XQ	XQ*c*
DELTA	10Base5 (2-port)	VAX	TURBOchannel	EC	EC*c*
DELUA	10Base5	VAX	UNIBUS	XE	XE*c*

Table 4–2 (Cont.)   CSMA-CD Devices

Device Name	Type	OS	I/O Bus	OpenVMS Name	DECnet Comm Port
DEMNA	10Base5	VAX,Alpha	XMI	EX	EX*c*
DEQTA	10Base5	VAX	Q-bus	XQ	XQ*c*
DESQA	10Base5	VAX	Q-bus	ES	ES*c*
DESVA	10Base5	VAX	embedded	ES	ES*c*
DEUNA	10Base5	VAX	UNIBUS	XE	XE*c*
DE20*c*	10Base2,5,T	Alpha	ISA	ER	ER*c*
DE422	10Base2/T	Alpha	EISA	ER	ER*c*
DE425	10Base2/5/T	Alpha	EISA	ER	ER*c*
DE434	10BaseT	Alpha	PCI	EW	EW*c*
DE435	10Base2/5/T	Alpha	PCI	EW	EW*c*
DE436	10BaseT (4-port)	Alpha	PCI	EW	EW*c*
DE450	10Base2/5/T	Alpha	PCI	EW	EW*c*
DE500-*xx*	100BaseTX,FX	Alpha	PCI	EW	EW*c*
DE504-BA	100BaseTX (4-port)	Alpha	PCI	EW	EW*c*
DE600-*xx*	100BaseTX,FX	Alpha	PCI	EI	EI*c*
DE602-*xx*	100BaseTX,FX (2-port)	Alpha	PCI	EI	EI*c*
KFE52	10Base5	VAX	Q-bus	EF	EF*c*
P2SE	100BaseTX	Alpha	PCI	EW	EW*c*
P2SE+	100BaseTX	Alpha	PCI	EW	EW*c*
PMAD	10Base5	VAX,Alpha	TURBOchannel	EC	EC*c*
SGEC	10Base2	VAX	Local	EZ	EZ*c*
TGEC	10Base2	Alpha	Local	EZ	EZ*c*

Note

ATM devices are supported in emulated LAN (ELAN) mode by the OpenVMS EL device. For information about configuring an ELAN (and creating the EL device), see the "Configuring an Emulated LAN (ELAN)" section in the "Local Area Network (LAN) Device Drivers" chapter in the *HP OpenVMS I/O Users Reference Manual*.

LAN failover sets are supported by the OpenVMS LL device. For a general discussion of LAN failover sets, see Chapter 10 in Volume 2 of the *HP OpenVMS System Manager's Manual*. For information about managing LAN failover sets, see the description of the LANCP utility's DEFINE DEVICE and SET DEVICE commands in the *HP OpenVMS System Management Utilities Reference Manual*.

4.3.1.2 FDDI Devices

The devices listed in Table 4–3 can be configured using DECnet-Plus software. These devices provide multi-access connections among many nodes on the same FDDI circuit.

Table 4–3 FDDI Devices

Device Name	Type	OS	I/O Bus	OpenVMS Name	DECnet Comm Port
DEFAA	100 mmf	Alpha	FutureBus+	FA	FA*c*
DEFEA-*xx*	100 mmf, UTP	Alpha	EISA	FR	FR*c*
DEFPA-*xx*	100 mmf, UTP	Alpha	PCI	FW	FW*c*
DEFPZ-*xx*	100 mmf, UTP	Alpha	PCI	FW	FW*c*
DEFQA	100 mmf	VAX	Q-bus	FQ	FQ*c*
DEFTA-*xx*	100 mmf, UTP	VAX,Alpha	TURBOchannel	FC	FC*c*
DEFZA	100 mmf	VAX,Alpha	TURBOchannel	FC	FC*c*
DEMFA	100 mmf	VAX,Alpha	XMI	FX	FX*c*

4.3.1.3 Synchronous Devices (OpenVMS VAX and Alpha Only)

The synchronous devices listed in Table 4–4 can be configured by DECnet-Plus software. All of the synchronous line devices are either point-to-point or multipoint tributary circuit devices.

