digital™

Software Product Information

PRODUCT NAME: DECserver Network Access Software V2.3

SPI T0.41.07
AE-RDDUA-TE
April 1999

Description

DECserver Network Access Software, Version 2.3 is the latest software release for the DECserver 700 equipped with 4 MB or more of memory; DECserver 900 equipped with 4 MB or more of memory; DECserver 90TL equipped with 4 MB of memory; and DECserver 90M equipped with 4 MB of memory. Throughout this document, the term "DECserver units" will be used to refer to the DECserver 700-08, DECserver 700-16, DECserver 900TM, DEC-server 900GM, DECserver 900MC, and the DECserver 90M hardware platforms onto which the DECserver Network Access Software may be loaded. DNAS will be used to refer to DECserver Network Access Software Version 2.3. Those features that are restricted to, or limited by, a specific DECserver hardware platform are noted.

Included with DNAS are a number of additional software programs that work with the DNAS software, but run on other systems, not on the DEC-server itself. These software programs, which may be used at the option of the user include: Access Server Manager which includes Access Server Loader, and DIGITAL Remote Access Security (DRAS). These programs are described separately within this SPI.

The DECserver units are communication servers for Ethernet LANs. They support remote PC dialup access for IP, IPX, and AppleTalk networks. They also provide a convenient method to logically connect asynchronous terminals, PCs, and other asynchronous devices using LAT, Telnet or Raw TCP to one or more service nodes (hosts) on an Ethernet. Once the terminal, asynchronous device, or PC is connected, a user can use application programs and utilities as though the device is directly connected to a host. Thus, it may be possible to use the DECserver to connect all terminals to service nodes in place of traditional interfaces.

New Features Supported by DNAS Version 2.3

- Rlogin is a utility that allows users to log onto remote computers. Rlogin is described in informational RFC 1282. Rlogin supports pre-authenticated sessions on hosts that have been configured with trust relationships. This allows users to connect to these hosts without needing to enter a username and password.
- Directed TFTP is a feature that allows the IP address of a TFTP server to be configurable on the DECserver. Once configured, the DECserver firmware will download its operating software from the specified TFTP server rather than soliciting a response from a BOOTP server. Directed TFTP makes it easier for the DECserver to obtain an image over the wide area network. Directed TFTP requires a minimum ROM code revision to be resident in the DECserver. The minimum revision is ROM code Version 5.1 for the DECserver 90M and Version 7.1 for the DECserver 700 and DECserver 900.

- DNAS reports "Termination Reason Codes" to the DIGITAL Remote Access Security RADIUS server utility. "Termination Reason Codes" identify the cause when a session terminates and can be helpful in network troubleshooting, as well as in billing applications.
- Local user account authentication now supports PPP CHAP.

PC Dialup Remote Access Support

The DECserver Network Access Software provides remote connectivity to IP networks via SLIP (Serial Line Internet Protocol), CSLIP (Compressed SLIP), and via PPP (Point-to-Point Protocol). As many IP systems as there are serial ports on the DECserver unit may be connected. These systems can run IP applications (such as Telnet, FTP, X-Windows, and so on) on the serial line and communicate with other IP services on the network. The DECserver software also routes IP datagrams between asynchronous SLIP or PPP ports.

DECserver units support host multiplexing for attached Novell NetWare clients. NetWare clients may attach directly to the DECserver via asynchronous lines or may dial into the DECserver. The DECserver uses IPXCP and PPP to establish an asynchronous link between the remote NetWare client and the DECserver. Once established, the DECserver provides a transparent link to the network for asynchronously connected clients. Each asynchronously attached client looks and acts as if it were directly connected to the local area network (LAN).

The DECserver software supports host multiplexing for attached AppleTalk hosts. The DECserver software acquires and assigns AppleTalk addresses for attached hosts via AARP and PPP. The DECserver unit uses the AARP protocol to acquire a new address for a connecting host, and it uses the PPP ATCP protocol to assign this address to the host. The DECserver keeps a cache of already acquired addresses to optimize the connection process. The system administrator can configure the address cache size.

