MultiNet® for OpenVMS

The MultiNet Solution

MultiNet is the complete networking solution for HP Corporation's VAX, Alpha and Integrity systems. MultiNet turns VAX, Alpha and Integrity computers into powerful application servers in multi-platform environments. It integrates OpenVMS systems with virtually any other system through industry-standard TCP/IP.

The MultiNet Services

MultiNet is a software product that includes several services and utilities, and provides support for the TCP/IP protocols. You can configure each product component on your system in any manner that suits your needs.

The MultiNet software services include:

* **FTP**—File transfer services
* **TELNET**—Virtual terminal services
* **NFS Client and Server**—Network File System services
* **SMTP**—Mail transfer services
* **SSH**—Secure Shell

The Core Services and Utilities

At the core of MultiNet are network services (TCP, UDP, IP, and ICMP), TCP/IP programming interfaces, and utilities that make your VAX, Alpha and Integrity computer fully TCP/IP compatible. MultiNet also includes utilities to manage and monitor your network.

All MultiNet components come complete with the product and you can configure and operate each one independently. You can also start and stop each MultiNet component without re-booting the entire system and affecting other products.

Fast and Efficient

MultiNet takes full advantage of the distinct architecture of OpenVMS for VAX, Alpha and Integrity systems. MultiNet implements lower-layer protocols (TCP, UDP, IP) as an executive image, focusing on minimal CPU loading. This provides peak performance so that MultiNet integrates cleanly into the OpenVMS environment.

With support extended now to OpenVMS versions 5.5-2 through 8.3, MultiNet supports the OpenVMS Communications Interface (VCI), a high-speed interface to Ethernet, FDDI, and Token Ring, and ATM and LAN over Galaxy shared memory drivers, for its TCP/IP Services.

Easy to Install and Operate

MultiNet is easy to install using the VMSINSTAL installation procedure. It takes 30 minutes or less to configure all services and utilities. A menu-driven configuration option is available also.

You can control most components in MultiNet by means of a single utility (MULTINET) that simplifies network management and allows you to manage MultiNet security. Using MULTINET you can:

* 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

Configuration Support

MultiNet supports VAX, Alpha and Integrity computers running various versions of OpenVMS. When each node in a VMScluster shares a common system disk, the cluster needs to store just one copy of most MultiNet files. You require only a few system-specific configuration files on each machine that runs the software.

MultiNet supports Symmetric Multi-Processing (SMP) for OpenVMS. Also supported by MultiNet are Class A, B, C, and D (multicast) networks, CIDR and IPv6.

HP Secure Web Server

MultiNet supports HP's secure Web server (Apache).

Multiple Interfaces (Paired Network Interface) Support on a Common Ethernet Cable

MultiNet supports systems that have multiple interfaces on a common Ethernet, FDDI, ATM, or Token Ring cable. MultiNet internally links 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, MultiNet assigns the data to the least busy linked interface for transmission.

TCP/IP Services for DECnet Applications

TCP/IP Services for DECnet Applications (*DECnet application services*, formerly known as Phase IP) lets applications designed to execute over DECnet® execute over TCP/IP instead.

Dynamic Host Configuration (DHCP) v3.0

MultiNet provides a Dynamic Host Configuration Protocol (DHCP) 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. With these features, 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 for two servers (primary and secondary) to share a configuration and service clients 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 Core Features of MultiNet...

* Provides fast and efficient operation that is designed and optimized for VAX, Alpha and Integrity systems

* Installs and operates easily, with no connectivity limitations

* Supports most system and hardware configurations, including LAN devices, Fast Ethernet, Serial Line IP, Point-to-Point, and X.25

* Follows OpenVMS standards closely for command syntax, basic security, and compatibility with standards products, such as TCP/IP Services for OpenVMS

* Provides access to a wealth of utilities and services, including:

