vms Software

Software Product Description

PRODUCT NAME: VSI TCP/IP for OpenVMS (Early Adopter's Kit) **SPD DO-DVTSPQ-00A**

DESCRIPTION

This document addresses VSI TCP/IP V10.5 for VSI OpenVMS Early Adopter's Kit (EAK)

VSI TCP/IP for OpenVMS, the TCP/IP stack produced by VMS Software, Inc., is the VSI implementation of the industry-standard TCP/IP protocol suite and Internet services. VSI TCP/IP takes full advantage of OpenVMS's distinct architecture to implement lower-layer protocols such as TCP, User Datagram Protocol (UDP), and IP as executive images, focusing on minimal CPU loading and yielding peak performance. VSI TCP/IP observes close adherence to OpenVMS standards for command syntax, basic security, and compatibility with standard products.

VSI TCP/IP provides interoperability between OpenVMS and other operating systems that support TCP/IP. A comprehensive suite of functions and applications based on industry-standard protocols allow heterogeneous network communications and file sharing, IP/multicasting, dynamic load balancing, network file access, email, application development, domain name system (DNS), and network time protocol (NTP), and remote activities such as login, terminal access, printing, and client booting. VSI TCP/IP supports IPv4 and IPv6. It provides high availability, secure authentication and data transfer for remote sessions, network applications, and email.

FEATURES

At VSI TCP/IP's core are network services TCP, UDP, IP, and Internet Control Message Protocol (ICMP), TCP/IP programming interfaces, and utilities that make a system fully TCP/IP compatible. VSI TCP/IP also includes network management and monitoring utilities.

Fast, Efficient, Easy to Install and Operate

VSI TCP/IP features fast and efficient operation, designed and optimized for industry-standard servers. VSI TCP/IP supports the OpenVMS Communications Interface (VCI), an efficient system interface to the LAN drivers.

VSI TCP/IP components can be configured and operated independently. You can start and stop most components without rebooting the entire system and affecting other products. You can control most components in VSI TCP/IP by means of a single utility (IP CONFIGURE) that simplifies network management and allows you to manage VSI TCP/IP configuration and security.

VSI TCP/IP allows you to perform the following tasks:

- Start and stop network interfaces
- Configure network hosts dynamically
- Add and remove services
- Provide secondary addresses for cluster failover
- Display and modify routing tables
- Display network counters and connections
- Enable gateway and multicasting support

Configurable Software Services

VSI TCP/IP for OpenVMS features the following software services and utilities:

- SSH—Secure Shell (SSH) allows users to log into and execute commands on a remote system.
- FTP—File Transfer Protocol (FTP) networking services allow you to transfer files from one computer to another.
- TELNET—Virtual terminal services implement the TELNET and TCP/IP protocols, providing TELNET users with immediate access to any remote system that supports TCP/IP and TELNET, eliminating the need for dedicated terminals and serial ports.
- NFS Client and Server—Network File System services.
    - NFS client implements the client side of the NFS protocol, providing access to file systems on remote NFS servers.
    - NFS server implements the server side of the NFS protocol, allowing remote client NFS users to access file systems on an OpenVMS host.
- SMTP—Provides complete mail transfer networking services by implementing the TCP/IP and Simple Mail Transfer Protocol (SMTP) networking standards for OpenVMS systems.

Additional Features, Services, and Utilities

VSI TCP/IP provides these additional features, services, and utilities:

- Utilizes available supported hardware, LAN devices, and serial devices.
- Supports CIDR, as well as older Class A, B, C, and D (multi-cast) networks.
- Supports systems that have multiple interfaces (paired network interfaces) on a LAN by internally linking the interfaces together. If an interface fails, a linked interface can be used. If data is to be transmitted on an interface that happens to be busy, VSI TCP/IP assigns the data to the least busy linked interface for transmission.
- Allows concurrent use of LAN devices with DECnet, Local Area Transport (LAT), and Local Area VMScluster (LAVC) software.
- Supports transmission of IP datagrams over certain X.25 packet switching networks (known as IP-over-X.25) using the Packetnet System Interface (PSI) product. You can connect separate TCP/ IP LANs over packet switching data networks (PSDNs) or other X.25 WANs.
- Provides access to PING, TCPDUMP, NSLOOKUP, TALK, and other utilities. The TALK utility allows remote users to share terminal messages in split windows in real time. The TCPDUMP utility can track TCP packets by printing information contained in the packet headers.
- Provides multiple gateways, routing, and multicasting to maximize network efficiency.
- Provides a Dynamic Host Configuration Protocol 4.0 (DHCP-4) server that assigns IPv4 network addresses to hosts based on a local reusable pool. DHCP also supports groups of clients on remote subnets on your network via relay agents. You can configure local host addresses quickly without relying on outside sources. DHCP supports Dynamic DNS (DDNS; see RFC 2136). DHCP also includes Safe-failover support, which allows two servers (primary and secondary) to share a configuration and service client using the same address pool. The Safe-failover protocol guards against duplication of address assignments during network failures, even if the network is partitioned so the primary and secondary servers cannot communicate and are independently leasing addresses.

  The DHCP client resides on the system and dynamically sets the network configuration. The VSI TCP/IP DHCP client communicates with a DHCP server to get an IPv4 address and other configuration information. It uses this information to configure the network parameters of the system and to start the network.

Network Performance Features

VSI TCP/IP includes services that provide fast and efficient network operation, and help minimize downtime.

- *Gateway Routing Daemon*: VSI TCP/IP includes the Gateway Routing Daemon (GateD) that consolidates RIP, DCN Hello, EGP, BGP, OSPF, and the Router Discovery Protocol into one distributed routing service. GateD supports route and protocol masks, and includes a flexible configuration language similar to C.
- *Routing*: VSI TCP/IP includes routing and gateway capabilities for WANs and complex LANs.
- *Dynamic TCP/IP Load Balancing*: The Domain Name Service supports dynamic TCP/IP Load Balancing, primarily for TCP-based applications such as TELNET. This allows the least-loaded systems running VSI TCP/IP in a TCP/IP cluster to appear first in response to DNS host name requests. A TCP/IP cluster can include independent systems, hosts anywhere, and several OpenVMS clusters, provided they have TCP/IP connectivity.
- *Cluster Alias Failover*: Cluster Alias Failover lets one node in a cluster take over incoming connection requests from a client system if the servicing node goes down. Cluster Alias Failover is used primarily for UDP applications, such as NFS. However, you can also use Cluster Alias Failover with TCP applications, such as FTP and TELNET, to establish a connection to the server.