Table 4–4 Synchronous Devices (OpenVMS VAX and Alpha Only)

Device Name	Type	OS	I/O Bus	OpenVMS Name	DECnet Comm Port
DIV32		VAX	Q-bus	SD	DIV-*c-u*
DMB32	1-port	VAX	VAXBI	SI	DMB-*c-u*
DMF32	1-port	VAX	UNIBUS	XG	DMF-*c-u*
DNSES	2-port	Alpha	EISA	ZE	ZE-*c-u*
DPV11	1-port	VAX	Q-bus	SE	DPV-*c-u*
DSB32	2-port	VAX	VAXBI	SL	DSB-*c-u*
DSF32	2-port	VAX	MI–bus	SF	DSF-*c-u*
DSH32	2-port	VAX	Busless	ZS	DSH-*c-u*
DST32	1-port	VAX	Busless	ZS	DST-*c-u*
DSV11	2-port	VAX	Q-bus	SJ	DSV-*c-u*
DSW21	1-port	VAX	Busless	ZT	DSW-*c-u*
DSW41	1-port	VAX	Busless	ZT	DSW-*c-u*
DSW42	2-port	VAX	Busless	ZT	DSW-*c-u*
DSYT1	2-port	Alpha	TURBOchannel	ZY	ZY-*c-u*
DUP11	1-port	VAX	UNIBUS	SE	DPV-*c-u*
PBXDD-A*x*	2-, 4-port	Alpha	PCI	ZZ	ZZ-*c-u*
PBXDI-A*x*	2-, 4-port	Alpha	ISA	ZS	ZS-*c-u*

Table 4–4 (Cont.)   Synchronous Devices (OpenVMS VAX and Alpha Only)

Device Name	Type	OS	I/O Bus	OpenVMS Name	DECnet Comm Port
PBXDP-A*x*	2-, 4-, 8-port	Alpha	PCI	ZW	ZW-*c-u*
SCC	1-port	Alpha	None	ZR	ZR-*c-u*

4.3.1.4 Asynchronous Devices (OpenVMS VAX Only)

The asynchronous devices listed in Table 4–5 can be configured by DECnet-Plus software on OpenVMS VAX systems.

Table 4–5   Asynchronous Devices (OpenVMS VAX Only)

Device Name	Type†	I/O Bus	OpenVMS Name	DECnet Comm Port
DHQ11	8-line,MC	Q-bus	TX	TX-*c-u*
DHU11	16-line,MC	UNIBUS	TX	TX-*c-u*
DHV11	8-line,MC	Q-bus	TX	TX-*c-u*
DMB32	8-line,MC	VAXBI	TX	TX-*c-u*
DMF32	8-line,MC	UNIBUS	TX	TX-*c-u*
DMZ32	24-line,MC	UNIBUS	TX	TX-*c-u*
DZ11	8-line,PMC	UNIBUS	TT	TT-*c-u*
DZ32	8-line,PMC	UNIBUS	TT	TT-*c-u*
DZQ11	4-line,PMC	Q-bus	TT	TT-*c-u*
DZV11	4-line,PMC	Q-bus	TT	TT-*c-u*

†MC = full modem control, PMC = partial modem control

4.3.2 DTR/DTS

Version 7.3   In Section 3.10.2 of the *DECnet-Plus Problem Solving* manual, the documentation for the /nodename qualifier of the DTS test command contains a statement that seems to indicate that DTS/DTR might support Phase V node names. The statement should read as follows:

The *node-id* can be 0, a Phase IV address or node name, or, on a Tru64 UNIX system, a DECnet-Plus NSAP address or Phase V node name. To specify a Phase V node on OpenVMS systems, you must use a node synonym of 6 characters or less.

4.4 OSAK Programming

The following sections provide information that updates the current OSI Applications Kernel (OSAK) programming documentation.

4.4.1 called_aei Parameter on A-ASSOCIATE and S-CONNECT Indication Events

Version 7.2 For A-ASSOCIATE indication events in the OSAK API, and S-CONNECT indication events in the SPI, the nsap field of the `called_aei` parameter is no longer filled in by OSAK. Previously, the `called_aei.paddress.nsap` structure contained the values specified in the `local_aei.paddress.nsap` parameter on the `osak_open_responder` or `spi_open_responder` call. However, these values are not used by `osak_open_responder` or `spi_open_responder` and may not contain correct information about the received connection (for example, the transport type).