  - Domain Name Services (DNS) BIND 9.4.2p (including DDNS)
  - Berkeley "R" Commands (RLOGIN, RSH, RMT, RCD) and Services, (`rlogin`, `shell`, and `rmt`)
  - Line Printer Services (LPR commands and LPD Server)
  - Terminal Server Print Services
  - IPP, the Internet Printing Protocol
  - SNMP Services, including SNMP Multiplexing (SMUX), and Agent Extensibility Protocol (AgentX)
  - DECwindows Transport Interface and XDM support
  - Network Time Protocol (NTP) version 4
  - TIMED, the Time Synchronization Protocol (TSP) daemon
  - Master Server Process
  - DECnet over IP
  - PING, TCPDUMP, NSLOOKUP, TALK, and other utilities
  - FTP and SMTP accounting statistics

* Allows additional third-party support via compatibility with HP and other products, services, and utilities

* Provides services to maximize network efficiency:

  - Dynamic Host Configuration Protocol (DHCP) Server and Safe-failover
  - Dynamic Host Configuration Protocol (DHCP) Client
  - Cluster alias failover
  - Multiple gateways, routing, and multi-casting
  - Dynamic TCP/IP load balancing
  - Paired Network Interface support

* Provides programming support, including a Socket Library, QIO interfaces, RPC services, and TCP/IP Services for OpenVMS compatibility

* Includes security features for Secure Shell (SSH) V1 and V2, Secure Copy Protocol v2 (SCP2), Secure File Transfer Protocol (SFTP), IP Security (IPSEC), access restriction, advanced packet filtering, Intrusion Prevention System (IPS), Kerberos protocol, and FTP over TLS.

Dynamic Host Configuration (DHCP) Client

The DHCP client resides on the system and dynamically sets the network configuration. The MultiNet 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 up the network.

LAN Devices

MultiNet operates with standard HP Ethernet/802.3, FDDI, and Token Ring network controllers. DECnet, Local Area Transport (LAT), and Local Area VMScluster (LAVC) software can share these controllers concurrently with MultiNet. There is also support for ATM controllers by means of the OpenVMS Alpha v7.1 (and later) Classical IP over ATM and LAN emulation support.

IP-over-X.25

MultiNet supports sending IP datagrams over certain X.25 packet switching networks using HP Computer Corporation's VAX Packetnet System Interface (PSI) product. You can connect separate TCP/IP LANs over packet switching data networks (PSDNs) or other X.25 WANs.

Serial Line IP (SLIP)

You can send IPv4 datagrams over serial lines using any standard OpenVMS serial line as a SLIP device. Dialup, dedicated serial lines, and Compressed SLIP (CSLIP) are supported.

Point-to-Point Protocol

MultiNet supports the Point-to-Point (PPP) interface for sending IPv4 datagrams over serial links. PPP provides more enhanced features than the SLIP interface, such as error detection and automatic negotiation of header compression, and supports PAP.

PATHWORKS (Advanced Server), DECnet/OSI Support

MultiNet provides TCP/IP support for PATHWORKS (Advanced Server) v5.0 and later, DECnet/OSI v6.0 and later through its PWIPDRIVER.

Third-Party Application Support

The MultiNet emulation of standard OpenVMS facilities supports several software products developed for compatibility with OpenVMS. For a complete list of companies and their products, refer to www.process.com.

Network Performance

MultiNet includes services that provide fast and efficient network operation and that minimize downtime.

Gateway Routing Daemon

MultiNet 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. GateD includes a language that is flexible in meeting any routing need for IPv4.

Routing

MultiNet includes routing and gateway capabilities for WANs and complex LANs.

Dynamic TCP/IP Load Balancing

The Domain Name Services supports dynamic TCP/IP Load Balancing, primarily for TCP-based applications such as TELNET. This allows the least-loaded systems running MultiNet 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 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

MultiNet incorporates the Berkeley remote access commands ("R" commands). These are UNIX client and server facilities for 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 (UNIX system) magnetic tapes using the RMT client. Remote users can back up their files on local magnetic tapes using the RMT server.

The Berkeley R commands use standard OpenVMS security facilities plus "host equivalence" files. For added security, you can use full Kerberos authentication with RLOGIN and RSH.