NETWORK SERVICES SUPPORT

Berkeley R Commands and Services

VSI TCP/IP incorporates the Berkeley remote access commands (“R” commands). These UNIX client and server facilities allow remote access to hosts in a TCP/IP network. They include the RLOGIN remote login command and the RSH remote execution command.

Local users can back up their files on remote magnetic tape using the RMT client. Remote users can back up their files on local magnetic tapes using the RMT server.

VSI TCP/IP supports RCD. Using RCD, local users can access remote CD-ROM drives as if they were local drives.

Path MTU Discovery

Support for Path MTU Discovery improves performance when large packets of data are sent over TCP. Path MTU Discovery causes TCP to segment data into the largest datagrams that can be transmitted to the remote host without fragmentation along the path.

DECwindows Transport Interface

VSI TCP/IP’s DECwindows transport interface lets you run DECwindows applications on remote workstations running TCP/IP, and X Window System applications on local Alpha and Integrity workstations.

X Display Manager Server

VSI TCP/IP provides an X Display Manager (XDM) server to manage remote X terminals. When an X display starts, it communicates with the XDM server through the UDP-based X Display Manager Control Protocol (XDMCP). The XDM server creates a DECwindows login process, which then prompts remote X display users to login and create a DECwindows session.

Domain Name Services

VSI TCP/IP provides the Domain Name Services (DNS) that implement the Berkeley Internet Name Domain (BIND) server standard, version 9.9.10-P3. You can configure DNS for a client or server. DNS includes Dynamic DNS (DDNS), updates, DNS notify support, and enhanced control. With DNS notify support, the primary server notifies the secondary servers when zone changes occur, and the secondary server can then immediately initiate zone transfers rather than wait for the polling interval to expire. Split views allow a single server to present different translations to Internet (external) and internal users.

Terminal Server Print Services

The Terminal Server Print Services allow system managers to configure the print queues using standard OpenVMS printer operations, including the autostart feature. Users have access to IPv4 terminal server-based printers plus printers that connect directly to Ethernet as they would to any other OpenVMS printer.

Line Printer Services (LPS)

VSI TCP/IP implements the client and server ends of the BSD 4.4 Line Printer Protocol for various print devices connected to LPD servers and connected directly to the network.

Using LPS you can do the following:

- Print local files on remote printers.
- Remove print jobs from remote queues.
- Display job status in remote print queues.

LPS supports the PRINT command and includes the LPD server.

IPP Print Symbiont

The IPP print symbiont is an OpenVMS print symbiont working with the OpenVMS printing subsystem to implement an IPP client. It allows printing over a network to printers and servers that support the IPP v1.0 network printing protocol. The user interface is similar to other print symbionts in that it uses PRINT commands or system library calls to submit jobs to print queues. The IPP protocol has specific qualifier values and queue settings that must be present to allow the symbiont to function.

SNMP Services

SNMP Services implements the agent (server) end of the Simple Network Management Protocol (SNMP). The agent supports management objects defined in the SNMP Management Information Base (MIB II), plus sub-agents serving private MIBs using an API.

SNMP Multiplexing (SMUX)

The SNMP Multiplexing (SMUX) protocol is an SNMP subagent extension protocol. Each subagent or peer registers a MIB sub-tree with the SNMP Agent. Requests for objects residing in a registered MIB sub-tree are passed from the SNMP Agent using the SMUX protocol to the subagent. The subagent passes the result of an SNMP query back to the SNMP agent.

SNMP Agent X

Agent X is a standardized protocol allowing the list of managed objects available from an SNMP agent to be dynamically extended. By using Agent X directly, writers of TCP/IP services can allow the state of the service to be queried and controlled remotely. This can be useful if the service does not have a user interface, or runs under batch, or as a detached process. HPE Insight Management Agents use the SNMP extensibility provided by Agent X to allow remote examination and notification of system conditions that may need attention.

Network Time Synchronization Facilities.

VSI TCP/IP supports time synchronization between network hosts through the use of Network Time Protocol version 4. NTPv4 is backwards compatible with prior protocol versions back to version 2, and version 1 in client/server mode. This allows other nodes in the network to be upgraded at a different time with minimal disruption.

Master Server Process

The master server process invokes many server processes, which are present when a connection is active. The master server also performs the following functions:

- Logs all activity for security monitoring
- Invokes user-written server processes
- Restricts access to services based on the source Internet address

DECnet over IP

DECnet over IP permits two machines running DECnet to communicate using IPv4 links by using TCP/IP's DECnet Application Services. This is an important service for TCP/IP WANs that might link several local sites running DECnet with others that run only TCP/IP.

Multicasting

VSI TCP/IP supports full Class D IP multicasting (IGMP V2 with fallback to IGMP V1) to host groups. Multicasting support is available for the UCXDRIVER, INETDRIVER, and Socket Library programming interfaces.

PROGRAMMING SUPPORT

Socket Library

VSI TCP/IP provides a socket library of C routines (also accessible from other high-level languages) to facilitate application development. These routines support the UNIX socket functions for raw, stream, and datagram sockets. Socket library calls include socket and lookup operations, and byte order and Internet address conversion functions, and AF_UNIX socket routines.

QIO Programming Interface

VSI TCP/IP provides a QIO interface for use by application programmers who want to develop their own networking programs using the TCP, IP, and UDP protocols. The QIO interface includes operations used to open and close connections or ports, and to transfer data over a connection or port. All high-level languages can use this interface.

Compatibility with HPE TCP/IP Services for OpenVMS

VSI TCP/IP is compatible with HPE's TCP/IP Services for OpenVMS, allowing applications written for products such as DECwindows and DECmcc to run transparently on top of VSI TCP/IP. The BG software device is the interface, providing the lowest level of user interface to the TCP/IP stack.

INETDRIVER Services

VSI TCP/IP provides the INETDRIVER Services that support the Stanford Research Institute (SRI) QIO interface. This provides a one-to-one mapping between the UNIX socket functions and the OpenVMS $QIO system services.

RPC Programming Services

RPC Services is a software development tool based on version 4 of Remote Procedure Calls (RPC) developed by Sun Microsystems, Inc. VSI TCP/IP supports the C Socket Library. RPC Services include:

- A shareable runtime library
- RPCGEN compiler
- TCP and UDP synchronous transports
- Broadcast RPC and batch RPC
- RTL and XDR routines

Enhanced Security Features

VSI TCP/IP network security features prevent unauthorized use of systems, services, and network information, providing data protection and security over the network.