4.4.2 ROSE Minimum Workspace Increased

Version 7.2 The minimum required size for the parameter block workspace for ROSE has increased. If your ROSE application is using the old minimum workspace size, you will now get a bad parameter error. It is recommended that your application use the constant ROSE_WS_SIZE defined in `osak_api.h` to get the correct minimum workspace size.

> **Note**
>
> Depending on the size of your application's parameter block workspace, you may have to recompile your ROSE applications.

4.4.3 Using OSAK with OSI over TCP/IP

Version 7.2 On the initiator side, to make a connection using OSI over TCP/IP, specify as the NSAP the IP address as a 6-byte nibble packed hex value including the port number in the first two bytes. For example, the address of 16.36.12.142 on port 102 would be encoded as follows:

```
102   16.36.112.142
 |    |  |   |  |
0066  10 24  70 8E
```

In this case, the NSAP would be 00661024708E (hex). Specify the NSAP type as OSAK_C_RFC1006. For the transport template, specify either the pseudo-template "1006" or no template at all. OSAK uses a default template of "1006" if the NSAP type is OSAK_C_RFC1006.

On the responder side, to listen for OSI over TCP/IP connections, specify as the transport template the pseudo-template "1006".

4.4.4 New Status Code for osak_send_more and spi_send_more Routines

Version 7.2 The routines `osak_send_more` and `spi_send_more` can now return a status code of OSAK_S_NODATA which indicates that there is no data remaining. In previous versions, the status code OSAK_S_INVFUNC may have been returned when this error occurred.

4.4.5 New OSAK API Routine: osak_tc_no_sc( )

Version 7.2   OSAK now contains a new API routine which allows application programs to query OSAK to determine whether a transport connection has been established on a port, but a session connection has not.

Syntax:

```
status = osak_tc_no_sc(port, state)
```

C Binding:

```
osak_tc_no_sc(port, state)
osak_port port;
int *state;
```

Arguments:

port

The OSAK port that you wish to query.

state

A pointer to an integer where OSAK should return the state information. If the port is connected at the transport layer, but not at the session layer, OSAK returns a non-zero value (true). If the port is connected at the session layer, OSAK returns a zero value (false).

Description:

Call this routine to determine whether the port is connected at the transport layer, but not at the session layer. This information can be useful when interoperating with some other OSI implementations that may incorrectly terminate the transport connection, or may establish a transport connection but never complete the session connection. Use of this routine can assist an application in determining if the OSAK port is hung. An equivalent routine also exists for the SPI interface: spi_tc_no_sc( ).

Return Values:

OSAK_S_NORMAL	The routine has finished without error.
OSAK_S_INVPORT	The port identifier is invalid.

4.4.6 Handling of Default Transport Templates

Version 7.1   The following information clarifies statements made about template defaulting in the *DECnet-Plus OSAK Programming Reference* and *DECnet-Plus OSAK SPI Programming Reference* manuals.

If no transport template is specified in the osak_associate_req (API and ROSE) or spi_connect_req (SPI) call, OSAK takes the following actions:

- If the NSAP in the osak_nsap data structure is CONS or CLNS, OSAK uses the default transport template.

- If the NSAP in the osak_nsap data structure is RFC 1006, OSAK uses the osit$rfc1006 transport template.

4.4.7 Omitted Parameter Block Parameters

Version 7.1   In the *DECnet-Plus OSAK SPI Programming Reference* manual, the following OSAK parameter block parameters were omitted from the SPI routine descriptions. Although the parameters are listed in Section 1.2 and described in Section 1.4.2, they should also appear in the Parameters Used table as follows:

Parameters Used	Data Type	Access
[user_context]	Address	read only
port_id	osak_port	write only

The preceding parameters should be listed for all SPI routines that have the OSAK parameter block argument, except for the following:

- `spi_async_close`

- `spi_close_port`

- `spi_collect_pb`

- `spi_expedited_req`

4.5 File Transfer, Access, and Management (FTAM)

The following section describes the documentation update for *DECnet-Plus FTAM Programming Manual.*

4.5.1 Possible Values for OSIF_FAILURE

Version 8.4   The error_code argument for the `osif_get_event` call provides further information if the status returned from the call is OSIF_FAILURE. All the possible values for OSIF_FAILURE is documented in *DECnet-Plus FTAM Programming Manual*. The two more possible values for OSIF_FAILURE, which is not documented includes the following values:

- 44743722 - corresponds to OSAK_S_INVAEI, invalid application entity invocation.

