MULTINET®

Complete TCP/IP Networking Solution for HP VAX, Alpha, and Integrity Systems

MultiNet TCP/IP for OpenVMS provides reliability, advanced functionality, and security for running mission-critical applications.

MultiNet for OpenVMS is a full suite of TCP/IP applications and services for HP's VAX, Alpha, and Integrity platforms. It enables OpenVMS systems to participate as fully functional TCP/IP hosts. Leveraging existing resources, MultiNet enables a VAX, Alpha, or Integrity system to take advantage of all the services and applications available on the Internet. OpenVMS users can easily exchange e-mail, as well as access and transfer files and data securely.

MultiNet is the preferred TCP/IP stack for systems administrators that are running mission critical applications. Process Software provides the most secure, reliable, and feature-rich TCP/IP stack for OpenVMS.

We have a proven track record of success within many Global 2000 companies running mission-critical applications using OpenVMS. Process Software products incorporate leading edge technologies and are backed with a dedicated customer support organization.

ADVANCED SECURITY

MultiNet provides several layers of security to protect against unauthorized network access and intruders from the Internet.

FTP OVER TLS: FTP over TLS supports RFC 4217. TLS provides server authentication with keys that may be either self-signed or signed by a trusted authority. Servers may be configurable to require secure data transfers. FTP over TLS requires an explicit request for encryption and server authentication.

INTRUSION PREVENTION SYSTEM (IPS): MultiNet's IPS monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. MultiNet SSH, FTP, SNMP, Telnet, IMAP, and POP3 have been instrumented with IPS to monitor traffic for malicious attacks. It is highly flexible and customizable. When an attack is detected, pre-configured rules will

MultiNet Advantages:

- *Secure communications with SSH , SFTP, and SCP servers and clients, IPSEC, IPS, Kerberos v5.0 and FTP over TLS*
- *Investment protection with new features support on OpenVMS v5.5-2 or later, and the ability to run DECnet applications without modification directly over TCP/IP*
- *Increased reliability and network performance with Paired Network Interface*
- *Ease of management with SMTP and FTP accounting and statistical reports*
- *Advanced printing and troubleshooting with the IETF standards-based Internet Printing Protocol*
- *Complete reliable DHCP solution: DHCP client and server with Safe-failover*

FREE EVALUATION SOFTWARE!
Please call 800-722-7770 to get your free evaluation copy of MultiNet.

PROCESS™ SOFTWARE

block an intruder's IP address from accessing their system, prevent an intruder from accessing a specific application, or both. The time period that the filter is in place is configurable. An API is provided so that MultiNet customers can incorporate the IPS functionality into their applications.

SECURE SHELL V1, V2 (SSH): SSH is a protocol that provides strong authentication and secure, encrypted communications over unsecured channels. This transport layer protocol provides server authentication, confidentiality, and integrity with perfect forward secrecy.

MultiNet offers SSH v1 and v2 servers and clients the ability for users to simultaneously use both protocols. The SSH v2 server and client code is compiled from an unaltered cryptographic source, which is FIPs 140-2 Level 2 compliant. SSH v2 uses a more secure host-based authentication exchange called Diffie Hellman. Diffie Hellman provides additional security by eliminating the need for exchanging private keys over the wire. It also allows users the advantage of continually authenticating throughout the entire session.

Security and flexibility are achieved through multiple levels of user authentication and strong encryption algorithms, including IDEA, DES, 3DES, ARCFOUR, Blowfish, Twofish, AES-128, and CAST-128.

The MultiNet SSH server and client are flexible, supporting a wide variety of third-party SSH servers and clients on OpenVMS, UNIX, Macintosh, Linux, and Windows platforms.

In addition, managing SSH authentication is simplified with single sign-on support. MultiNet SSH works with existing PKI cetificates and Kerberos infrastructure.

SECURE FILE TRANSFER PROTOCOL (SFTP) AND SECURE COPY PROTOCOL (SCP): MultiNet increases security with SFTP and SCP support. Both protocols provide a secure mechanism for transferring, copying, or deleting files over networks. SFTP and SCP utilize the SSH server and client as a basis for accomplishing this advanced level of security *(see Figure 1).*

Both SCP and SFTP can transfer files as ASCII, BINARY, or in OpenVMS format when implementing SSH file transfer protocol v4 (IETF draft). Support for this protocol improves file transfer interoperability between different operating systems.

IP SECURITY (IPSEC): IPSEC is a standards-based technology which provides a secure tunnel for transmitting data through an unsecured network, such as the Internet. IPSEC's architecture, authentication header (RFC 2401 & 2402), and IPSEC Encapsulation Security Payload (RFC 2406) are supported in transport and tunnel mode, which secures packets between any compliant hosts. MultiNet also supports IKE, which negotiates the IPSEC security associations and generates the required key automatically (RFC 2407-09).