MultiNet supports RCD which provides local users the ability to 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

MultiNet contains a DECwindows transport interface that operates over TCP/IP. This lets you run DECwindows applications on remote workstations running TCP/IP, and X Window System applications on local VAX, Alpha and Integrity workstations.

X Display Manager Server

MultiNet 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

MultiNet provides the Domain Name Services (DNS) that implement the Berkeley Internet Name Domain (BIND) server standard, version 9.4.2p. 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 any other OpenVMS printer.

Line Printer Services

MultiNet 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:

* Print local files on remote printers.

* Remove print jobs from remote queues.

* Display job status in remote print queues.

LPS supports the UNIX commands `lpr`, `lpq`, and `lprm`, as well as the PRINT command. LPS 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 subagents 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 subtree with the SNMP Agent. Requests for objects residing in a registered MIB subtree 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. The HP Insight Management Agents use the SNMP extensibility provided by Agent X to allow remote examination and notifica-

tion of system conditions that may need attention. The Insight Management Agents are available on Alpha systems with OpenVMS v7.1 or higher, and Integrity systems.

Network Time Synchronization Facilities

MultiNet supports two types of time synchronization between network hosts:

* 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.

* TIMED, the Time Synchronization Protocol (TSP) daemon

Master Server Process

The master server process invokes all server processes, which are present when a connection is active.

The master server also:

* Logs all activity for security monitoring

* Can invoke user-written server processes

* Can restrict access to services based on the source Internet address

DECnet over IP

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

Multi-casting

MultiNet supports full Class D IP multicasting (IGMP V2 with fallback to IGMP V1) to host groups. Multi-casting support is available for the UCXDRIVER, INETDRIVER, and Socket Library programming interfaces.

Programming Support

Socket Library

MultiNet 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.

QIO Programming Interface

MultiNet provides a QIO interface for application programmers 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 TCP/IP Services for OpenVMS

MultiNet is compatible with HP's TCP/IP Services for OpenVMS, allowing applications written for products, such as DECwindows, PATHWORKS (Advanced Server), and DECmcc, to run transparently on top of MultiNet. The interface is the BG device.

INETDRIVER Services

MultiNet 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. MultiNet supports the HP 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

The security features in MultiNet provide data protection and security over the network that far exceeds what normal networks offer. This added security is important with the ever-increasing number of LANs, WANs, and hosts on the network. Network security prevents unauthorized use of systems, services, and network information.

The SSH2 server and client are compiled from unaltered cryptographic source which is FIPS 140-2 Level 2 compliant.

MultiNet offers the following types of security services:

* Secure Shell (SSH) v1 and v2 client and server

* Secure Copy Protocol v2 (SCP2)

* Secure File Transfer Protocol (SFTP) server and client

* Outgoing and incoming access restrictions

* Packet filtering

* Kerberos password authentication

* Kerberos v5 Telnet server and client

* IP Security with the Racoon key exchange daemon

* SSH Publickey Assistant

* CERTENROLL

* CERTVIEW

* FTP over TLS

* Intrusion Prevention System (IPS)

Secure Shell (SSH) v1 Client and Server

MultiNet SSH (Secure Shell) v1 is a program for logging into and executing commands on a remote system. It replaces rlogin, rshell, TELNET pro-grams, 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 MultiNet 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). This key 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 MultiNet, but any SSH client that uses SSH v1 protocol may be used to access the server. Examples of such programs are FISSH and MultiNet SSH on Open-VMS systems; TTSSH, SecureCRT®, F-Secure SSH Client, and PuTTY on Windows®-based systems; and other SSH programs on UNIX-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.

Secure Shell (SSH) v2

MultiNet 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 MultiNet. Although the protocols are incompatible, they may exist simultaneously on a MultiNet system. The MultiNet server front-end identifies what protocol a client desires to use, and will create an appropriate server for that client.

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.

The multiple encryption algorithms supported by SSH v2 are 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 v2 can be integrated with Process Software's VMS Authentication Module to provde LDAP and SecurID authentication for SSH.