DECserver units using either SLIP or PPP can be configured to provide asynchronous communications between two LANs for hosts supporting TCP/IP. This support requires that manual routing table entries be made for all hosts that need to communicate across the wide area link. Once table entries have been made, hosts use the DECserver port like a gateway. Since the routing entries are static, there is no forwarding or fallback in the event the DECserver link is broken. This feature provides a low-cost wide area network (WAN) link appropriate for smaller remote LANs.

AUTOLINK

This feature provides a generic asynchronous serial data link connection (or session) for dial-in ports. This feature allows a Server Manager to configure a dial-in port to service both PPP and SLIP users with minimal user interaction. An AUTOLINK session examines characters received from the attached devise. If a PPP or SLIP packet is detected, the current session will attempt to change itself into the corresponding type of data link session, PPP or SLIP. If AUTOLINK does not detect a PPP or SLIP start frame character, it will select character cell terminal emulation.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a combination of four IETF RFC's, which together enable automatic and reliable distribution of IP addresses. DNAS V2.3 support for DHCP allows the DECserver to operate as a DHCP proxy to obtain a leased IP address for a remote client from a DHCP server on the network. The DECserver maintains the address on behalf of the remote client for the duration of the session. This feature eases the network manager's job by letting the DHCP server automatically provide IP addresses for each port as needed, rather than having to assign and maintain permanent IP addresses for each DECserver port. The DECserver itself does not learn its IP address from a DHCP server.

Inactivity Timer

DECserver software supports an inactivity timer for SLIP- and PPP-based connections. Inactivity can be monitored on a server-wide or per-port basis. When the configurable inactivity threshold is exceeded, the DNAS Version 2.3 software automatically tears down the SLIP or PPP connection. The inactivity timer ignores normal keepalive or maintenance messages, such as PING, counting only data traffic as activity.

Gateway Failover

DECserver units can detect whether the default gateway has gone out of service, and can locate and use other gateways (if available and configured).

TCP/IP Keepalive Timer

TCP/IP Keepalive Timer (RFC 1122). The TCP keepalive timer determines whether a TCP connection with a remote host is active and should remain open. After a TCP connection is established, the TCP/IP keepalive timer waits a configurable length of time and then sends a probe to the remote host. If the remote host responds, the TCP keepalive timer waits again. If it does not receive a response, it continues to send probes until a set maximum is reached. If the host does not respond after the last probe is sent, the access server drops the connection.

WINS Autoconfigure

WINS autoconfigure support. The Windows Internet Name Service (WINS) provided by Microsoft with Windows NT and Windows 95 provides a distributed database for mapping NetBIOS names to IP addresses. WINS is often used in combination with DHCP so that dynamically assigned IP addresses can be automatically updated in the WINS database. WINS requires a WINS server (that is, a Windows NT server) and a WINS client (Windows for Workgroups, Windows 95, or Windows NT Workstation). This feature on the DECserver allows dial-up clients to receive WINS configuration information automatically when a PPP connection is initially established.

Security and Access Control Features

- Serverwide Login Passwords-A serverwide login password can be enabled by the Server Manager. If enabled, the terminal user must enter a login password to access server functions. Login password provides low-level, basic security.

- PAP-Password Authentication Protocol (PAP) is the password scheme supported by PPP. PAP uses an ID/ password pair. PAP ID/passwords may be stored in the DECserver unit, or may be stored in a sepa rate authentication service such as Kerberos V4 or RADIUS.

- CHAP-Challenge Handshake Authentication Protocol (CHAP) is a PPP based challenge/response authentication scheme. If enabled, users accessing the DECserver unit via applications supporting CHAP may use the PPP CHAP scheme, with passwords stored on the DECserver unit or with RADIUS.