- 44743770 - corresponds to OSAK_S_INVPCTXT, invalid presentation context list.

5

Operational Notes

This chapter contains operational notes and restrictions for HP DECnet-Plus for OpenVMS. This chapter also includes known problems with the current release.

5.1 Network Management

The following sections discuss several operational notes about network management.

5.1.1 CTF Utility Now Requires Process Privileges

Version 8.2
The CTF utility has always required that the invoking process have certain rights identifiers in order to use the START and STOP commands to control the collection of trace records. These rights identifiers are described in Chapter 3 of the *DECnet/OSI for VMS CTF Use* manual.

Now, in addition to one or more of the required rights identifiers, the invoking process must have the following process privileges before invoking CTF for any purpose:

ALTPRI, BYPASS, CMKRNL, NETMBX, PRMGBL, PRMMBX, PSWAPM, SYSGBL, SYSLCK, SYSNAM, TMPMBX, and WORLD

If you invoke CTF from a process without the required process privileges, the utility exits with an error message indicating the first of the required privileges not granted.

5.1.2 Tuning to Support the Larger CML BYTLM Value

Version 8.2 and 7.3–1
The default BYTLM value for CML has been increased from 10,000 to 64,000. This correction was done to prevent NCL from returning the NCL-E-OVERFLOWBYTLM error message when large amounts of data were needed from CML. If you have ever experienced this problem, or if your MAXBUF value is already set to 64000 and you have received NCL-E-NORESOURCEAVAIL error messages, then you should make the changes described in this section.

To fully take advantage of the increased BYTLM value, do the following:

1. Increase the value of MAXBUF to 64,000.

2. Raise the BYTLM quota on any account that might issue NCL commands requiring the increased resources to at least 65,000. Be sure to do this to at least the SYSTEM, CML$SERVER, and MIRRO$SERVER accounts. For example, to modify the CML$SERVER account, use the following command:

```
$ run sys$system:authorize
UAF> modify cml$server/bytlm=65000
```

3. Check for the existence of the logicals NETACP_BYTLM, NETEVD_
    BYTLIM, and NET$MOP_BYTLIM. If any of these logicals are defined
    and they are set to a value lower than 65,000, modify their entries in
    SYS$MANAGER:NET$LOGICALS.COM to raise their value to at least
    65,000.

4. Check for the existence of the NET$LESACP_BUFFER_LIMIT logical. If this
    logical is defined and it is set to a value lower than 65,000, modify its entry
    in SYS$STARTUP:NET$LES_STARTUP.COM to raise the value to at least
    65,000.

5. Check for the existence of the NET$ADVER_BUFFER_LIMIT logical. If this
    logical is defined and it is set to a value lower than 300,000, modify its entry
    in SYS$STARTUP:SYLOGICALS.COM to raise the value to at least 300,000.

6. Reboot the system to make all the preceding changes effective.

If, after applying the measures described in the previous list, you now receive
NCL-E-NORESOURCEAVAIL errors instead of NCL-E-OVERFLOWBYTLIM
errors, this generally indicates that your process BYTLM quota is not set high
enough. Set the quota to a value slightly higher than the MAXBUF value.
Setting process BYTLM quotas to 65,000 (as specified in the previous list) should
be sufficient to avoid this problem.

5.1.3 COLLECT Command and Addressing in decnet_migrate Commands

Version 7.1   Some connection errors might be reported for nodes with DECnet-Plus addresses
that are not Phase-IV compatible as well. These errors occur because the network
management interface on the OpenVMS operating system does not recognize
connections to nodes by the explicit use of a DECnet-Plus address that is not
Phase-IV compatible.