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

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

CERTVIEW
Allows users 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. The CERTVIEW tool can be used for certificate viewing and validation.

For PKCS#10, CERTTOOL creates certificate requests, allowing the user 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 a 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, and not all implementations will offer all levels of functionality. The basic functionality is binary file transfers. MultiNet 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 MultiNet offers, MultiNet uses various methods to improve the chances that files will be useful upon transfer.

MultiNet 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 MultiNet v5.3, the file header information will also be transferred and the file will have 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 make sure that sshd2 is running on the remote host that you are connecting to.

SFTP2 is an evolving file transfer protocol, and not all implementations will offer all levels of functionality. The basic functionality is binary file transfers. MultiNet supports BINARY and ASCII transfers with SFTP2, 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 MultiNet offers, MultiNet uses various methods to improve the chances that files will be useful upon transfer.

FTP over TLS (FTPS)
FTPS allows users 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 as only a single process is used for encrypting and transferring the data. FTPS provides more reliable interchange of files between dissimilar systems as 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), source and destination address, or source destination port (UDP and TCP). In MultiNet V5.3, the packet filter definition files are fully IPv4 and IPv6 aware.

Intrusion Prevention System (IPS)
Components of MultiNet, including SSH, ftp, snmp, smtp, telnet, IMAP and POP3 have been instrumented to report various failures ("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 such that certain source networks or addresses are excluded from event correlation, or have event correlation applied with different

parameters, allowing the same rule to be applied differently, for example, to internal versus external network traffic.

An API is supplied so that MultiNet 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 a 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 Authentication

MultiNet provides Kerberos v4 authentication. Kerberos, an established authentication protocol, relies on a secure server to ensure login security. Kerberos uses data encryption to produce password "ciphertext" on TCP/IP networks.

With Kerberos, hosts prove their identity to other systems without transmitting "cleartext," or human-readable passwords. Their systems do not have to rely on the network for security.

Kerberos Applications

The following MultiNet applications allow Kerberos authentication for added security:

* RCP command

* RLOGIN command and rlogin services

* RSH command and rsh service

* TELNET-OpenVMS client and server

To requesting hosts, the Kerberos server issues tickets that contain keys to lock or unlock encrypted tickets, which in turn contain keys to lock or unlock encrypted passwords. The server is available to any heterogeneous Kerberos clients and servers from different vendors running different operating systems.

The Kerberos server includes a Key Distribution Center (KDC) and the Kerberos Administration (KADM) functions also.

Kerberos Administration Server

The Kerberos Administration Server provides an administration model so that system managers have remote access to the Kerberos database and remote users can change their passwords.

Kerberos User

Using the Kerberos User (KUSER) model, users can obtain and manage Kerberos tickets to use with their secured applications.

Kerberos v5 Telnet Server and Client

MultiNet v5.3 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. It requires Kerberos for HP OpenVMS (version 2.0), which is available via download on HP's Website.

Classless Inter-Domain Router (CIDR)

CIDR assures large organizations of connectivity to their entire network by allowing expansion of the available IPv4 addresses. This can be critical given today's complex topologies, high traffic loads, and the explosive growth of the Internet. New scaling problems at an unprecedented rate have occurred, including exhaustion of Class B network addresses, backbone routing overload, and exhaustion of IPv4 network numbers. This feature implements CIDR RFC 1517, 1518, and 1519. Use of variable-length subnet masks with CIDR solves these problems by allowing for supernetting and aggregating address assignments.

Gateway Routing Daemon (GATED)

GATED, based upon GATED Release 3.5 from Cornell University, is provided with this version of MultiNet. This version of GATED has 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.

Additional Features

MultiNet provides the TALK Utility and the TCPDUMP utility. The TALK utility enables remote users to share terminal messages in split windows in real time. The TCPDUMP utility is a useful mechanism for tracking TCP packets by printing information contained in the packet headers.

IPv6

MultiNet 5.3 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 tunnelled through an IPv4 network.