- Kerberos Authentication-Provision for user authentication is included in the DECserver Network Access Software using Kerberos V4. In addition, users may change their Kerberos passwords (stored on the Kerberos master database) remotely from the DECserver unit. User authentication is a security feature that requires a user to enter a valid user name and password pair before being allowed to log in to the DECserver. The user must have been previously registered (user name and password) with a Kerberos Key Distribution Center on a host running the Kerberos server software. This effectively gives users on the network their own password to log in to the network through the DECserver, using Kerberos. Kerberos uses the Data Encryption Standard to authenticate its messages over the network. No Kerberos passwords are transmitted in the clear.

- Kerberos Authenticated PAP-The DECserver software allows a PPP Password Authentication Protocol user name/password pair to be directly forwarded to a Kerberos V4 Key Distribution Center for authentication without the need for an interactive login process, but directly from the PPP login.

- Dial-back Authentication-DNAS supports a dialer service that allows both mandatory and interactive dial-back. The dialer service is made up of configurable "dial service" parameters that control how a user may use the dialer service, and a dialer engine responsible for processing the outbound request and placing the port into a desired state upon successful call completion. User profile information required to support the dialer service and dial-back may be stored either directly in the DECserver unit for a limited number of users, or may be obtained from the RADIUS user profile database. DNAS supports both standard LCP-based callback negotiation (Call Back Control Protocol) and the Microsoft Call Back Control Protocol for Windows 95 and Windows NT clients. The DECserver automatically supports either type when configured for dial-back.

- RADIUS Authentication and Authorization-DNAS includes a RADIUS client application that conforms to IETF RFC 2138 and RFC 2139. RADIUS is an Internet standard that describes an open protocol for communicating authentication, authorization, and accounting data between remote access servers and shared authentication servers. The RADIUS client may interoperate with other RADIUS server implementations, but is supported when used with the DIGITAL Remote Access Security (DRAS) RADIUS server application. The DRAS server utility is included on the DNAS media kit.
- SecurID-DNAS includes ACE/Server Client Code support for the Security Dynamics ACE/Server system. The ACE/Server Client Code included with the DNAS software provides encrypted authentication of one-time passcodes. DNAS code includes both an SDI-developed encryption algorithm and a DES encryption algorithm. Users can select the appropriate algorithm based on the ACE/Server available from Security Dynamics in their geography.

The DNAS Version 2.3 client supports Version 1.3 through Version 2.3 of the Security Dynamics ACE/Server.

The DECserver unit provides functions that enhance security features already available in the service nodes. DECserver security includes the ability to lock a terminal's keyboard from other users, optional login protection, and nonprivileged local mode of operation as a default.

A user may lock the terminal by using a lock password. This allows the user to leave sessions running at the terminal without fear of security violations. When a terminal is locked, all input from the terminal is ignored until the lock password is reentered. The lock feature may be disabled by the Server Manager.

Each terminal port can be set up to operate in a secure mode, which causes all commands that relate to other users to be disabled for that port.

DECserver users usually have access to the nonprivileged local mode. In this mode, users may only issue commands that affect their own terminal environment. The server has a privileged mode for Server Manager's use. The mode is password protected.

The Server Manager can further restrict nonprivileged and secure ports by enabling the LIMITED VIEW characteristic, which prohibits users from viewing tables of LAT nodes, LAT services, and certain Internet databases. The Server Manager can restrict the port user to a predetermined set of commands by creating a command menu with these commands in it, and defining this menu as the default menu on the port. In this case, the menu is automatically entered when the user logs into the port. The user cannot exit from the menu, except to log out of the port.

- Groups (LAT)-Every terminal and service node in a LAT network is a member of one or more groups specified by a list of numbers from 0 to 255. Groups allow an easy means of subdividing the network into what appears to be many smaller networks. A terminal user is only aware of the services that are offered by nodes in the same group(s). The Server Manager can specify the authorized group(s) in which a terminal is a member. The authorized groups define the set of services that the user is allowed to access. In addition, for those nodes that implement group codes, a user can further limit access to services by disabling some of the authorized groups using a non-privileged group command. The user-settable group codes are a sub-set of the authorized groups. Groups provide a restrictive view of the network. This restricted view is mainly for user convenience. Groups apply only to LAT connections.