VSI TCP/IP offers the following types of security services:

- Secure Shell (SSH) v2 client and server
- SSH Publickey Assistant
- Secure Copy Protocol v2 (SCP2)
- Secure File Transfer Protocol (SFTP) server and client
- Outgoing and incoming access restrictions
- Packet filtering
- Kerberos V5 Telnet server and client
- IP Security with the Racoon key exchange daemon
- FTP over TLS
- Intrusion Prevention System (IPS)

Secure Shell (SSH) v2

The VSI TCP/IP SSH v2 implementation is based on the V2 protocol and the WRQ Reflection for Secure IT 6.1.0.16 code base. While SSH v2 is generally regarded to be more secure than SSH v1, both protocols are offered by VSI TCP/IP. Although the protocols are incompatible, they may exist simultaneously on a VSI TCP/IP system. The VSI TCP/IP server front-end identifies what protocol a client desires to use, and will create an appropriate server for that client. The SSH2 server and client are compiled from unaltered cryptographic source that is FIPS 140-2 Level 2 compliant.

The client and server together, using the Diffie-Hellman key-exchange method, determine a 256-bit random number to use as the session key. This key is used to encrypt all further communications in the session.

SSH v2 supports the multiple encryption algorithms 3DES (the default), TWOFISH, BLOWFISH, DES, CAST-128, and ARCFOUR.

SSH v2 includes the following server system authentications: host-based, public-key, password, keyboard interactive and Kerberos.

SSH functionality has been extended to include the following:

- *Diffie-Hellman-group14-sha256* (RFC 4250). This addition improves security of the key exchange by using a hash with more bits.
- *Elliptic curve Diffie-Hellman (ECDH) key agreement [RFC 5656].* Curves are: nistp256, nistp384, nistp521. The curve chosen will be sufficient to support the hash for the host keys involved. For example:
  - If the host key is ECDSA-nistp521, only the curve nistp521 will be available.
  - If the host key is ECDSA-nistp384, the curves nistp384 and nistp521 will be available.
  - If the host key is ECDSA-nistp256, the curves nistp256, nistp384 and nistp521 will be available.
- *Elliptic curve digital signature algorithm (ECDSA) [RFC 5656]*. Public keys are written in a format close to what is used by OpenSSH; OpenSSH public keys can be read as-is. The "Subject" and "Comment" lines in the key may need to be removed to make the keys readable by OpenSSH. ECDSA supports curves nistp256, nistp384, nistp521.
- *Advanced Encryption Standard running in Galois/Counter Mode (AES-GCM) [RFC 5647].* AES-GCM was modified by OpenSSH to resolve a potential ambiguity because the encryption and message authentication are both provided by a single algorithm. In this case the ciphers are named: aes128-gcm@openssh.com, aes256-gcm@openssh.com
- *New MACs: SHA-256, SHA-384 and SHA-512 [RFC 6668]*. These can be used with any ciphers, except the gcm ciphers, which provide both encryption and MAC functionality.

Secure Shell (SSH) v1 Client and Server

NOTE: VSI recommends use of SSH2, which is considered more secure than SSH1. With VSI TCP/IP SSH (Secure Shell) v1 you can log into and execute commands on a remote system. It replaces rlogin, rshell, and TELNET programs, and provides secure encrypted communications between two untrusted hosts over an insecure network. X11 connections and arbitrary TCP/IP ports can be forwarded over the secure channel. SSH connects and logs into the specified hostname.

The VSI TCP/IP SSH v1 implementation is based on the version 1.3.7 protocol. The Secure Shell daemon (SSHD) is the daemon program for SSH v1 that listens for connections from clients. When the SSHD daemon starts, it generates a server RSA key (normally 768 bits) that is regenerated every hour (the time may be changed in the configuration file) if it has been used, and is never stored on disk. A new daemon is created for each incoming connection. The multiple encryption algorithms supported by SSH v1 are IDEA (the default), DES, 3DES, BLOWFISH, and ARCFOUR.

A client program (SSH) is provided with VSI TCP/IP, but any SSH client that uses SSH v1 protocol may be used to access the server. Example programs are FISSH and VSI TCP/IP SSH on OpenVMS systems, and TTSSH, SecureCRT®, F-Secure SSH Client, and PuTTY on Windows®-based systems.

SSH v1 offers the following server system authentications: rhosts, rhosts-rsa, rsa challenge-response, and password.

SSH v1 and v2 offer break-in and intrusion detection, session termination, X11 forwarding, and port forwarding.

SSH Publickey Assistant

The public key assistant can be used to add, remove, and list SSH v2 public keys that are stored on a remote server.

CMPCLIENT

Allows you to enroll certificates by connecting to a CA (certification authority) and using the CMPv2 protocol for enrolling a certificate. You may supply an existing private key when creating the certification request or allow a new key to be generated.

CERTVIEW

Allows you to view and validate certificates, and, optionally, to output the information from a certificate that is formatted correctly to use when creating the SSH certificate mapping configuration.

CERTTOOL

The CERTTOOL utility is used for different needs concerning X.509 certificates in PKCS#10 and PKCS#12 format.

For PKCS#10, CERTTOOL creates certificate requests, allowing you to specify specific keyUsage and extended-KeyUsage flags.

For PKCS12, CERTTOOL creates a PKCS#12 package containing any number of private keys and certificates. The final PFX package is encoded with an HMAC and by default contains one password-protected safe, which contains all the other objects in an unshrouded format.

Secure Copy Protocol v2 (SCPv2)

SCP2 is an evolving file transfer protocol; not all implementations will offer all levels of functionality. The basic functionality is binary file transfers. VSI TCP/IP supports BINARY and ASCII transfers with SCP2, and will also transfer VMS file characteristics when the remote system has the capability. When operating with systems that do not support the full range of transfer mechanisms that VSI TCP/IP offers, VSI TCP/IP uses various methods to improve the chances that files will be useful upon transfer.

VSI TCP/IP uses the defined extensions in the protocol to transfer information about the OpenVMS file header characteristics such that when a file is transferred between two OpenVMS systems running VSI TCP/IP V10.5, the file header information is also transferred and the file has the same format on the destination system as it had on the source system. Also, when a file is transferred to a non-OpenVMS system, a method has been provided to translate those files that can be translated into a format that will be usable on the remote system. Files that are transferred from non-OpenVMS systems are stored as stream files on the OpenVMS system, which provides compatibility for text files from those systems.