If a DECnet-Plus node also has a Phase-IV compatible address, information is
collected for it using that address.

5.1.4 Decimal Syntax DSPs Not Supported

Version 7.1   DECnet-Plus supports only those IDPs (initial domain parts) that specify the use
of binary syntax DSPs (domain-specific parts). IDPs that specify decimal syntax
DSPs are not supported.

5.2 Devices and Data Links

The following sections discuss operational notes about device support and data
links.

5.2.1 Receive Buffers Attribute on HDLC LINK Entity Not Implemented (Integrity servers and Alpha only)

Version 7.1   The receive buffers attribute of the hdlc link entity is not implemented in
DECnet-Plus. If you attempt to set the attribute according to the following
example, NCL displays the subsequent informational messages:

```
NCL>set node 0 hdlc link hdlc-0 receive buffers 8

Node 0 HDLC Link HDLC-0
at 2004-04-28-09:51:10.780-04:00I0.113

Command failed due to:
set list error
```

```
Characteristics
no such attribute ID: Receive Buffers = 8
```

HDLC (High-level Data Link Control) allocates the number of receive buffers that it requires; you cannot specify this setting.

5.2.2 FDDI Large Packet Support

Version 7.1   Phase IV nodes do not support FDDI large packets. If your node has an FDDI controller that uses large packets, routing selects a smaller segment size for Phase IV adjacencies. To communicate with Phase IV nodes, you must enable Phase IV addressing on the routing circuit. Verify that the `enable phaseiv address` attribute is set to `true` on one FDDI circuit in the SYS$MANAGER:NET$ROUTING_STARTUP.NCL file.

5.3 Transport Layer

The following sections discuss operational notes for the transports in DECnet-Plus.

5.3.1 NSP Characteristics for X.25 PVCs

Version 7.3   If a node has routing circuits of type `x25 permanent` you should set the NSP `flow control policy` characteristic to `no flow control`. In addition, if the call packet window size is 8 or less, you should set the NSP `maximum window` characteristic to 8. This lowers the number of NSP unacknowledged transmits and thus prevents the NSP out-of-order cache from filling.

5.3.2 NSP Flow Control Policy and DECnis and x25Gateway Routers

Version 8.2   In DECnet-Plus Version 6.3, several corrections were made to NSP flow control algorithms. Previous to these changes, if segment flow control was used flow control credits were sometimes improperly handled and the connections would appear to hang. The NSP software in DECnis routers and the x25Gateway product is based on the pre-DECnet-Plus Version 6.3 software. For this reason, whenever a connection is set up to one of these hardware products the NSP flow control should always be set to no flow control. Note that segment flow control is the default for NSP's `flow control policy` characteristic. Therefore, you must explicitly select NONE when running NET$CONFIGURE, use NCL to modify the running system, or edit the NCL startup script created by NET$CONFIGURE.

5.3.3 OSI Transport

Version 7.2   The following notes apply to OSI transport:

- If OSI transport times out during data transfer mode because the remote end is unreachable, the error SS$_CONNECFAIL may also be returned in the IOSB for the $QIO(IO$_READVBLK) or $QIO(IO$_WRITEVBLK) call. User code should handle SS$_TIMEOUT as well as SS$_CONNECFAIL.

- When defining an RFC 1006 address using the OSIT$NAMES logical name table, you must put a quotation mark around the address portion.

- The requirement against using 0 (zero) and 1 as valid NSELs (network selectors) has been removed, but the following restrictions apply:

  - The selector fields for OSI transport must be the same in both transport partners if the packet is traversing a backbone containing Phase IV routers (as opposed to routing vector domains).

— Although the cluster alias uses two ranges of network transport selector fields to reduce the risk of a collision, HP recommends that you do not choose values from those ranges, or at least that you do not choose the first few values in each range.

- The `osi transport` entity does not support a value of 0 for the `maximum remote NSAPs` (network service access points) attribute.

- The `osi transport template` entity does not support a value of `any` for the `network service` attribute. If this attribute is set to `any`, it is treated by OSI transport as `clns`.

5.4 Session Control

The following sections discuss operational notes about Session Control.