DIGITAL Remote Access Security Utility

DIGITAL Remote Access Security (DRAS) is a standalone application that allows you to configure and manage secure remote access to your network. DRAS controls which users can access the network, when users can access the network, and what users can do when connected to the net work. DRAS also provides accounting capabilities to track users' activities.

The DRAS server software uses the Remote Authentication Dial-In User Service (RADIUS) protocol as defined in the current Internet Engineering Task Force (IETF) RFC 2138 and RFC 2139. Any network access server that communicates with the DRAS server needs to support the RADIUS protocol.

The DRAS V2.3 features described in this document are fully supported when the DRAS server is used in combination with DECserver network access servers running DECserver Network Access Software V2.3, which includes a fully compatible RADIUS client. Network access servers from other vendors may also support RADIUS clients and may work with DRAS, but interoperability is not guaranteed nor support implied.

The DRAS product has two major components: the DRAS Server and the DRAS Manager. The DRAS Server is the application that communicates with various clients that send it access requests. A client can be a network access server (NAS) or a remote management workstation. The DRAS Server stores information about groups, users, clients, sessions, and authentication methods as objects in a local database. Objects include:

- All RADIUS clients that send authentication, authorization, and accounting requests to the DRAS server.
- All remote management stations that are authorized to access the DRAS Server's database.
- All users for whom the DRAS Server performs authentication. Users do not interact directly with the DRAS Server, but with a RADIUS client that then sends the authentication requests to the DRAS Server.
- All administrative users that are authorized to access the DRAS Server's database for management purposes.
- The DRAS Manager is the Windows-based graphical user interface application that is used to manage the DRAS Server and to configure its database. The DRAS Manager can:
- Stop, pause, and resume a remote or local DRAS Server
- View status of local or remote servers
- Manage objects in the local or remote DRAS Server databases

DRAS Services and Features:

The DRAS Server provides the following services to its clients:

Service	Description
Authentication	Allows the NAS to identify an external user requesting network access correctly and reliably
Authorization	Defines what services the user may access on the network
Accounting	Provides information about services used by the user for billing, audit trail, and troubleshooting purposes

The DRAS Server supports the following authentication methods:

- CHAP-Static password authentication using PPP's Challenge Handshake Authentication Protocol.
- DEFENDER-AssureNet Pathway's challenge/response two factor authentication. It uses the DES algorithm to generate unique one-time passwords.
- HOST-DRAS Server host login authentication.
- OTP-An MD5-based challenge/response authentication. It implements one-time password authentication and is derived from Bellcore's S /key.
- PASSWORD (PAP)-The DRAS Server uses a static password, in conjunction with a username, registered in its database for the user. Typically, the user can change this password.
- SECURID-Security Dynamics Technologies' SecurID token card one-time passcode authentication. You need an SDI ACE/Server on the network for this authentication method.
- WATCHWORD-RACAL-Guardata's challenge/response authentication. It uses the encryption algorithm that the Watchword calculator implements.

The DRAS Server supports the following criteria for authorization:

Criteria	Description
User Account	The DRAS Server checks the user object in its enabled database to determine whether the user account is enabled. User objects are likely to be disabled following break-in detection or a configurable amount of time during which the object is not used
User account	The DRAS Server checks the user expiration date expiration and time in the user database against the current local time.
User account	The DRAS Server checks the user access hours, access hours which define a weekly access schedule, against the local time.
User group	The DRAS Server checks group objects in its check database against the following criteria: group enabled, group expiration, group access hours.