Secure File Transfer Protocol v2 (SFTP2)

SFTP2 is an FTP-like client that can be used to transfer files over a network. SFTP2 transfers the files through ssh2 connections to ensure that the file transport is secure. In order to connect using SFTP2, you need to verify that sshd2 is running on the remote host to which you will connect.

SFTP2 is an evolving file transfer protocol; not all implementations offer all levels of functionality. The basic functionality is binary file transfers. VSI TCP/IP supports BINARY and ASCII transfers with SFTP2, and also transfers OpenVMS file characteristics when the remote system has the capability. When operating with systems that do not support the full range of transfer mechanisms that VSI TCP/IP offers, VSI TCP/IP uses various methods to improve the chances that files will be useful upon transfer.

FTP over TLS (FTPS)

FTPS allows you to establish a secure, encrypted connection to the FTP server for user authentication. File transfers can also be secured at the user's option. FTPS offers better performance than SFTP because only a single process is used to encrypt and transfer the data. FTPS provides a more reliable interchange of files between dissimilar systems because it uses the well-developed FTP protocol.

Advanced Packet Filtering

Packet filtering restricts the datagrams a network interface can receive. You can filter datagrams by protocol (IP, ICMP, UDP, or TCP), by source and destination address, or source destination port (UDP and TCP). In VSI TCP/IP V10.5, the packet filter definition files are fully IPv4 and IPv6 aware.

Intrusion Prevention System (IPS)

Components of VSI TCP/IP, including SSH, FTP, SNMP, SMTP, TELNET, IMAP and POP3 have been instrumented to report failures (known as events) such as invalid login attempts, etc, to a central filter server.

The filter server correlates reported events via rulesets and may implement a packet filter on an interface based on the results of the event correlation. This can be based on either the source address, essentially blocking all traffic of a particular protocol (e.g., IP, UDP, etc.) from a system, or on the destination address and port, blocking traffic only to that port.

Rules may be implemented to exclude certain source networks or addresses from event correlation, or to apply event correlation with different parameters, allowing the same rule to be applied differently. For example, a rule can be implemented for internal versus external network traffic.

An API is supplied so that VSI TCP/IP users may incorporate this event reporting into their own applications, as well as implementing the corresponding rulesets for event correlation for their applications in the filter server.

IP Security (IPSEC)

IPSEC is standards-based technology that provides a secure tunnel for transmitting data through an unsecured network, such as the Internet. IPSEC's authentication header (RFC 2402) and IPSEC Encapsulation Security Payload (RFC 2406) are supported in transport mode, which secures packets between any compliant hosts. Internet Key Exchange (RFC 2409) allows systems to establish and maintain encryption keys in a secure environment.

Kerberos V5 Telnet Server and Client

VSI TCP/IP V10.5 provides strong authentication for client/server applications using secret-key cryptography. After a client and server have used Kerberos V5 to prove their identity, they can encrypt all of their communications to assure privacy and data integrity. Kerberos V5 requires VSI Kerberos.

Classless Inter-Domain Router (CIDR)

CIDR allows expansion of the available IPv4 addresses to alleviate scaling problems such as exhaustion of Class B network addresses and backbone routing overload. This feature implements CIDR RFC 1517, 1518, and 1519. Use of variable-length subnet masks with CIDR solves these problems by allowing the user to supernet and aggregate address assignments.

Gateway Routing Daemon (GATED)

GATED is based upon GATED Release 3.5 from Cornell University and contains support for CIDR and OSPF. GATED provides dynamic routing information in order to determine the best path to use between a source and destination host. It is more efficient than static routing, because the system administrator does not have to update a host's or gateway's routing table manually. GATED determines the best route for a packet to travel by gathering and using various standard routing protocol information from OSPF (Open Shortest Path First), RIP2 (Routing Information Protocol), route discovery, and others.

IPv6

VSI TCP/IP 10.5 can operate as an end node in an IPv6 network as well as an IPv4 network. IPv6 services are available to both IPv6 and IPv4. DNS Resolver, SMTP, POP3, IMAP, LPD, stream printing, FTP, Telnet, SSH, NTP, CharGen, Discard, Echo and Daytime support IPv6. IPv6 packets can be transmitted over Ethernet interfaces or tunneled through an IPv4 network.

FTP

FTP provides TCP/IP File Transfer Protocol (FTP) networking services that allow users to transfer files from one computer to another. The number of simultaneous connections to FTP is limited by the available system resources. FTP supports RFC 4217 - Securing FTP with TLS, which allows you to log in over an encrypted connection and to transfer data over an encrypted connection.

Client and Server Support

FTP supports a File Transfer Protocol client and server. You can transfer files in both directions between local and remote systems that implement the TCP/IP and FTP protocols. The FTP client uses SRI encoding for filenames.

OpenVMS and UNIX Commands

Use the command line interface to initiate file transfers using native OpenVMS commands or equivalent UNIX-style commands, either interactively or with command procedures.

Session Accounting and Statistics

VSI TCP/IP records accounting information from services that have been enabled, such as FTP and SMTP. The accounting data includes information about when a network session took place and how much data was transferred. Use the SERVER-CONFIG tool to enable the ACCOUNTING facility. The facility reads the file VSI TCP/IP:ACCOUNTING.CONF for additional configuration information.

Full File Protection and Security

FTP uses maximum OpenVMS file protection for each user. You can limit access for ANONYMOUS users or CAPTIVE accounts. Network managers can log all attempted connections to a local host. FTP supports token authentication and full OpenVMS break-in detection and evasion.

Ease of Use

FTP provides the same environment to remote users as if they were logged in locally and supports many features to make file transfers easy:

- Multi-line recall of up to 20 lines
- Startup command files
- Automatic file transfer format determination
- Record structure transfer support
- STRU O VMS and VMS PLUS server support. These compatibility modifications to FTP file transfer mechanisms preserve OpenVMS file characteristics when a file is transferred to between systems running VSI TCP/IP.
- Multi-homed hosts support. If Client-FTP needs to reach a host that has multiple internet addresses, it tries all possible addresses
- Centralized logging
- Records accounting information from enabled services
- IPv6 support with the EPRT and EPSV commands

NFS Client

NFS client implements the client side of the Network File System (NFS) protocol, providing access to file systems on remote NFS servers. Authorized users on the local system have transparent access to remote NFS servers.

