Software Product Description

PRODUCT NAME: HP TCP/IP Services for OpenVMS Version 5.6
SPD 46.46.21

DESCRIPTION

The HP TCP/IP Services for OpenVMS software product is the OpenVMS implementation of the industry-standard TCP/IP protocol suite and Internet services for OpenVMS Industry standard 64 (I64) and OpenVMS Alpha systems. The kernel software is ported from the Berkeley Software Distribution (BSD) Versions 4.3 and 4.4, with enhancements from HP.

TCP/IP Services installation is integrated with the OpenVMS installation. It provides interoperability between OpenVMS and other operating systems that support TCP/IP, such as UNIX® and Microsoft® Windows®. A comprehensive suite of functions and applications based on industry-standard protocols allow heterogeneous network communications and file sharing, as well as network services such as IP/multicasting, dynamic load balancing, remote login, network file access, remote terminal access, remote printing, email, application development, remote client booting, domain name system (DNS), and network time protocol (NTP).

TCP/IP Services operates in both IPv4 and IPv6 networks, as well as in mixed environments, and provides high availability, performance scalability for SMP systems, and secure authentication and data transfer for remote sessions, network applications, and email.

Licenses

For Alpha systems, the following TCP/IP Services for OpenVMS licenses are available:

License	Description
Server	Provides complete product functionality.
Client	Provides a subset of the server license. The client license does not include BIND, BOOTP, DHCP, failSAFE IP, TFTP, NFS server, PC-NFS, and the load broker.
Client upgrade	Provides a subset of the server license for customers who previously purchased a client license and now require full functionality.

For OpenVMS I64, the Operating Environment (OE) includes the TCP/IP Services for OpenVMS product and a server license for it.

Network Interface Layer Support

With support for multiple network interfaces for each physical network controller, the TCP/IP Services for OpenVMS software allows OpenVMS systems to connect to individual host computers on different types of networks:

- Ethernet for IPv4 and IPv6 (OpenVMS I64 and OpenVMS Alpha)

- Fiber Distributed Data Interface (FDDI) for IPv4 and IPv6 (OpenVMS Alpha only)

- Token Ring for IPv4 (OpenVMS Alpha only)

- Asynchronous transfer mode (ATM) for IPv4 (OpenVMS Alpha only)

Individual host computers can also connect with other hosts or networks over serial communications lines using either the Serial Line Internet Protocol (SLIP or CSLIP) or the Point-to-Point Protocol (PPP).

Note: SLIP is supported on Alpha systems only.

Internet Layer Support

The TCP/IP Services for OpenVMS product supports the following Internet layer protocols that work together to move data around the Internet:

- Internet Protocol (IP) provides a connectionless packet delivery service for IPv4 and IPv6.

- Internet Control Message Protocol (ICMP) provides diagnostic functions and handles error and control messages for IPv4 and IPv6.

- Address Resolution Protocol (ARP) dynamically maps an IP address to a physical hardware address for IPv4.

- Neighbor Discovery discovers neighbors in the same link, dynamically detects routers, dynamically maps all IP addresses to a physical hardware address for IPv6, and maintains information about the paths to active neighbors.

- Path MTU for TCP and UDP calculates the most efficient means of transporting data across a network.

- Classless Interdomain Routing (CIDR) reduces routing tables and makes more efficient use of the IP address space.

- Routing protocols and routing daemons enable gateways to exchange current routing information about hosts and directly connected networks. Supported protocols include:

  — Routing Information Protocol (RIP) Version 1 (RFC 1058) and RIP Version 2 (RFC 1388) for IPv4, and RIPng (RFC 2080) for IPv6

  — Open Shortest Path First (OSPF) Version 2 (RFC 1583) for IPv4

  — Exterior Gateway Protocol (EGP) (RFC 904) for IPv4

  — Border Gateway Protocol (BGP) (RFC 1163, RFC 1267) for IPv4

  — Router Discovery (RFC 1256) for IPv4

  — Routing daemons communicate with the kernel to add new routes or to delete or modify existing routes. The following routing daemons are supported:

    * ROUTED for IPv4

    * GATED for IPv4 [1]

    * *ip6rtrd* for IPv6

High Availability

- failSAFE IP supports IPv6

The failSAFE IP service provides higher availability of IP addresses by removing the NIC as a single point of failure. failSAFE IP is cluster aware, so standby IP addresses can be configured within the same node or across a cluster. Typical failures that failSAFE IP guards against include NIC failure, broken cable, failed port on a switch, and node shutdown.