KERBEROS V5.0 TELNET SERVER AND CLIENT: MultiNet's Kerberos v5 TELNET server and client provides strong authentication for applications by using secret-key cryptography. Once a client and server have used Kerberos to prove their identity, all communications are encrypted to assure privacy and data integrity. MultiNet runs with Kerberos for HP OpenVMS which is available on the HP website.

INCOMING/OUTGOING ACCESS RESTRICTIONS: MultiNet's access restrictions provide an additional method of security to the network. The outgoing access restrictions provide system administrators with additional security by controlling those applications local users can or cannot access (such as restricting Web surfing or access to services like FTP or TELNET). MultiNet also imposes incoming restrictions on the remote hosts' access to local services.

SECURE FILE TRANSPORT PROTOCOL (SFTP), SECURE COPY PROTOCOL (SCP), AND SSH OPERATION

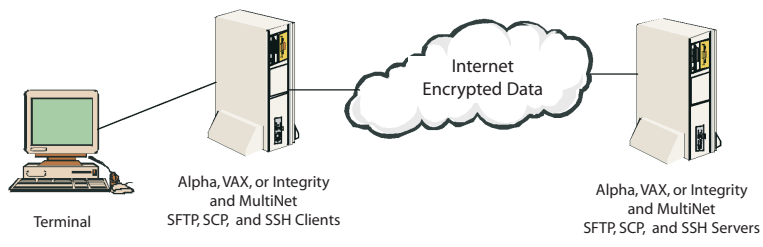

Figure 1

Robust IP Stack

Paired Network Interface: Paired Network Interface support increases performance and reliability. It allows two or more network interface cards (NIC) with their own unique IP addresses in a VAX, Alpha, or Integrity system to be connected to the same virtual cable in order to optimize throughput and create NIC redundancy. Any number of OpenVMS supported NIC types can be used including Ethernet, Token Ring, Fast Ethernet, FDDI, and ATM *(see Figure 2).*

MultiNet's Paired Network Interface support provides network reliability, redundancy, and increased throughput without the use of additional systems.

If one NIC fails in an Alpha, VAX, or Integrity system, information will be transmitted from the second NIC. Additionally, multiple NICs can be used to increase throughput if a data communications bottleneck is suspected from the server. Areas where Paired Network Interface will improve connectivity include e-commerce applications where there are frequent database transactions, multimedia applications where there is high bandwidth consumption, and any applications where a single server connection is causing delays for clients.

Gateway Routing Daemon (GATED): 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.

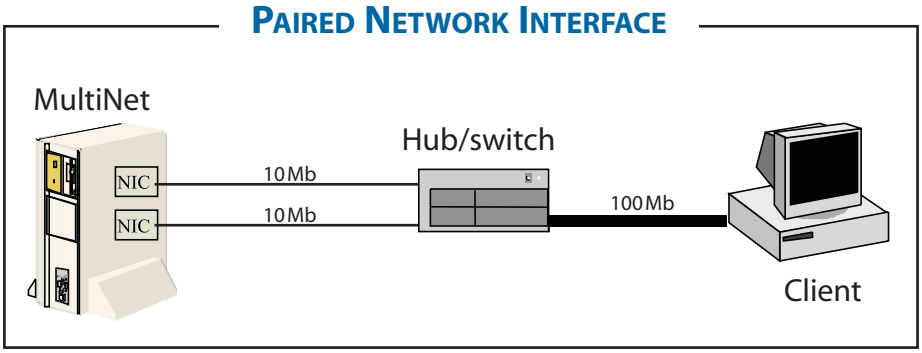

Figure 2 - *Dual 10Mb NICs improve throughput by utilizing bandwidth on a 100Mb Ethernet segment downstream from the server segment. The Paired Network Interface combines failover with an ability to use existing network interface cards as well as increase transmission performance from the server.*

Classless Inter-Domain Router: CIDR assures large organizations of connectivity to their entire network by allowing expansion of the available IP 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 IP 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.

New Feature Support on OpenVMS v5.5-2 or Later: MultiNet offers new feature support on OpenVMS v5.5-2 or later. MultiNet provides users with the unique ability to implement new features, without having to go to the expense or time to upgrade to the latest OpenVMS release. TCP/IP Services for OpenVMS does not support new functionality unless users are running the latest major OpenVMS release. Users are forced to upgrade to the most current versions in order to implement new TCP/IP Services for OpenVMS functionality.

Servers and Clients

DHCP Server: MultiNet includes a DHCP server based on the Internet Software Consortium's (ISC) v3. DHCP v3 allows more granular control of the DHCP server with client classing and conditional behavior. With client classing, clients can be assigned to classes based on information sent in packets, such as MAC address, the client name, etc. Then address assignments can be made based on the client's class. For example, a remote user may be assigned a shorter lease time of 2 hours versus a local user with an 8-hour lease time.