The DRAS Server supports the following security facilities:

- Break-in detection - The DRAS Server can detect and track consecutive authentication failures for a particular user. When consecutive authentication failures occur, the DRAS Server disables the user account. Enabling requires manual intervention. The DRAS Server can also detect and track consecutive authentication failures from a particular port/NAS. When consecutive failures occur in this way, the DRAS Server rejects any further requests from this port on the NAS and puts the port/NAS on a blacklist.
- Duress login detection - Certain authentication devices allow a user under a threat to connect and tell the NAS that the connection is occurring under abnormal conditions. When detecting this, the NAS must allow the connections but tracks, flags, and possibly reports the exception to the management station. This detection depends on the capabilities of the authentication method in use.

The DRAS Server collects accounting and event information about the DRAS Server operation and connection activity. The DRAS Server stores this information in its accounting database. The information in the accounting log file can be displayed or exported as a common delimited text file to be printed or imported into another application.

HARDWARE REQUIREMENTS

DRAS Server Software

The DIGITAL Remote Access Security server software runs on the following systems:

- DIGITAL Alpha Systems
- DIGITAL VAX systems
- Intel PCs

DIGITAL Remote Access Security Software Disk Space Requirements

To install and operate the DIGITAL Remote Access Security server software, you need the following minimum disk space:

Operating System	Disk Space
For OpenVMS VAX	1400 disk blocks server
For Open VMS Alpha	2100 disk blocks server
For Digital UNIX	2 MB server on Alpha
For Windows NT	7 MB server on Alpha
For Windows NT	4 MB server on Intel PCs

Management Utility Software Disk Space Requirements

To install and operate the DIGITAL Remote Access Security management utility software, you need the following minimum disk space:

Operating System	Disk Space
For Windows NT	4 MB management utility on Alpha
For Windows NT	2 MB management utility on Intel PCs
For Windows 95	2 MB management utility on Intel PCs

SOFTWARE REQUIREMENTS

DRAS Server Software

The DIGITAL Remote Access Security server software runs in the following operating system environments:

- OpenVMS Alpha Version 6.2 or greater
- OpenVMS VAX Version 6.1 or greater
- DIGITAL UNIX Version 3.2 or greater
- Windows NT Version 3.51 or greater

DRAS Management Utility Software

The DIGITAL Remote Access Security management utility software runs in the following operating system environments:

- Windows NT Version 3.51 or Windows NT Version 4.0
- Windows 95

Accounting and Billing

The DECserver unit running DNAS supports two accounting methods. One is an SNMP-based UNIX utility called HarvestD. The other is via Remote Access Dialup User Services protocol (RADIUS).

- HarvestD - The HarvestD utility provides reliable logging of significant user actions (for example; logins, session connects, password failures, and so on.). These events can be useful in supporting capacity planning, audit trails, billing, and connection troubleshooting. The DECserver unit logs these events in its volatile memory. HarvestD reliably copies these logs to a host's disk.

Events can be sent, as they occur, to a physical port where they can be displayed on a connected terminal/printer or redirected to a remote connection. To print or display events as they occur, does not require that any reserved DECserver memory.

DECserver memory can be reserved for storing events so that the DECserver unit itself contains a log of accounting events. These events can be browsed via an SNMP station or via the user interface. The accounting log will store all events until the user-selected buffer size is exceeded. Once the buffer size is exceeded, the oldest event will be dropped and the newest added.

An accounting threshold variable can also be set that will notify a potential harvester application to begin reading entries before the accounting log is full. These notifications are in the form of SNMP traps.

- RADIUS - The DNAS software includes a RADIUS client. The RADIUS client is capable of generating accounting information for significant user actions including logins, session connects and services used. All DECserver units ship with a companion RADIUS server application called DIGITAL Remote Access Security (DRAS). DNAS and DRAS together provide a complete solution for RADIUS based accounting.

Accounting data is stored by the DRAS server in a tabbed format so that the data may be imported into many popular billing applications.

Server Management

The DECserver unit supports several facilities supporting both local and remote management. These include the command line interface, the console port, the remote console port, and Access Server Manager. Protocols that are used to manage the DECserver include MOP, Telnet, and SNMP.