Transport Layer Support

To provide either connection-oriented or connectionless data transmission between two hosts (local or remote), the TCP/IP Services for OpenVMS product supports both TCP and UDP protocols. These protocols form the bridge between the Application layer and the Internet layer:

- Transmission Control Protocol (TCP) provides reliable, connection-oriented, sequenced data transfers for applications that must guarantee delivery of the data.

- User Datagram Protocol (UDP) provides fast, connectionless data transfers for applications that do not require delivery confirmation.

The TCP Extensions for High Performance (RFC 1323), and the IETF Wireless TCP Standards help prevent congestion on low-bandwidth high-delay wireless and satellite networks. The wireless TCP set of standards encompasses TCP Extensions for High Performance (RFC 1323), SACK (RFC 2018), and Path MTU Discovery for IPv4 (RFC 1191) and IPv6 (RFC 1981).

Application Layer Support

The TCP/IP Services for OpenVMS product supports numerous Application layer protocols that allow OpenVMS users to:

- Run software on remote systems.

- Transfer data files between local and remote systems.

- Share remote system resources such as disk storage space and printers as if they were directly connected to the user's local system.

---

[1] The Enhanced Gateway Routing Daemon (GATED) is based on GateD Unicast Version 4.0.6, with advanced routing options.

- Send and receive electronic mail messages locally or across the worldwide Internet.

- Provide consistent, reliable, and efficient network services to all users on the Internet.

Remote Computing New Features:

- TELNET Upgrade with Kerberos Support

- TELNET Server Device Limit

With TELNET, an OpenVMS user can log in to remote hosts in the network. The TELNET features include:

- Simultaneous multiple sessions

- IBM 3270 model terminal emulation (TN3270)

- Support for both OpenVMS style and UNIX style interfaces

- Support for window sizing (rows and columns) and location options

- Kerberos authentication

The popular UNIX Remote commands, called R commands, let OpenVMS users work in accounts on remote internet hosts that are either UNIX or OpenVMS systems. The TCP/IP Services for OpenVMS software supports the RLOGIN, RSH, REXEC, and RMT/RCD commands.

In addition, the secure shell (SSH) command logs into a remote server and provides remote command execution using authentication and data encryption to ensure a secure connection.

The FINGER utility enables users to obtain information about each user on local or remote systems. This information includes user name, account name, and the program the user is running.

The X Display Manager Control Protocol (XDMCP) allows display devices to request that the login server present a login screen.

File Transfer

New Feature:

- FTP Performance Enhancements for VMS Plus Mode

OpenVMS users transfer data files between local and remote systems through the use of the following components:

- File Transfer Protocol (FTP) creates, deletes, and copies files and directories between hosts. FTP supports OpenVMS Extended File Specifications (long file names, deep directories, and extended character sets) for ODS-5 disks.

- Trivial File Transfer Protocol (TFTP) transfers files using the UDP protocol and no authentication and is typically used during the bootstrap process of diskless systems.

- The remote copy (rcp) command copies files between the local host and a remote host or between two remote hosts.

- The secure copy (SCP) and secure file transfer (SFTP) commands ensure secure file copy operations using authentication and data encryption.

Resource Sharing New Feature:

- IPv6 Support for LPD and TELNETSYM

The TCP/IP Services for OpenVMS software provides network printing services through the line printer/line printer daemon (LPR/LPD) and the TELNET print symbiont (TELNETSYM).

- LPD provides remote printing services for UNIX and OpenVMS client hosts through local and remote print queues. Once the system manager sets up the print queues, OpenVMS client users enter the DCL command PRINT, and UNIX client users enter the lpr command. LPD can be configured for cluster-wide availability, providing load balancing and automatic failover for LPD-controlled print queues on the OpenVMS host.

- TELNETSYM provides remote print services that enable the use of standard OpenVMS printing features not available with LPR/LPD.

Network File System New Features:

- NFS Client TCP Support

- NFS Server Support for Integrity

- NFS Symbolic Link Support

The Network File System (NFS) server software allows NFS client users to gain transparent access to remote file services. With NFS, when a user accesses files and directories from a remote system, they appear to reside on the local system regardless of operating system, hardware type, or architectural differences between the local and remote systems. The PC-NFS daemon provides authentication services to PC-NFS clients.