File System Mount Flexibility

Users can obtain access to remote file systems by mounting them. The client provides flexibility so you can mount any level of the NFS Server Filesystem directory structure onto any level of the Client File system directory structure, subject to OpenVMS Record Management Services (RMS) restrictions.

Complete File Protection

The client fully supports system, directory, and file protection. Access confirmation to NFS files is through user ID mappings. You can add mappings with the NFS-CONFIG utility. The client supports Network Lock Manager as well as the standard file locking and sharing protocols.

File Format

The VSI TCP/IP client adheres to NFS file organization and record format specifications so that you can write files back to the VSI TCP/IP server. The client preserves file structures across the network, and maintains file attributes the NFS protocol does not address by using companion data files in FDL (File Description Language) format. Automatic format handling treats existing UNIX files as sequential, variable-length, carriage-return-carriage-control files on an OpenVMS system.

Filename Mapping

While OpenVMS uses different conventions for naming files from those on an NFS server, special characters are not rejected. Instead, the client maps file name characters between the operating systems. Users in each environment can continue to use the naming conventions to which they are accustomed, subject to the RMS restrictions on file name length.

Flexible Command Interface

You can mount file systems and display mount information interactively at the DCL or VSI TCP/IP level or by using command procedures. Command syntax is convenient and straightforward, and is documented in the VSI TCP/IP Administrator's Reference manual.

NFS Server

NFS server implements the server side of the NFS protocol, providing access to file systems on an OpenVMS host to remote client NFS users. The NFS server lets your network share data among different systems. This minimizes hardware costs by eliminating data duplication. The server supports NFS over UDP and TCP, and can also export files to VSI TCP/IP NFS client systems.

File Operations

The NFS server supports all normal file operations, even those on multi-volume disks, including these:

- Create or remove directory
- Create, remove, or rename file
- Got or set attributes
- Get file system statistics
- Look up file or read directory

NFS clients can use the server system's files as if they were local files. The server supports the MOUNT and Port Mapper protocols and operations. It also supports symbolic links and hard links.

System resources are the only limitations to the number of simultaneous users. A multi-threaded architecture provides fast, high-performance service for many clients, while keeping processor overhead to a minimum.

Complete File Protection

The server fully supports system, directory, and file protection. Access to OpenVMS files is restricted to preapproved clients named in an NFS configuration database that maps between NFS UID/GIDs and OpenVMS user accounts. The server uses the OpenVMS UIC and user access rights to validate all file access.

To further increase security, the network administrator can assign rights identifiers to NFS users, restrict remote mounts to superusers only, and track attempted access violations.

ODS-5 for NFS Server

This feature allows for long filenames and a mixed-case naming convention.

File Format

The VSI TCP/IP server allows VSI TCP/IP clients to read OpenVMS files in their most commonly used formats, including sequential, variable-length, and variable with fixed-length control (VFC), without having to manually convert these files. You can use OpenVMS disks for information sharing as well as file storage.

Filename Mapping

While OpenVMS uses different conventions for naming files from those on an NFS client system, special characters are not rejected. The server maps file name characters between the operating systems. Users in each environment can continue to use the naming conventions to which they are accustomed, subject to the RMS restrictions on file name length. NFS Server supports these standard protocols for file sharing:

- **UNIX Support Protocols**: The server supports the Network Lock Manager and Status Monitor RPC protocols. These provide advisory UNIX System V locking and PC file sharing. This lets you coordinate access to file and file records using standard methods in a distributed environment.
- **PC Support Protocols**: The server supports the PCNFSD protocol, providing PC users with access to OpenVMS file systems and the ability to use OpenVMS print queues.
- **Performance Tuning**: The server generates statistics and optionally logs security violations, MOUNT requests, errors, and other activities to help you tune the performance of the NFS server system. Tuning parameters control such things as datagram sizes, cache sizes, and the number of server threads.

SMTP

SMTP provides complete mail transfer networking services by implementing the TCP/IP and Simple Mail Transfer Protocol (SMTP) networking standards for OpenVMS systems. You can implement mail rejection rules, necessary for blocking mail relaying and adding anti-spamming capabilities to VSI TCP/IP. You can also deliver files as base64-encoded MIME messages by way of VMSmail. SMTP also records accounting information from enabled services (see the FTP section for details). With SMTP, any user can be the postmaster. SMTP can also function as a gateway between SMTP and DECnet and foreign mail products.

SMTP Client and Server Support

SMTP provides an SMTP client and server. Users on a system running SMTP can send mail messages to and receive mail messages from users on systems that support SMTP and TCP/IP.

IMAP4 Server

The Internet Message Access Protocol (IMAP) server lets the mail program of your IMAP-compliant client access remote message storage as if the storage were local. This implementation is based on IMAP version 4, revision 1. IMAP4 and the Post Office Protocol (POP3), described in the next section, operate differently. IMAP4 retains the message on the server, while POP3 retrieves the message and stores it offline on the client, thus deleting it from the mail server. IMAP4 allows you to access your mail from more than one client workstation simultaneously.

POP3 Server

The Post Office Protocol version 3 (POP3) multi-threaded server allows users on remote hosts (such as PCs) who do not want to maintain their own message transport systems to retrieve mail from an OpenVMS MAIL server's incoming mailbox.

Transparent User Interface

Users have a transparent interface to the SMTP messaging system from within the OpenVMS MAIL utility. All features of OpenVMS MAIL message processing are available, such as these:

- All OpenVMS MAIL commands, including SET FORWARD
- Alias names, mailing lists, and special mail headers
- Distribution name lists
- Automatic notification of incoming mail
- Reading incoming mail using OpenVMS MAIL
- Carbon copy (CC:) recipients

Store, Forward, and Relay

SMTP notifies users automatically of incoming or undeliverable mail, defers mail delivery to unavailable hosts, and can forward mail to a central mail-handling system. You can forward all mail or only mail with unknown addresses to the central mail-handling system.

ARPA Standard Message Formats

SMTP supports standard message formats and addresses used in the ARPA Internet community.

Mail Exchanger (MX) Records

SMTP uses mail exchanger (MX) records on systems using DNS. MX records specify which hosts can accept mail for a domain. If the first attempt to deliver mail fails, SMTP tries each MX record until it finds a host that can accept the mail.

Performance Tuning

You can set parameters at runtime to customize and enhance SMTP performance. These parameters include:

- Connection timeout value
- Delivery check and retry intervals
- Maximum message life

TELNET

TELNET provides complete virtual terminal networking services to OpenVMS systems by implementing the TELNET and TCP/IP protocols. TELNET users have immediate access to any remote system (such as UNIX and ULTRIX) that supports TCP/IP and TELNET, eliminating the need for dedicated terminals and serial ports.