- Management via the console port using the command line interface (CLI)

  The Server Manager environment using the CLI is a logical extension of the user environment. The Server Manager is a server user with a privileged status. The Server Manager sets a terminal to this status using a command that requires a password. This privileged status allows the Server Manager to enter commands not usually available to server users. These commands set server characteristics, provide control over server port usage, and provide the ability to control the user's access to the server and network services.

  In service mode, the terminal input is passed directly to the connected service node with several exceptions. One exception, called the local switch character, allows the user to enter local mode from service mode. The key may also be used for this function. Other exceptions, called the forward and backward switch characters, allow the user to switch between sessions without the need to enter local mode. The switch characters are disabled by default but may be enabled by command. Both Ctrl/S and Ctrl/Q are usually interpreted locally, but flow control using these characters can be disabled.

- Remote management of the DECserver unit using the CLI

  The DECserver unit implements the console carrier feature that enables access to the DECserver local mode from either a Telnet host or from a Phase IV or Phase V DECnet host on the same LAN. With the exception of remote console port configuration, the entire local mode user interface is accessible to the remote console carrier user. This includes the privileged commands if the user knows the server's privileged password. This capability allows centralized server management and remote server diagnosis.

  The Telnet remote console feature is also available and can be used to support remote server management as stated above.

Management of the DECserver unit using Access Server Manager

The Access Server Manager application runs on 32-bit Windows-based operating systems and has a graphical user interface that allows easy configuration of many access server features. The Access Server Loader application is integrated with Access Server Manager. Access Server Manager supports the following tasks:

- Tests to see if the target DECserver's remote console is reachable.

- Downloads firmware from a PC load host to the access server using Access Server Loader.
- Connects to the remote console for customized configuration and monitoring of the DECserver.
- Supports "Save" and "Restore" functions to read and store the DECserver's NVRAM locally on the PC or write the stored configuration on the same or different DECserver.
- Runs customized command files containing access server console commands, as well as VMS's Terminal Server Manager command scripts.
- Reboots (ie initializes) the DECserver

Access Server Manager provides support for:

- Configuring IP characteristics including: addresses, gateways, DNS clients, DNS/DHCP/WINS servers, Hosts, and ARP tables.
- Configuring IPX and Appletalk on the DECserver.
- Configuring ports on the DECserver.
- Configuring modems attached to DECserver ports.
- Configuring the DECserver login password and security realms including local, Kerberos, RADIUS, and SecurID.
- Configuring accounting on the DECserver.
- Configuring SNMP on the DECserver.
- Configuring the Dialer application.
- Configuring LPD printers.

Management of the DECserver unit using SNMP

The DECserver unit has an SNMP (Simple Network Management Protocol) agent that allows it to be managed by an SNMP network management system such as clearVISN MultiChasis Manager. Information can be retrieved (GET) and modified (SET) from the server.

Features supporting the DEChub environment

DECserver Network Access Software supports IP Services. IP Services support allows clearVISN MultiChassis Manager software to communicate through DECserver 900 modules with the DEChub 900 MultiSwitch Management Access Module (MAM).

DECserver Network Access Software supports Console Redirect. Console Redirect Support allows DECserver 900 modules to be initialized from the DEChub 900 MultiSwitch out-of-band management (OBM) port. This features allows the OBM port to act as the DECserver console port.

Additional DNAS Features

Terminal to Host Support

The DECserver Network Access Software provides concurrent local area terminal (LAT) and Telnet TCP/IP protocol support from a DECserver communications server to enable connectivity to host systems that use LAT or TCP/IP protocols. The TCP/IP protocol suite is used to connect to UNIX host systems and other host systems that support the TCP/IP protocol suite. The TCP/IP protocols are based on the University of California's 4.3 Berkeley Software Distribution (BSD).