TCP/IP Services provides support for NFS Version 2 and Version 3 in the NFS server. The NFS client is limited to Version 2.

The NFS client is supported on OpenVMS I64 and OpenVMS Alpha systems. The NFS server is supported on OpenVMS Alpha systems only.

NFS supports IPv4 only.

The main benefit of NFS Version 3 is increased maximum file size—up to 1 terabyte for an OpenVMS file system and up to 4 gigabytes for a container file system. Performance gains may result from the improvements to file-size processing and the enhanced write performance that allows the NFS server to acknowledge a write operation before the files are actually written to disk. Afterward, the server's response to a commit message confirms that the data has been written to disk.

The NFS server supports communication over both TCP and UDP. NFS over TCP offers better support for file access over wide area links than UDP. The NFS client is limited to UDP only.

The NFS server and client support OpenVMS Extended File Specifications, including long file names, deep directories, and extended character sets on ODS-5 file structures.

Mail Services

- Secure IMAP (SSL support)

- Secure POP (SSL support)

With the Simple Mail Transfer Protocol (SMTP), OpenVMS users can send and receive electronic mail to and from local and remote hosts. The TCP/IP Services for OpenVMS implementation of SMTP uses the OpenVMS Mail facility, which automatically recognizes an SMTP host address in the format *smith@widgets.com*. SMTP provides support for SFF (Send From File) and outbound alias specification.

The following mail systems work with SMTP, providing reliable, server-based mail repositories for clients:

- Post Office Protocol (POP) server

- IMAP Mail server (Alpha systems only)

Note: Secure IMAP and Secure POP require the use of the HP SSL for OpenVMS software.

Network Services

New Features:

- BIND 9 Resolver

- DNS/BIND V9.3 Server

- NTP Security Update (SSL)

With the following TCP/IP Services for OpenVMS management components, network and system managers can provide consistent, reliable, and efficient services to their users with minimal interruption:

- Simple Network Management Protocol (SNMP) Version 2 includes a master agent and subagents that allow the OpenVMS system to be managed by a

management station on the network. SNMP supports IPv4 only.

- Network Time Protocol (NTP) Version 4 provides a means to synchronize time and coordinate time distribution throughout a TCP/IP network. NTP provides accurate and dependable timekeeping for OpenVMS hosts on TCP/IP networks.

- Berkeley Internet Name Domain (BIND) is a distributed database system that distributes and manages host information so that hosts do not need to locally manage the address of every other host on the internet. The BIND 9 server is based on the Internet Software Consortium's (ISC) BIND 9.2.1 implementation. It includes dynamic updates and BIND server cluster failover, which allows multiple BIND master servers to share a common database, thus providing both redundancy and a failover mechanism when one of the servers becomes unavailable.

The BIND server is based on the ICS's BIND 9.2.1 implementation, and supports IPv4 and IPv6.

The BIND resolver is based on the BIND 8.1.2 implementation. The BIND resolver supports communication over IPv4 only, but it is capable of querying for IPv6 addresses (AAAA records).

The BIND server and the BIND resolver are available on OpenVMS I64 and OpenVMS Alpha systems.

- Load broker supplies cluster load balancing, round-robin scheduling, and automatic failover.

- Metric server calculates and reports the DNS load on the local host. It includes dynamic configuration of logical names, which can be defined for CPU rating, compute interval, and debug level, as well as support for multihomed systems to allow load balancing of incoming traffic across multiple IP addresses.

- Portmapper allocates ports so that system managers do not need to preconfigure client applications with port numbers for each service.

- Auxiliary server process is the TCP/IP Services for OpenVMS implementation of the UNIX internet daemon (*inetd*). The auxiliary server greatly simplifies application writing, manages overhead by reducing simultaneous server processes, provides system security through authentication of service requests, and supports event and error logging.

- Dynamic Host Configuration Protocol (DHCP) is a superset of the Bootstrap Protocol (BOOTP). In addition to BOOTP functionality (answering bootstrap requests), DHCP offers robust configuration services, including IP address, subnet masks, and default gateways. The DHCP server can be configured to support BOOTP clients. If BOOTP is enabled without DHCP, DHCP functionality is not available.

- DHCP dynamically updates BIND using a feature that allows DHCP clients to be configured with a registered name. DHCP uses this name to assign an address when it updates the BIND database. In addition, this release offers both a DHCP client and server, which provides a centralized approach to the configuration and maintenance of IP address space. With DHCP server, the system manager can provide dynamic allocation of IP addresses from an OpenVMS host.