FTP

FTP-OpenVMS provides TCP/IP File Transfer Protocol networking services for OpenVMS computer users that need to transfer files from one computer's system to another. The number of simultaneous connections to FTP-OpenVMS is limited only by the available system resources.

FTP supports RFC 4217 - Securing FTP with TLS, which allows the user to log in over an encrypted connection and for data to be transferred over an encypted connection.

Client and Server Support

FTP-OpenVMS 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 server no longer lowercases the filenames returned in an NLST command. The FTP client now uses SRI encoding for filenames.

OpenVMS and UNIX Commands

Using the command line interface, you can initiate file transfers using native OpenVMS commands or equivalent UNIX-style commands interactively or with command procedures.

Session Accounting and Statistics

MultiNet can record accounting information from services that have been enabled. Currently this includes FTP and SMTP. The accounting information includes information about when a network session took place and how much data was transferred. The accounting facility is enabled from MULTINET CONFIGURE/SERVER ENABLE ACCOUNTING and reads MULTI-NET:ACCOUNTING.CONF for additional configuration information.

Full File Protection and Security

FTP-OpenVMS uses maximum Open-VMS 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-OpenVMS supports token authentication and full OpenVMS break-in detection and evasion.

Ease of Use

FTP-OpenVMS 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

* 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.

TELNET-OpenVMS

TELNET-OpenVMS provides complete virtual terminal networking services to OpenVMS systems by implementing the TELNET and TCP/IP protocols. TELNET-OpenVMS 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-OpenVMS provides a TELNET client and server. Users on a MultiNet system can login to remote systems, and users on remote systems can login to a MultiNet system via TELNET-OpenVMS.

Designed for Efficiency

Server-TELNET is for high-bandwidth applications. MultiNet 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 that is fully compatible with all TTDRIVER QIOs.

Permanence of NTY Devices

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

Full Password Protection (Kerberos)

TELNET-OpenVMS fully supports username and password protection by using the optional Kerberos v4 authentication scheme, provided with the token authentication security feature.

TELNET-OpenVMS optionally supports Kerberos v5 authentication and encryption via the KTELNET_SERVER image. 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.

TN3270 Mode

Client-TELNET supports TN3270 mode, providing IBM 3270-class terminal emulation for local OpenVMS terminals. Remote IBM hosts must support TELNET Servers.

Client-TELNET maps the OpenVMS keyboard to emulate IBM 3270 keyboard functions. You can use the default keyboard mappings or customize them.

TN3270 Internationalization

Client-TELNET supports the conversion of Western European EBCDIC character sets to corresponding OpenVMS character sets for TN3270 mode.

TELNET Protocol Options

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

TELNET-OpenVMS Features...

* Provides a client and a server

* Represents a fast, efficient design

* Permanence of NTY devices

* Supports Kerberos v4 authentication

* Provides a familiar interface to UNIX and OpenVMS users

* Provides a customizable TN3270 mode

Additional Features

TELNET-OpenVMS also offers:

* 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 and enabling flow control

NFS Client

NFS-OpenVMS 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 Alpha, VAX or Integrity system have transparent access to remote NFS servers, such as UNIX or IBM VM machines.

Filesystem 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 Filesystem 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 client adheres to NFS file organization and record format specifications so that you can write files back to the 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, vari-able-length, carriage-return-carriage-control files on your OpenVMS system.

Filename Mapping

Even though 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 filesystems and display mount information either interactively at the DCL or MULTINET level, or by using command procedures.

The command syntax, shown next, is convenient and straightforward:

```
NFSMOUNT server::"path"
[mount [logical]]
```

An example command is:

```
NFSMOUNT FLOWER::"/usr/
users" NFS1:
```

NFS Client features...

* Maintains consistent file protection and security

* Supports OpenVMS file types using companion data files to preserve file type information

* Maps filename characters to pre-serve file naming conventions between systems

10

NFS Server

NFS-OpenVMS server implements the server side of the NFS protocol, providing access to filesystems on your Open-VMS 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 MultiNet NFS client systems.