Client and Server Support

TELNET provides a TELNET client and server. Users on a VSI TCP/IP system can log in to remote systems, and users on remote systems can log in to a VSI TCP/IP system via TELNET.

Designed for Efficiency

Server-TELNET is ideal for high-bandwidth applications. VSI TCP/IP implements the server as an OpenVMS device driver, operating with minimal CPU overhead. Server-TELNET performs processing within a port driver for the TTDRIVER class driver. This makes the server a standard OpenVMS terminal device, fully compatible with all TTDRIVER QIOs.

Permanence of NTY Devices

TELNET provides the option to permanently assign NTY devices, making NTY setup and operations similar to LAT outgoing connections.

Full Password Protection (Kerberos)

TELNET supports Kerberos V5 authentication and encryption via the KTELNET_SERVER. KTELNET_SERVER is configured to run with the LOADABLE_KTELNET_CONTROL image invoked from the Master Server. KTELNET_SERVER uses FTA devices instead of NTY devices.

OpenVMS and UNIX Commands

You can use native OpenVMS commands or a UNIX-style command interface for many VSI TCP/IP commands.

.

TELNET Protocol Options

TELNET supports the TELNET protocol options BINARY, ECHO, END-OF-RECORD, SUPPRESS-GOAHEAD, TERMINAL-TYPE, and TRANSMIT-BINARY.

Additional Features

TELNET offers the following additional features:

- Multi-line recall of up to 20 command lines
- Startup command files
- OpenVMS process spawning
- Control character mapping
- Interactive, online help
- Support for multi-homed hosts. If Client-TELNET needs to reach a host that has multiple internet addresses, it tries all possible addresses
- Support for X Display Location option to set the user's current X display location on the remote end
- Support for the Remote Flow Control option for disabling ad enabling flow control

HARDWARE REQUIREMENTS

VSI TCP/IP runs on any Integrity system capable of running the VSI OpenVMS Integrity Operating System Version 8.4-2L1 or higher.

Refer to the latest VSI OpenVMS Integrity Software Product Description for information about supported servers.

Disk Space Requirements

Disk space required for kit installation:	500,000 blocks
Disk space required for use (permanent):	5,000 blocks for configuration and related system files, and 500-1000 blocks per user of key files and/or log files

These counts refer to the disk space required on the system disk. The sizes are approximate. Actual sizes may vary depending on the user's system environment, configuration, and software options.

SOFTWARE REQUIREMENTS

Please note the following prerequisites for VSI TCP/IP V10.5. For additional information, refer to the VSI TCP/IP Installation and Quick Start Guide.

- On Integrity servers, VSI OpenVMS Integrity Version 8.4-2L1 or higher is the required operating system version for this product.
- You must perform a fresh installation of VSI TCP/IP V10.5. No upgrade paths are available.
- You must install the VSI OpenVMS patch kit, VMS842L1I_CLUCONFIG-V0100.PCSI$COMPRESSED prior to beginning the VSI TCP/IP V10.5 installation. If this patch kit is not installed, the VSI TCP/IP 10.5 installation procedure will terminate.
- For compatibility with VSI TCP/IP V10.5, VSI highly recommends that you install the VSI WBEM Service (WBEMCIM) kit V3.0-C180108 for VSI OpenVMS Integrity Servers prior to installing VSI TCP/IP V10.5.

SOFTWARE LICENSING

A VSI OpenVMS Integrity BOE or HA-OE software license is required in order to use the VSI TCP/IP software product. Rights to use future revisions of VSI TCP/IP are available only through a Support Agreement or through a new license purchase.

For more information about OpenVMS licensing terms and policies, contact your VSI account representative. Information is also available at the following website:
http://www.vmssoftware.com/services.html

LICENSE MANAGEMENT FACILITY SUPPORT

VSI TCP/IP for OpenVMS supports the *OpenVMS License Management Facility*. For more information about the License Management Facility, refer to the *VSI OpenVMS License Management Utility Manual* in the OpenVMS documentation set.

CLUSTER ENVIRONMENT

This layered product is fully supported when installed on valid and licensed OpenVMS Cluster configurations, which are fully described in the *OpenVMS Cluster Software Product Description* **(SPD DO-VIBHAA-032).** When each node in a VMScluster shares a common system disk, the cluster needs to store just one copy of most VSI TCP/IP files. You require only a few system-specific configuration files on each machine that runs the software.

DOCUMENTATION

VSI TCP/IP for OpenVMS documentation provides comprehensive reference and usage information for all product components. The VSI TCP/IP documentation set is included as part of the downloadable VSI TCP/IP software product offering. Hardcopy documentation is available from VSI by ordering part number DO-LITC0G-05V. Note that individual manuals are not separately orderable; they are only available as part of a complete set.

The following table lists the documents included in the VSI TCP/IP documentation set:

Part Number	***Title***
DO-DVTCLR-00A	VSI TCP/IP for OpenVMS V10.5 Cover Letter and Release Notes
DO-DVTIA1-00A	VSI TCP/IP for OpenVMS V10.5 Administrator's Guide, Volume 1
DO-DVTIA2-00A	VSI TCP/IP for OpenVMS V10.5 Administrator's Guide, Volume 2
DO-DVTADR-00A	VSI TCP/IP for OpenVMS V10.5 for OpenVMS Administrator’s Reference
DO-DVTQSG-00A	VSI TCP/IP for OpenVMS V10.5 Installation and Quick Start Guide
DO-DVTMLD-00A	VSI TCP/IP for OpenVMS V10.5 OpenVMS Messages, Logicals, and DECnet Applications
DO-DVTPRG-00A	VSI TCP/IP for OpenVMS V10.5 OpenVMS Programmer’s Reference
DO-DVTUSG-00A	VSI TCP/IP for OpenVMS V10.5 User’s Guide

GROWTH CONSIDERATIONS

The minimum hardware and software requirements for any future version of this product may be different from the requirements for the current version.

ORDERING INFORMATION

VSI TCP/IP is included in the VSI OpenVMS Integrity BOE or HA-OE software license. It is not available for purchase as a separately orderable product.

SOFTWARE PRODUCT SERVICES

A variety of service options are available from VSI. For more information, contact your VSI account representative or distributor. Information is also available at the following website:
http://www.vmssoftware.com/services.html

SOFTWARE WARRANTY

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

The information contained herein is subject to change without notice. The only warranties for VSI 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. VSI shall not be liable for technical or editorial errors or omissions contained herein.