This high-performance server also offers Dynamic DNS (DDNS) support and a powerful configuration file format.

DHCP Safe-failover: MultiNet's DHCP server includes Safe-failover support, a protocol co-authored by Process Software and Cisco Systems. DHCP Safe-failover provides uninterrupted IP services to clients during network or server failures so that they can reliably obtain IP addresses to connect to corporate resources. It increases significantly the reliability and availability of DHCP services.

DHCP Client: DHCP client allows you to remotely centralize administration of your VAX, Alpha, or Integrity. A DHCP client is needed in order to receive IP addresses from the DHCP server. The DHCP client saves system administrators time by enabling them to retrieve changes to the DHCP server automatically, versus having to assign IP addresses and DNS servers manually.

DNS Server with Dynamic DNS: MultiNet's DNS server is based on BIND v9.4. This version includes support for multiple views (split DNS), DNSSEC, incremental zone transfer, Dynamic DNS (DDNS) updates, DNS notify, IPv6, and enhanced standard conformance for over 25 RFCs. With split DNS, administrators can create two zones for the same domain. One of the zones is used by internal network clients and the other zone is used by external network clients.

DNSSEC (RFC 2065) provides security when updates are made to the DNS server via zone transfer or DDNS. DNSSEC ensures that the information is coming from a legitimate source by using authentication.

Incremental zone transfer (RFC 1995) or IXFR improves the performance of a DNS environment. The name server (or DNS server) only transfers the changes in a zone, e.g., add or delete a record. Reducing the size and length of zone transfers is important where there are large zones (e.g., .com) or dynamic environments (e.g., DDNS) for DNS server efficiency.

Dynamic DNS updates allow applications (such as DHCP) to modify resource records dynamically. This feature simplifies systems administration management and saves time because the DNS server maintains an up-to-date record of the address space.

MultiNet's DNS notify feature means that when zone changes occur on the primary server, it notifies the secondary servers, which can initiate immediately a zone transfer rather than having to wait for the polling interval to expire. Thus, zone changes propagate much faster through the servers.

MultiNet's support for BIND provides granular control of which servers are allowed to do zone transfers, DDNS updates, queries, etc. Control is available on a zone-by-zone basis, not just on the entire server.

Flexible and Robust Printing Options

Internet Printing Protocol (IPP): IPP is an open standard protocol developed by the Printer Working Group (under IETF) for printing over the Internet. IPP provides enhancements over the existing commonly used LPD protocol including the ability for a user to print to a remote printer using the same methods and operations as if the printer was located locally.

System administrators using print protocols such as the LPD print protocol have had to spend a significant amount of time administering printing tasks with limited troubleshooting capabilities. For example, a system administrator receives no information on why a print job fails. The MultiNet IPP print symbiont provides a reason for a print job failure. This saves time in troubleshooting printing problems.

The MultiNet IPP print symbiont provides standard commands for advanced printer functionality (e.g. double-sided printing) regardless of what printer is being used. A system administrator requires no additional training or programming to use IPP. In addition, when using the MultiNet IPP print symbiont, a user will not need to inquire about the functionality of a particular printer with a system administrator because this information is provided automatically.

Line Printer Daemon (LPD): LPD print services are supported, allowing LPR clients that are on a TCP/IP network to access print queues on Integrity, Alpha or VAX systems.

Line Printer (LPR/LPD) and Telnet Printing: LPR, LPD, and Telnet printing provide flexibility to users that need access to printers in a remote location and interoperability with UNIX and Terminal Servers. LPR clients can access LPD printer servers that are on a TCP/IP network. Print queues can be accessed on Integrity, Alpha or VAX systems.

Management Services

Statistics and Accounting Reports: MultiNet has the ability to generate statistical and accounting reports on SMTP and FTP usage to assist with capacity planning, billing, and trouble-shooting. FTP accounting and statistics are based on the Network Monitoring MIB (RFC 2788). Information that is collected on the FTP server includes: user names logged into the server, client and server session start and end time, amount of data sent and received, total number of files sent and received, number of active connections, and other operational statistics.

SMTP accounting and statistics is based on the Mail Monitoring MIB (RFC 2789). It records a log of each message sent and received. This includes the record's message date, time, size, From: and To: strings. It also provides a count of detected loops.

Throughput statistics assists system administrators with trouble-shooting by providing information on system performance. Information is available on the rate data was transmitted and received in bytes and packets per second.

Ease of Management: MultiNet also simplifies network management and configuration by offering a single management utility. It provides options for installation as a standalone system or on a cluster-wide basis.