5.4.1 Transport Precedence in Predominantly Phase IV Networks

Version 7.3　　When using a Phase V node in a predominantly Phase IV network, the default for session control's `transport precedence` characteristic is {OSI,NSP}. This causes session control to attempt an OSI connection first, followed by an NSP connection. If you have a predominantly Phase IV network, this causes an unnecessary delay when connecting to Phase IV nodes. If the precedence is causing the delay, the delay is not seen when connecting in the reverse. To change the precedence, insert the following line at the end of the NET$SESSION_STARTUP.NCL file:

```
set node 0 session control transport precedence = {NSP,OSI}
```

Remember to reinsert this line if you run NET$CONFIGURE.

5.4.2 Session Control Back Translation Soft Links

Version 7.3–2　　Although the default for Session Control's `maintain backward soft links` characteristic is correctly documented as `false`, on OpenVMS systems the Session Control startup script always sets this characteristic to `true`.

5.4.3 Restriction When Using Applications Supported Using Cluster Aliases

Version 8.2　　Due to a design restriction, incoming ALIAS connections are forwarded to cluster members somewhat differently depending upon whether the SESSION CONTROL APPLICATION entity's ADDRESS set contains a NUMBER parameter (equivalent to Phase IV's connect by object number) or a TASK parameter (equivalent to Phase IV's connect by object name). For an incoming connect by object number, each ALIAS entity has access to a cluster-wide object number table that specifies which object numbers have been defined for each cluster member and the status of their INCOMING ALIAS characteristic. The result is that the connection forwarding mechanism works as expected, that is, connections are forwarded or not forwarded to cluster members correctly depending upon whether the application exists on the member and depending on the setting of the INCOMING ALIAS parameter.

However, the mechanism for mapping incoming connections by object name using this cluster-wide object number table does not exist and the result is that connections are forwarded to a given cluster member regardless of whether the application exists on a given member and regardless of the setting of the INCOMING ALIAS parameter on a given member. If you wish to restrict access to a network application supported using a cluster alias (either by not having the application present on a member or by setting the INCOMING ALIAS characteristic to FALSE on a member), you must create

the SESSION CONTROL APPLICATION by supplying the NUMBER keyword for the ADDRESS characteristic (that is, supplying the object number), so that connection forwarding works as expected.

5.5 Distributed Naming Service (DECdns)

The following sections discuss operational notes for DECdns.

5.5.1 Creating Clearinghouses When IP Address is Zero Causes DNS Server Hang

Version 7.3–2   Do not create a clearinghouse when the node's IP address is all zeros. You can determine if the address is zero by using the NCL command SHOW ADDRESS.

After each system boot, the local node's IP address is zero until the first incoming or outgoing OSI over TCP/IP or DECnet over TCP/IP connection occurs on the local node. At that time, the PATHWORKS Internet Protocol (PWIP) driver included with HP TCP/IP Services for OpenVMS provides DECnet-Plus with its IP address. Consequently, at least one OSI over TCP/IP or DECnet over TCP/IP connection must occur before attempting to create a clearinghouse.

An easy method to ensure that at least one OSI over TCP/IP or DECnet over TCP/IP connection has been made is to use the SET HOST command with the IP address of the local node. (If you don't know the local node's IP address, use the DCL SHOW LOGICAL *HOSTADDR command to display it.) The SET HOST command causes HP TCP/IP Services for OpenVMS to provide the local IP address to DECnet-Plus. Remember to use the NCL SHOW ADDRESS command to verify that the local node's IP address has been defined.

If fail to do this, you may have to delete the clearinghouse and start over after you have obtained a non-zero IP address.

If you try to use a clearinghouse with zero IP addresses in the towers it is likely that the DECdns server will hang.

5.5.2 Server Startup Delay

Version 7.3–2   There can be a delay in the startup of the DECdns server when the server is using DECnet over TCP/IP connections. This delay is due to the time required for the server to obtain a non-zero IP address from DECnet and the PATHWORKS Internet Protocol (PWIP) software. The IP address is initially zero until it is updated by DECnet and PWIP with the actual IP address for the node.