Host to Printer Support

The DECserver unit also allows for host-initiated connections to serial printers. A serial printer can be shared between LAT printer quests and Telnet requests. Telnet requests cannot be queued on the server. A print symbiont on service nodes can initiate connections to serial printers connected to DECserver ports. This allows the printers to be distributed throughout a facility and accessed transparently by service node users. Incoming host-initiated connect requests may be queued FIFO at the server.

The DECserver Network Access Software kit includes software that allows serial printing from UNIX or Windows NT hosts by using Line Printer Daemon (LPD). The DECserver listens for print requests from remote hosts on the Local Area Network and responds to them. The DECserver implementation of LPD supports printing of ACSII and Postscript files.

UNIX hosts can also use a Telnet print filter that encapsulates the output of a printer interface program into Telnet format and sends the encapsulated data through a DECserver Telnet Listener port to the specified printer. LPD is the recommended method and use of the print filter is not supported.

DNAS also supports raw TCP Listeners for remote printing. Local Mode and Service Mode

For the most part, the environment provided by the DECserver unit is identical to the environment that the user would experience if attached directly to the service node. When operating in this mode, the user is said to be in service mode. Occasionally, such as during connection establishment, the user interacts directly with the DECserver. When operating in this mode, the user is in local mode.

In local mode, the terminal input is interpreted directly by the software as commands to be performed by the server.

Local mode has three different levels of privilege: privileged, non-privileged, and secure.

- Privileged mode is provided for the Server Manager to control the environment of the server and the terminal users. Access to this mode is password protected.
- Nonprivileged commands allow the terminal user to control their service sessions, set the terminal characteristics, and show server information.
- The Server Manager can set the server to secure mode on a per-terminal basis, which further limits the commands that users can enter to only those that directly relate to the user's own terminal.

Autoconnection (LAT)

Autoconnection is a function that automatically connects a user terminal to a service node when connection failures occur or upon user login to the server. In conjunction with this function, a dedicated or preferred service can be specified for each terminal user.

If a dedicated service is specified, the DECserver unit will attempt to connect to that service when a character is typed on the terminal keyboard or when an existing connection fails. In dedicated service mode, only one session is available. As this mode is designed to simulate a direct terminal connection, no local mode commands or messages are available to the terminal user. Ports with dedicated service can be automatically logged out of the server when the user logs out of the service node.

If a preferred service is specified, the DECserver unit will attempt to connect to that service as with the dedicated service mode of operation. However, the terminal user can enter local mode and establish other sessions. Automatic Protocol Selection

It is possible to automatically connect to an Internet host or LAT service without explicitly identifying the connection as LAT or Telnet. If the port is configured with a value for the default protocol as "ANY," the terminal server will attempt a LAT connection first to the name specified in the LAT service field. If the service is not available or unknown, the terminal server will then automatically attempt a Telnet connection to the Internet host specified in the command.

Automatic Session Failover (LAT)

If a service is available on two or more service nodes, and a connection to a service fails, the server will attempt to connect the user to another service node offering the same service. The user does not have to be connected to that service node. Furthermore, the user's context at the time of failure is not automatically restored and login to the new service is required. This feature is supported only for LAT connections.

Management and Ease of Use

- Online HELP Facility

  A full online reference HELP facility is available. The server's HELP command provides information on the correct syntax and details about each command. In addition, a tutorial HELP feature allows new users to quickly learn the basics of DECserver operation. Tutorial HELP may be entered upon logging into the server. HELP is based on whether the user is secure, nonprivileged, or privileged.

- Command Prompting

  The command prompting feature allows users to solicit specific help based upon where they are in the command sequence. The user types a question mark and is presented with a list of next possible commands or keywords.

- Command Groups

  The command group feature allows users to define their own command word(s), which, when invoked, will execute a sequence of stored server commands.

- Command Line Recall and Editing

  The DECserver unit supports multiple command line entry recall and editing.

- Customized Menus

  This feature allows the privileged user to create a customized menu style user interface rather than the command line interface.