Agent X: MultiNet supports RFC 2257. Agent X allows the MIB subagents delivered with HP's Insight Manager to manage OpenVMS using MultiNet. Host Resource MIB and other MIBs that ship with HP software can also be used.

SNMP Subagent: The SNMP Subagent provides users with the ability to write their own custom MIBs.

MultiNet v5.3 - Features at a Glance

IP Stack

IPv6 Kernel, TELNET, BIND, SSH, NTP, FTP, DNS Resolver, SMTP, POP3, IMAP, LPD and STREAM printing

IPv6 six to four interface

BSD 4.4 Kernel

CIDR

Paired Network Interface

PPP

PathMTU Discovery

GATED

New Feature Support for OpenVMS v5.5-2 or later

Servers and Clients

DHCP Server with Safe-failover

DHCP Server v3.0

DHCP Client

Dynamic DNS (DDNS)

DNS BIND v9.4

Management Services

SMTP and FTP Statistical and Accounting Reports

Throughput Statistics

Start/Stop Individual Services

SNMP Subagent

Agent X

NTP v4.2

Infrastructure

DECnet Phase IV over IP

DECnet Applications over IP

IP over DECnet Tunneling

E-mail Services

SMTP

POP3

IMAP4 Mailserver

Spam Prevention

Security Services

Secure Shell v1, v2 (SSH) clients and servers

Secure Copy Protocol (SCP) client and server

Secure File Transfer Protocol (SFTP) client and server

IP Security (IPSEC)

SSH single sign-on with support for Kerberos and PKI certificates

Intrusion Prevention System

Incoming Access Restrictions

Outgoing Access Restrictions

Kerberos v5.0

FTP over TLS

Ephemeral Port Randomization

Applications

NFS over UDP or TCP

ODS-5 for NFS Server

"R" Services

FTP

TELNET

Several Application Programming Interfaces (APIs) are supported, including:

Socket Library (v4.3 BSD)

DEC C/VAX C Socket Library

MultiNet/SRI $QIO Interface

UCX $QIO Interface

RPC Interface

DCE for OpenVMS

Printing Services

IPP (Internet Printing Protocol)

LPD (Line Printer Daemon)

LPR (Line Printer)

TELNET/Stream Printing

E-Mail Services

IMAP4 Server: IMAP4 lets a client mail program access messages stored on an OpenVMS server as if these messages were local. IMAP4 retains the message

on the server, either in the in-box or in a folder that the user creates.

The advantage of retaining e-mail messages centrally (using IMAP4) is that if employees work from multiple locations using multiple computer systems (e.g., home or branch office), they have access to all their e-mail messages regardless of their location and systems used.

Complete Intranet and Internet File, Print, and Terminal Services

MultiNet includes a wide choice of file services to access, transfer, and print networked data. Network File System (NFS) client and server provides transparent and quick access to remote files and directories. The NFS server provides access to the OpenVMS file system from the NFS client. ODS-5 support for NFS server allows for long file names and a mixed case naming convention. The NFS client allows OpenVMS users and applications access to any system running an NFS server, including UNIX systems. Additionally, MultiNet provides File Transfer Protocol (FTP) client and server functionality for transferring files.

Seamless Execution of DECnet Applications over TCP/IP without Modification

Moving your OpenVMS systems from DECnet to TCP/IP is seamless with MultiNet. The DECnet Application Programming Interface (API) for TCP executes applications designed to run over DECnet transparently across TCP/IP. Because no DECnet protocols are involved, there is no need to run DECnet. No user retraining or applications recoding is necessary. System administrators can perform a rolling conversion from DECnet to TCP/IP at their own pace while users continue to work uninterrupted.

Prerequisite Software

MultiNet requires OpenVMS AXP v6.2 and higher, OpenVMS VAX v5.5-2 and higher, or OpenVMS I64 v8.2 and higher. Message Router v3.1 or later is required for Simple Mail Transfer Protocol (SMTP) to ALL-IN-1 gateway capability. In order to enable Kerberos v5 authentication in the SSH server, the HP OpenVMS Kerberos v5 product must be installed (see http://h71000.www7.hp.com/openvms/products/kerberos/). This restricts support for Kerberos to OpenVMS Alpha v7.2-2 and higher.

Media

MultiNet is distributed on CD-ROM. It is also available on a TK50 cartridge for VAX systems.

About Process Software

Process Software is a premier supplier of communications software solutions to mission critical environments. The company has been in business since 1984 and has a loyal customer base of over 3,000 organizations, 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's Technical Services Program

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.

PROCESS™ SOFTWARE

Process Software
959 Concord Street
Framingham, MA 01701

Telephone:
U.S./Canada (800)722-7770
International (508)879-6994
Fax: (508)879-0042
Web: www.process.com
E-mail: info@process.com

N-1004-53-NN-B