Security

New Feature:

- SSH Upgrade with Kerberos Support

The TCP/IP Services for OpenVMS product includes the secure shell (SSH) client and server, which provide secure login, remote command execution, and file transfer. TCP/IP Services for OpenVMS 5.6 includes SSH support for Kerberos, the popular network authentication protocol from the Massachusetts Institute of Technology. SSH password authentication method has been enhanced to support Kerberos.

Performance and Scalability

The TCP/IP kernel has been modified to provide increased performance on symmetric multiprocessing (SMP) systems.

This complete redesign of the TCP/IP kernel provides enhanced performance on SMP systems by removing CPU contention among users. The new kernel uses a dynamic spinlock to lock the main internal database. All processing that requires locking is directed to a designated TCP/IP CPU, thereby eliminating CPU contention with other CPU users. Essentially, network I/O becomes a series of asynchronous, transaction-based operations.

Management Control Program

The TCP/IP Services for OpenVMS product provides the Management Control Program, which is a comprehensive, easy-to-use network management tool based on familiar OpenVMS DCL command syntax. These commands let system managers configure and monitor the product components locally.

The flexible configuration process includes an interactive configuration procedure.

Startup and shutdown files are provided for individual services, allowing system managers to stop and start individual services without affecting the operation of the remaining TCP/IP Services software.

Support for both DCL or UNIX management commands provides a choice of methods for configuring and managing the network connections and the TCP/IP Services software.

UNIX Network Management Utilities

- TCPDUMP Version 3.8.3 for IPv4 and IPv6

The TCP/IP Services for OpenVMS product provides UNIX networking management utilities for system managers who are experienced in managing and troubleshooting the UNIX network subsystem. Supported utilities include:

- *arp*

- *finger*

- *ifconfig*

- *netstat*

- *ping*

- *ripquery*

- *route*

- *sysconfig*

- *sysconfigdb*

- *tcptrace*

- *traceroute*

- *tcpdump*

Subsystems can be configured in the *sysconfigtab* database.

Note that some UNIX flags and parameters may not be supported.

Error Message Documentation

The TCP/IP Services for OpenVMS product provides online help for error messages for TCP/IP facilities and components. The information is included as part of the OpenVMS Help Message utility (MSGHLP).

Application Programming Interfaces (APIs)

- *libpcap* for IPv4 and IPv6

The TCP/IP Services for OpenVMS product provides the following APIs for programmers to develop customized applications:

- Berkeley Sockets and Sockets Library provide UNIX like access for TCP, UDP, and raw IP to applications written in the C programming language. The library includes support for:

  — Both IPv4 and IPv6 basic socket interface extensions for IPv6 (RFC 2553 and IETF updates)

  — Advanced sockets API for IPv6 (RFC 2292 and IETF updates)

- The $QIO interface extends the OpenVMS system services for socket communications, providing access to TCP, UDP, and IP for applications written in supported programming languages.

- The SRI $QIO interface translates older, incompatible SRI $QIO interfaces into $QIO interfaces.

- ONC RPC provides an industry-standard, portable API for programmers who do not have an in-depth knowledge of networking protocols. This is an efficient alternative to application development using sockets.

- Extensible Simple Network Management Protocol (eSNMP) provides routines for building SNMP sub-agents.

PATHWORKS, Advanced Server, and DECnet over TCP/IP

The TCP/IP Services for OpenVMS product includes the PATHWORKS IP (PWIP) driver and the PWIP ancillary control process (PWIP_ACP) for improved Advanced Server and TCP/IP integration.

The PWIP driver allows communication between OpenVMS systems running either Advanced Server for OpenVMS or PATHWORKS, and TCP/IP Services software, as well as personal computers running PATHWORKS 32 client software. It also enables the DECnet-over-TCP/IP feature, which is included with the DECnet-Plus for OpenVMS software. (For more information, see the DECnet-Plus for OpenVMS documentation.)

INSTALLATION AND CONFIGURATION

System managers install the TCP/IP Services for OpenVMS product using the POLYCENTER Software Installation utility. A menu-driven configuration procedure makes it easy to enable either all components and services or only those needed.

HARDWARE REQUIREMENTS

Supported Processors

The TCP/IP Services for OpenVMS product supports central processing units (CPUs) running OpenVMS.