A. Trademark and Copyright Notifications

This appendix contains a complete listing of trademarks and copyright notification contained in this manual.

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

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

The following third-party software may be included with your product and will be subject to the software license agreement.

Network Time Protocol (NTP). Copyright © 1992-2004 by David L. Mills. The University of Delaware makes no representations about the suitability of this software for any purpose.

Point-to-Point Protocol. Copyright © 1989 by Carnegie-Mellon University. All rights reserved. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by Carnegie Mellon University. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

RES_RANDOM.C. Copyright © 1997 by Niels Provos <provos@physnet.uni-hamburg.de> All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by Niels Provos.
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

Copyright © 1990 by John Robert LoVerso. All rights reserved. Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by John Robert LoVerso.

Kerberos. Copyright © 1989, DES.C and PCBC_ENCRYPT.C Copyright © 1985, 1986, 1987, 1988 by Massachusetts Institute of Technology. Export of this software from the United States of America is assumed to require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting. WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

DNSSIGNER (from BIND distribution) Portions Copyright (c) 1995-1998 by Trusted Information Systems, Inc.
Portions Copyright (c) 1998-1999 Network Associates, Inc.
Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies. THE SOFTWARE IS PROVIDED "AS IS" AND TRUSTED INFORMATION SYSTEMS DISCLAIMS
ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES
OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL TRUSTED INFORMATION SYSTEMS BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

ERRWARN.C. Copyright © 1995 by RadioMail Corporation. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of RadioMail Corporation, the Internet Software Consortium nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY RADIOMAIL CORPORATION, THE INTERNET SOFTWARE CONSORTIUM AND CONTRIBUTORS ``AS IS’’ AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RADIOMAIL CORPORATION OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This software was written for RadioMail Corporation by Ted Lemon under a contract with Vixie Enterprises. Further modifications have been made for the Internet Software Consortium under a contract with Vixie Laboratories.

IMAP4R1.C, MISC.C, RFC822.C, SMTP.C Original version Copyright © 1988 by The Leland Stanford Junior University

ACCPORNAM technology Copyright (c) 1999 by Brian Schenkenberger - TMESIS SOFTWARE

NS_PARSER.C Copyright © 1984, 1989, 1990 by Bob Corbett and Richard Stallman
This program is free software. You can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 1, or (at your option) any later version. This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details. You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139 USA

IF_ACP.C Copyright © 1985 and IF_DDA.C Copyright © 1986 by Advanced Computer Communications

IF_PPP.C Copyright © 1993 by Drew D. Perkins

ASCII_ADDR.C Copyright © 1994 Bell Communications Research, Inc. (Bellcore)

DEBUG.C Copyright © 1998 by Lou Bergandi. All Rights Reserved.

NTP_FILEGEN.C Copyright © 1992 by Rainer Pruy Friedrich-Alexander Universitaet Erlangen-Nuernberg

RANNY.C Copyright © 1988 by Rayan S. Zachariassen. All Rights Reserved.

MD5.C Copyright © 1990 by RSA Data Security, Inc. All Rights Reserved.

Portions Copyright © 1981, 1982, 1983, 1984, 1985, 1986, 1987, 1988, 1989 by SRI International

Portions Copyright © 1984, 1989 by Free Software Foundation

Portions Copyright © 1993, 1994, 1995, 1996, 1997, 1998 by the University of Washington. Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notices appear in all copies and that both the above copyright notices and this permission notice appear in supporting documentation, and that the name of the University of Washington or The Leland Stanford Junior University not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. This software is made available "as is", and THE UNIVERSITY OF WASHINGTON AND THE LELAND STANFORD JUNIOR UNIVERSITY DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, WITH REGARD TO THIS SOFTWARE, INCLUDING WITHOUT LIMITATION ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND IN NO EVENT SHALL THE UNIVERSITY OF WASHINGTON OR THE LELAND STANFORD JUNIOR UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR STRICT LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions Copyright © 1980, 1982, 1985, 1986, 1988, 1989, 1990, 1993 by The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions Copyright © 1993 by Hewlett-Packard Corporation.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Hewlett-Packard Corporation not be used in advertising or publicity pertaining to distribution of the document or software without specific, written prior permission. THE SOFTWARE IS PROVIDED "AS IS" AND HEWLETT-PACKARD CORP. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL HEWLETT-PACKARD CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions Copyright © 1995 by International Business Machines, Inc.

International Business Machines, Inc. (hereinafter called IBM) grants permission under its copyrights to use, copy, modify, and distribute this Software with or without fee, provided that the above copyright notice and all paragraphs of this notice appear in all copies, and that the name of IBM not be used in connection with the marketing of any product incorporating the Software or modifications thereof, without specific, written prior
permission. To the extent it has a right to do so, IBM grants an immunity from suit under its patents, if any, for the use, sale or manufacture of products to the extent that such products are used for performing Domain Name System dynamic updates in TCP/IP networks by means of the Software. No immunity is granted for any product per se or for any other function of any product. THE SOFTWARE IS PROVIDED "AS IS", AND IBM DISCLAIMS ALL WARRANTIES, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL IBM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE, EVEN IF IBM IS APPRISED OF THE POSSIBILITY OF SUCH DAMAGES.

Portions Copyright © 1995, 1996, 1997, 1998, 1999, 2000 by Internet Software Consortium. All Rights Reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies. THE SOFTWARE IS PROVIDED "AS IS" AND INTERNET SOFTWARE CONSORTIUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (c) 1996-2000 Internet Software Consortium.

Use is subject to license terms which appear in the file named ISC-LICENSE that should have accompanied this file when you received it. If a file named ISC-LICENSE did not accompany this file, or you are not sure the one you have is correct, you may obtain an applicable copy of the license at: http://www.isc.org/isc-license-1.0.html.

This file is part of the ISC DHCP distribution. The documentation associated with this file is listed in the file DOCUMENTATION, included in the top-level directory of this release. Support and other services are available for ISC products - see http://www.isc.org for more information.