File Operations
The NFS server supports all normal file operations, even those on multi-volume disks. 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 stem, 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 server allows clients to read Open-VMS 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
Even though 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.

Standard Protocols for File Sharing
NFS Server supports these 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 Open-VMS filesystems 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.

NFS Server features...

* Supports file operations in all forms, including:

  - Create or remove directory
  - Create, remove, or rename file
  - Get or set attributes
  - Get filesystem statistics
  - Look up file or read directory
  - Read from or write to file
* Maintains consistent file protection and security

* Maps filename characters to preserve file naming conventions among systems

* Supports standard protocols for locking and file sharing across differing systems

SMTP

SMTP-OpenVMS 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 MultiNet. You can also deliver files as base64-encoded MIME messages by way of VMSmail.

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. MultiNet's 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 provides a way for 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, including:

* 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 Open-VMS MAIL
* Carbon copy (CC:) recipients

Store, Forward, and Relay

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

ARPA Standard Message Formats

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

SMTP-OpenVMS user names have the format:

```
SMTP%"address
[,address[,...]]"
```

Network mailbox addresses have the basic format:

```
username[@domain]
```

The *domain* is the name of the destination host, according to DNS standards.

SMTP features...

* Provides full SMTP Client and Server

* Provides IMAP4 Server

* Provides POP3 Server

* Uses standard MX records when using DNS

* Supports ARPA-standard formats and addresses, and mail request expansion

* Automatically stores, forward, and relays mail traffic as needed

* Supports performance tuning parameters

* Provides additional functionality, such as gateway to other mail services (such as ALL-IN-1)

* SPAM prevention

* Records accounting information from enabled services (See FTP for details)

Mail Exchanger (MX) Records

SMTP-OpenVMS 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-OpenVMS 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-OpenVMS performance. These parameters include:

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

Additional Features

SMTP-OpenVMS also provides the following features:
* Any user can be the postmaster
* SMTP-OpenVMS can function as a gateway between SMTP and DECnet and foreign mail products

Standards
and RFCs

MultiNet products conform to the
following military standards and Internet
Requests for Comments.

Military Standard Style	Mil-Std
Internet Protocol	1777
Transmission Control Protocol	1778
File Transfer Protocol	1780
Simple Mail Transfer Protocol	1781
TELNET Protocol and Options	1782

Request for Comments Title	RFC No.
User Datagram Protocol (STD 6)	768
DARPA Internet Protocol Specification	791
Internet Control Message Protocol	792
Transmission Control Protocol	793
Domain naming convention for Internet user applications	819
Simple Mail Transfer Protocol (STD 10)	821
Standard for the Format of Internet Text Messages (STD 11)	822
An Ethernet Address Resolution Protocol	826
TELNET Protocol Specification (STD 8)	854
TELNET Option Specification (STD 8)	855
TELNET Binary Transmission (STD 27)	856
TELNET Echo Option (STD 28)	857
TELNET Suppress Go Ahead Option (STD 29)	858
Echo Protocol (STD 20)	862
Discard Protocol (STD 21)	863
Character Generator Protocol (STD 22)	864
Quote of the Day Protocol	865
Daytime Protocol (STD 25)	867
Time Protocol (STD 26)	868
Domain names plan and schedule (Updated by RFC0897)	881
TELNET End of Record Option	885
Trailer Encapsulations	893
Transmission of IP Datagrams over Ethernet Networks	894
Domain name system implementation schedule (Updates RFC0881) (Updated by RFC0921)	897
Reverse Address Resolution Protocol	903
BSD EGP	904
Broadcasting Internet Datagrams (STD 5)	919