TCP/IP Services for OpenVMS Version 5.6 is supported on Integrity Servers and Alpha servers that are listed in the OpenVMS Version 8.2-1 SPD (SPD 82.35.02) and in the OpenVMS Version 8.3 SPD (SPD 82.35.08). (For VAX systems, use Version 5.3 of the TCP/IP Services for OpenVMS product.)

For a complete list of hardware products, see the Software Product Description (SPD) for the specific OpenVMS operating system release.

Required Network Controllers

The TCP/IP Services for OpenVMS software supports all network devices listed in the OpenVMS Operating System SPD.

The TCP/IP Services for OpenVMS software can share an Ethernet interface with other HP networking products such as DECnet-Plus for OpenVMS.

Memory Requirements

The minimum amount of memory required for the TCP/IP Services for OpenVMS product is the same as the requirement for OpenVMS Version 8.2 and Version 8.2-1. Refer to SPD 82.35.01.

Disk Space Requirements

The approximate amount of space required on the system disk to support the TCP/IP for OpenVMS software under the client or server license is 150,000 blocks. Actual sizes may vary depending on the system environment, configuration, and software options.

CLUSTER SUPPORT

The TCP/IP Services for OpenVMS product is fully supported when installed on any valid and licensed OpenVMS Cluster configuration.

SOFTWARE REQUIREMENTS

To qualify for a software support contract, the TCP/IP Services for OpenVMS Version 5.6 product requires one of the following OpenVMS operating system versions:

- OpenVMS I64 Version 8.3
- OpenVMS I64 Version 8.2-1
- OpenVMS I64 Version 8.2
- OpenVMS Alpha Version 8.3
- OpenVMS Alpha Version 8.2-1
- OpenVMS Alpha Version 8.2

Client access requires a system that supports the protocols specified by NFS Version 2 or Version 3, and all TCP/IP application protocols defined by the TCP/IP Request for Comments (RFCs).

For Systems Running XDMCP: DECwindows Motif for OpenVMS, Version 1.2-5 (or later)

DISTRIBUTION MEDIA

Media and documentation for the TCP/IP Services for OpenVMS product are available on the CD-ROM Software Library for OpenVMS.

- To order the DVD for OpenVMS I64, use order number BA322AA (HP OpenVMS I64 Foundation Operating Environment (FOE)). The TCP/IP Services for OpenVMS product is included in the FOE.
- To order the CD-ROM Software Library for OpenVMS for Alpha systems, use order number QA–03XAA–H8.

ORDERING INFORMATION

TCP/IP Services for OpenVMS I64

With OpenVMS I64 Version 8.2 and higher, the operating system software, layered product software (including TCP/IP Services), and documentation are delivered together in one media kit. One license is required for each active processor. For license options and order numbers, refer to SPD 82.35.01. For additional information about HP Operating Environments for OpenVMS Industry Standard 64 for Integrity Servers, see SPD 82.34.02.

TCP/IP Services for OpenVMS Alpha Server

Software Licenses: QL–0LXA*–**
Software Documentation: QA–0LXAA–GZ
Software Product Services: QT–0LXA*–**

TCP/IP Services for OpenVMS Alpha Client

Software Licenses: QL–0M2A*–**
Software Documentation: QA–0LXAA–GZ
Software Product Services: QT–0M2A*–**

TCP/IP Services for OpenVMS Alpha Client Upgrade

Software License: QL–0PHA*–**
Software Documentation: QA–0LXAA–GZ
Software Product Services: QT–0PHA*–**

The asterisk (*) denotes variant fields. For additional information about available licenses, services, and media, refer to the appropriate price book. This ordering information was valid at the time of release. Contact your HP representative for current ordering information.

SOFTWARE LICENSING

This software is furnished under license only. For more information about HP licensing terms and policies, contact your HP representative.

License Management Facility Support

The HP TCP/IP Services for OpenVMS product supports the OpenVMS License Management Facility (LMF).

For information about the License Management Facility, see SPD 82.35.01, or consult the OpenVMS documentation.

SOFTWARE WARRANTY

This software is provided by HP with a 90-day conformance warranty in accordance with the HP warranty terms applicable to the license purchase.

SOFTWARE PRODUCT SERVICES

A variety of service options are available from HP. For detailed information about the service options, contact your local HP office.

The product information in this SPD was valid at time of release. For current product information, contact your local HP office.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

© 2005 Hewlett-Packard Development Company, L.P.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

UNIX is a registered trademark of The Open Group.