5.5.3 Delay in Node Name-to-Address Translations When DECdns Is Using DECnet over TCP/IP Connections

Version 7.3–2   When DECdns is using DECnet over TCP/IP connections, you may experience delays whenever DECnet has to translate a node name to a node address using the node's IP tower. These delays can occur when you are using NCL, when you invoke a DECnet application, or when you perform any other action that requires translating the node's name to its IP address.

The DECdns clerk, like any other DECnet application, uses DECnet to access the DECdns server. Currently, Session Control's `transport precedence` characteristic does not support a value for the IP tower. Therefore, Session Control always attempts to connect to the DECdns server using the NSP and OSI towers before trying the IP tower. After DECnet notifies DECdns that it cannot make a connection on a OSI or NSP tower, the DECdns clerk tries the IP tower.

_____ **Note** _____

This problem is especially noticeable in environments where a process
spawns multiple subprocesses, each of which performs a network
command. This is common in some batch environments.

_____

5.5.4 Problem Creating Clearinghouse Using DECnet over TCP/IP Connections

*Version
7.3–2*

When creating a new clearinghouse that joins an existing namespace in an
environment that uses DECnet over TCP/IP connections, it is possible to have
a clearinghouse created without the root directory. This is usually due to an
intermittent communications error during clearinghouse creation. This problem
occurs infrequently.

The current workaround is to force the creation of the root directory by issuing a
manual skulk command as shown below:

```
$ mcr dns$control
DNS>set dir . to skulk
```

5.5.5 DNS$CONFIGURE Option 4 Does Not Display IP Address

*Version
7.3–2*

Option 4 of the DECdns configuration program (DNS$CONFIGURE.COM) is
used to display a server node's address (as described in Section 10.5 of the *HP
DECnet-Plus for OpenVMS DECdns Management* manual). This option has not
been enhanced to display the node's IP address. As a workaround, use the NCL
show node [*node-id*] address command.

5.5.6 Limitation on Size of Checkpoint File Records

Version 7.3

The checkpoint file has a limitation of 500 blocks maximum on the size of
individual records. To detect any records over this limit or approaching this limit,
run the SURGEON "-scanrx" option. You will need to take corrective action if
you see a line indicating greater than 500 blocks and the number of records is
one (RECS: 1) because the server may bugcheck with a 902 error in the DB_
COMPRESSION.C module.

Records that exceed the 500 block maximum can be caused by an application
that is writing records larger than this limit or the garbage collector mechanism
(removes deleted records) is not running.

To correct the problem, apply one of the following actions:

• Use the SURGEON "-exciser" option to remove the offending records

• Use the recreate object command (if the garbage collector is not running).

If you have any questions about doing this, consult your HP representative.

Avoid the situation with the garbage collector not running by making sure all
your directories skulk to a success status and that the DNS$ALLUPTO date is
recent.

Use the following command in DNS$CONTROL to check the skulk status of all
directories in the namespace:

SHOW DIR ... DNS$SKULKSTATUS

Use the following command in DNS$CONTROL to check the DNS$ALLUPTO
date on all directories in the namespace:

SHOW DIR ... DNS$ALLUPTO

5.5.7 PAGEDYN Resources: Clerks and Servers

Version 7.1 DECdns clerk and server systems can require additional paged dynamic memory resources (PAGEDYN).

For DECdns clerk systems, consider increasing the PAGEDYN resource on the node if you see either the RESOURCEERROR or NONSRESOURCES error during skulk operations.

Before you configure a system as a DECdns server, check that the system has at least 50,000 free bytes of paged dynamic memory. Insufficient paged dynamic memory on servers can cause configuration errors, skulk failures, and in some cases normal clerk operations can fail, returning either the RESOURCEERROR or NONSRESOURCES error.

The DNS$SERVER.LOG file can also contain messages regarding failures caused by this resource.

Servers holding master replicas of directories that have many read-only replicas can also require additional paged dynamic memory.

5.5.8 Error Message Generated by DECdns Clerk During Startup

Version 7.1 The DECdns clerk startup might output the following error message:

```
create node 0 dns clerk known namespace CZ
```

```
command failed due to:
process failure
```

```
A Known Namespace with this name or NSCTS already exists
```

You can disregard this message. The DECdns clerk configuration procedure puts a `create dns clerk known namespace` command for the default namespace into the DECdns clerk NCL startup file. The command remains there in case the DECdns cache file has been deleted or corrupted.