ISC LICENSE, Version 1.0

1. This license covers any file containing a statement following its copyright message indicating that it is covered by this license. It also covers any text or binary file, executable, electronic or printed image that is derived from a file that is covered by this license, or is a modified version of a file covered by this license, whether such works exist now or in the future. Hereafter, such works will be referred to as "works covered by this license," or "covered works."
2. Each source file covered by this license contains a sequence of text starting with the copyright message and ending with "Support and other services are available for ISC products - see http://www.isc.org for more information." This will hereafter be referred to as the file's Bootstrap License.
3. If you take significant portions of any source file covered by this license and include those portions in some other file, then you must also copy the Bootstrap License into that other file, and that file becomes a covered file. You may make a good-faith judgement as to where in this file the bootstrap license should appear.
4. The acronym "ISC", when used in this license or generally in the context of works covered by this license, is an abbreviation for the words "Internet Software Consortium."
5. A distribution, as referred to hereafter, is any file, collection of printed text, CD ROM, boxed set, or other collection, physical or electronic, which can be distributed as a single object and which contains one or more works covered by this license.
6. You may make distributions containing covered files and provide copies of such distributions to whomever you choose, with or without charge, as long as you obey the other terms of this license. Except as stated in (9), you may include as many or as few covered files as you choose in such distributions.
7. When making copies of covered works to distribute to others, you must not remove or alter the Bootstrap License. You may not place your own copyright message, license, or similar statements in the file prior to the original copyright message or anywhere within the Bootstrap License. Object files and executable files are exempt from the restrictions specified in this clause.
8. If the version of a covered source file as you received it, when compiled, would normally produce executable code that would print a copyright message followed by a message referring to an ISC web page or other ISC documentation, you may not modify the the file in such a way that, when compiled, it no longer produces executable code to print such a message.
9. Any source file covered by this license will specify within the Bootstrap License the name of the ISC distribution from which it came, as well as a list of associated documentation files. The associated documentation for a binary file is the same as the associated documentation for the source file or files from which it was derived. Associated documentation files contain human-readable documentation which the ISC intends to accompany any distribution.

If you produce a distribution, then for every covered file in that distribution, you must include all of the associated documentation files for that file. You need only include one copy of each such documentation file in such distributions.

Absence of required documentation files from a distribution you receive or absence of the list of documentation files from a source file covered by this license does not excuse you from this requirement. If the distribution you receive does not contain these files, you must obtain them from the ISC and include them in any redistribution of any work covered by this license. For information on how to obtain required documentation not included with your distribution, see: http://www.isc.org/getting-documentation.html.

If the list of documentation files was removed from your copy of a covered work, you must obtain such a list from the ISC. The web page at http://www.isc.org/getting-documentation.html contains pointers to lists of files for each ISC distribution covered by this license.

It is permissible in a source or binary distribution containing covered works to include reformatted versions of the documentation files. It is also permissible to add to or modify the documentation files, as long as the formatting is similar in legibility, readability, font, and font size to other documentation in the derived product, as long as any sections labeled CONTRIBUTIONS in these files are unchanged except with respect to formatting, as long as the order in which the CONTRIBUTIONS section appears in these files is not changed, and as long as the manual page which describes how to contribute to the Internet Software Consortium (hereafter referred to as the Contributions Manual Page) is unchanged except with respect to formatting.

Documentation that has been translated into another natural language may be included in place of or in addition to the required documentation, so long as the CONTRIBUTIONS section and the Contributions Manual Page are either left in their original language or translated into the new language with such care and diligence as is required to preserve the original meaning.

10. You must include this license with any distribution that you make, in such a way that it is clearly associated with such covered works as are present in that distribution. In any electronic distribution, the license must be in a file called "ISC-LICENSE".

If you make a distribution that contains works from more than one ISC distribution, you may either include a copy of the ISC-LICENSE file that accompanied each such ISC distribution in such a way that works covered by each license are all clearly grouped with that license, or you may include the single copy of the ISC-LICENSE that has the highest version number of all the ISC-LICENSE files included with such distributions, in which case all covered works will be covered by that single license file. The version number of a license appears at the top of the file containing the text of that license, or if in printed form, at the top of the first page of that license.

11. If the list of associated documentation is in a seperated file, you must include that file with any distribution you make, in such a way that the relationship between that file and the files that refer to it is clear. It is not permissible to merge such files in the event that you make a distribution including files from more than one ISC distribution, unless all the Bootstrap Licenses refer to files for their lists of associated documentation, and those references all list the same filename.

12. If a distribution that includes covered works includes a mechanism for automatically installing covered works, following that installation process must not cause the person following that process to violate this license, knowingly or unknowingly. In the event that the producer of a distribution containing covered files accidentally or wilfully violates this clause, persons other than the producer of such a distribution shall not be held liable for such violations, but are not otherwise excused from any requirement of this license.

13. COVERED WORKS ARE PROVIDED "AS IS". ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO COVERED WORKS INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

14. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OF COVERED WORKS.

Use of covered works under different terms is prohibited unless you have first obtained a license from ISC granting use pursuant to different terms. Such terms may be negotiated by contacting ISC as follows:

Internet Software Consortium
950 Charter Street
Redwood City, CA 94063
Tel: 1-888-868-1001 (toll free in U.S.)
Tel: 1-650-779-7091
Fax: 1-650-779-7055
Email: info@isc.org
Email: licensing@isc.org

DNSSAFE LICENSE TERMS
This BIND software includes the DNSsafe software from RSA Data Security, Inc., which is copyrighted software that can only be distributed under the terms of this license agreement.

The DNSsafe software cannot be used or distributed separately from the BIND software. You only have the right to use it or distribute it as a bundled, integrated product.

The DNSsafe software can ONLY be used to provide authentication for resource records in the Domain Name System, as specified in RFC 2065 and successors. You cannot modify the BIND software to use the DNSsafe software for other purposes, or to make its cryptographic functions available to end-users for other uses.

If you modify the DNSsafe software itself, you cannot modify its documented API, and you must grant RSA Data Security the right to use, modify, and distribute your modifications, including the right to use any patents or other intellectual property that your modifications depend upon.

You must not remove, alter, or destroy any of RSA's copyright notices or license information. When distributing the software to the Federal Government, it must be licensed to them as "commercial computer software" protected under 48 CFR 12.212 of the FAR, or 48 CFR 227.7202.1 of the DFARS.

You must not violate United States export control laws by distributing the DNSsafe software or information about it, when such distribution is prohibited by law.

THE DNSSAFE SOFTWARE IS PROVIDED "AS IS" WITHOUT ANY WARRANTY WHATSOEVER. RSA HAS NO OBLIGATION TO SUPPORT, CORRECT, UPDATE OR MAINTAIN THE RSA SOFTWARE. RSA DISCLAIMS ALL WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO ANY MATTER WHATSOEVER, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS.

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