Request for Comments Title (Continued)	RFC No.
Domain requirements	920
Domain name system implementation schedule - revised (Updates RFC0897)	921
Broadcasting Datagrams in the Presence of Subnets (STD 5)	922
Internet Standard Subnetting Procedure (STD 5)	950
Bootstrap Protocol (BOOTP)	951
DoD Internet host table specification (Obsoletes RFC0810)	952
File Transfer Protocol (STD 9)	959
Mail Routing and the Domain System (STD 14)	974
XDR: External Data Representation Standard	1014
Domain Administrators Guide	1032
Domain Administrators Operations Guide	1033
Domain names - concepts and facilities (Obsoletes RFC0973, RFC0882, RFC0883) (Obsoleted by RFC1065, RFC2308) (Updated by RFC1101, RFC1183, RFC1348, RFC1876, RFC1982, RFC2065, RFC2181, RFC2308, RFC2535)	1034
Domain names - implementation and specification (Obsoletes RFC0973, RFC0882, RFC0883) (Updated by RFC1101, RFC1183, RFC1348, RFC1876, RFC1982, RFC1995, RFC1996, RFC2065, RFC2181, RFC2136, RFC2137, RFC2308, RFC2535)	1035
Standard for IP Datagrams over IEEE 802 Networks	1042
Network Systems HYPERchannel Protocol Specification	1044
Transmission of IP Datagrams over Serial Lines: SLIP	1055
RPC: Remote Procedure Call Protocol, Version 2	1057
TELNET Window Size Option	1073
TELNET Terminal Speed Option	1079
TELNET Terminal-Type Option	1091
NFS: Network File System Protocol Specification	1094
TELNET X Display Location Option	1096
DNS encoding of network names and other types (Updates RFC1034, RFC1035)	1101
U.S. Dep't of Defense Security Options for Internet Protocol	1108
Host Extensions for IP Multicasting (level 2) (STD 5)	1112
Requirements for Internet hosts - communication layers	1122
Requirements for Internet hosts - application and support (Updates RFC0822) (Updated by RFC2181)	1123
Compressing TCP/IP Headers for Low-Speed Serial Links	1144
Management Information for TCP/IP Internets (STD 17)	1155
A Simple Network Management Protocol (SNMP) (STD 15)	1157
BSD BGP	1163, 1267, 1654
Choosing a name for your computer	1178
Line Printer Daemon Protocol	1179

Services, Documentation, and Ordering Information

Technical Services

Process Software's Technical Services Program has a well-deserved reputation for excellence. Services include consulting, training, software maintenance, support, online resources, and 24-hour support. In short, everything you need to keep your Process Software products and your network operating at peak efficiency.

Consulting

A comprehensive suite of programs is available on a host of topics, including MultiNet installation and configuration, DNS setup and use, network security, troubleshooting, and others.

Hot Line Support

Networking experts are available by telephone, e-mail, or fax. Optional 24-hour support is also available.

Updates

All maintenance customers with current service contracts receive automatic software and documentation updates of major releases.

Training

A wide range of educational services can be provided at your site, at regional training locations throughout North America, or at our own training facility in Framingham, MA.

Documentation

Comprehensive documentation for all MultiNet products includes user guides, installation and configuration information, management functions and utilities, programming facilities, and network security. Documentation in HTML and PDF format is included on your product CD, and is available in HTML format on Process Software's web site, www.process.com.

You can find Frequently Asked Questions (FAQs) on the Tech Support web page on the Process Software web site (http://www.process.com/techsupport/MultiNet.html).

Ordering Information

MultiNet is shipped on CD-ROM and TK50.

Software Warranty

Process Software warrants all products for 90 days from the date of delivery.

Hardware and Software Requirements

MultiNet requires one or more of the following hardware devices:

* HP Ethernet controller

* HP FDDI controller

* HP Token Ring controller (except DEQRA)

* IP-over-x.25 controller

MultiNet requires, at a minimum, these operating system versions:

* VAX/VMS v5.5-2 and later

* OpenVMS Alpha v6.2 and later

* OpenVMS I64 v8.2 and later

About Process Software

Process Software is a premier supplier of communications software solutions to mission critical environments since 1984. With thousands of loyal customers worldwide, including Global 2000 and Fortune 1000 companies, Process Software has earned a strong reputation for meeting the stringent reliability and performance requirements of enterprise networks. Process Software products incorporate leading edge technologies and are backed with a dedicated customer support organization.