5.5.9 Miscellaneous DECdns Operational Notes

Version 7.1 You might encounter the following DECdns problems:

- DNS$CONTROL might return `Syntax Error` if the clerk is disabled.

- You should not use DNS$CONTROL to modify the `DNA_NodeSynonym` attribute on DECnet node objects. DNS$CONTROL displays the attribute properly but does not modify it properly. Use the `decnet_register` node registration tool to modify DECnet data stored in DECdns.

- Re-created entries retain the case of the original entry name.

- If you have trouble creating a clearinghouse, make sure that both the `dns$server` account (user authorization file entry) and its default directory exist.

5.6 Distributed Time Service (DECdts)

The following sections discuss operational notes for DECdts.

5.6.1 Automatic Time Zone Changes on Rebooting Clusters

Version 7.1   If all members of a cluster are down when daylight saving time (DST) takes effect and automatic time zone changes are enabled, then members may reboot with the incorrect local time. If you anticipate that the cluster will be down during the change to or from daylight saving time, you should disable automatic time zone changes and make the changes manually.

5.7 OSAK Programming

The following sections discuss operational notes for the OSI Applications Kernel (OSAK) interface.

5.7.1 User Data Size Restriction for Tracing

Version 7.2   OSAK does not support tracing with user data buffers larger than 32,765 bytes.

5.7.2 OSAK Version 1.1 No Longer Supplied

Version 7.1   HP no longer provides the OSAK Version 1.1 interface.

If you use the OSAK Version 1.1 interface, you must migrate to the OSAK Version 3.0 SPI (session programming interface). The OSAK Version 3.0 SPI provides the same capabilities as the OSAK Version 1.1 interface.

For detailed information about the OSAK Version 3.0 SPI, see the *DECnet-Plus OSAK SPI Programming Reference* manual.

5.7.3 Migrating Applications from Version 2.0 to Version 3.0 OSAK API Interface

Version 7.1   Version 3.0 of OSAK includes a programming interface that is backwards compatible with the Version 2.0 programming interface. As a result of more rigorous conformance testing, some additional problems have been uncovered in the Version 2.0 interface.

As a result, applications built against OSAK Version 2.0 might encounter problems when using the Version 2.0 backwards-compatible interface in OSAK Version 3.0 if the applications contain previously untrapped application problems.

5.7.4 Misleading OSAK Error Message: SPM Congestion at Connect Time

Version 7.1   When OSAKserver receives an association request that specifies a nonexistent user identity, it generates the error message "SPM Congestion at Connect Time."

If you see this error, check that the user name and password specified in the request are correct. If the user name is correct but the password is incorrect, the OPCOM message %LOGIN-F-INVPWD is logged. If the user name is incorrect, no OPCOM message is logged.

5.8 DECnet Programming

The following sections discuss programming issues that apply to the DECnet programming interface.

5.8.1 64-Bit Virtual Address Restrictions

Version 7.1   You can use 64-bit virtual addresses only with $QIO operations on the NET: devices; you cannot use 64-bit virtual addresses with $QIO operations on the OS: devices.

For transparent task-to-task communication, the $ASSIGN system service accepts only 32-bit addresses and 32-bit descriptors for the DEVNAM parameter when it describes a network connect block (NCB). You can use non-transparent task-to-task operations when you want 64-bit descriptor addresses and 64-bit descriptors to specify an NCB.

5.8.2 Backtranslation of IP Addresses

Version 7.1   For IP addresses, session control returns the full name if the synonym is not available regardless of the Session Control Application Node Synonym setting. If neither the full name nor synonym is available, the `IP$aa.bb.cc.dd` format is returned.

If the system is configured to use IP addresses, you should prepare the application to receive a node name or address string longer than six characters in length even if `Session Control Application Node Synonym = TRUE` is specified for the application.

5.8.3 Applications Connection Requirement

Version 7.1   With DECnet-Plus, your application must wait for the completion of the $QIO system service call used to accept the connection before attempting to use the connection.