Directory Service (LAT)

Any DECserver user can obtain a directory of LAT services available to that user with a SHOW SERVICES command. Services for which the user is not authorized will not be displayed. Services apply only to LAT connections.

Welcome Identification

The DECserver unit standard welcome banner, which includes server type, version number, and internal base level, is issued whenever a user successfully logs in to the server. The server will also print a ServerManager-settable identification string. This can be useful for automatic server identification or for small daily messages used for communications with the terminal server users.

Troubleshooting Facilities

Several facilities exist for managing and troubleshooting server operation. The Server Manager in privileged mode can set up server identification information, change port characteristics, or fine-tune the operating characteristics of the server. Troubleshooting facilities include diagnostic tests, a remote console feature, and online statistics.

A privileged user can diagnose Ethernet communications problems by looping messages to an Ethernet host and through the Ethernet hardware interface at the server. To diagnose terminal problems, users can execute a command to transmit test data to their terminal, or the Server Manager can send test data to any terminal.

The capability also exists for the Server Manager to test a service connection by sending data from the initiating port to the service node, and then back again. The data is then compared and any discrepancies reported. At the service node, the data can be looped back by the LAT protocol, or internally or externally at the service port. This feature is supported only by DECserver service nodes; OpenVMS service nodes do not support this service loopback capability.

The server maintains a variety of statistics and counters. These include the following: Ethernet data link statistics, LAT protocol statistics, port character counters, and port error statistics. This data can be displayed and zeroed by the Server Manager. Server parameters that can be modified and displayed include the server identification, circuit timer, session limits, and login limits.

Internet statistics are also maintained by the server. Internet characteristics such as Internet address and subnet mask can be modified and displayed. IP, ICMP, TCP, IP, UDP, DNS, and SNMP protocol statistics can be displayed. Load Balancing (LAT)

When a connection is made to a service, the actual node for the connection is determined by load balancing. Load balancing is a process that the server uses when more than one node offers the same service. Service nodes do not have to be configured in a cluster in order for load balancing to be used. Service nodes with the same names may be running different operating systems. Using the load balancing process, the server connects to the node with the highest rating for the service desired. This rating is based on the current loading on the nodes that offer the service.

Multiple Sessions

The DECserver unit allows each user to establish and maintain up to eight sessions to one or more service nodes. Only one session per user can be active at a time. Through simple switching commands, the user can access the different sessions without repeating a login dialogue each time. Some operating systems may impose limits on the number of LAT or Telnet sessions that a host will support.

On-Demand Loading

The DECserver unit implements the ODL (On-Demand Loading) font-loading protocol, which allows Asian-language terminals that implement the ODL protocol to communicate with an OpenVMS host via a terminal server. The Asian-language terminals will be able to request font definitions from an OpenVMS host when connected to a DECserver. This feature is supported only for LAT connections.

Outbound Connection Queues (LAT)

If a terminal user requests a connection to a service and the requested service is currently in use, the terminal server users may opt to have the requested connection queued to the remote service. If the user's port has been appropriately configured, this feature is performed automatically whenever a connection fails for this reason. The connection request is queued at the service node end and is processed first-in/first-out (FIFO) until such time as the user's connection request can be completed. This feature assists in the fair management of limited network resources. Once queued for connection, the user also has the option to cancel the queue entry and proceed with other sessions. This feature is supported only for LAT connections. Similar functionality may be available via a print filter program on a Telnet host.

Reverse LAT, Telnet Listener, and TCP Listener

The DECserver unit supports reverse LAT, Telnet Listener, and TCP Listener. These facilities are provided to enable a network node, such as a host system, to connect to a DECserver port. This facility could be used to support printers, a modem pool for outgoing calls, and connection to the asynchronous ports of a system without other network access, such as an Ethernet controller. Reverse LAT, Telnet Listener, and TCP Listener also provide the ability to group physical ports into logical groupings. For example, ports connected to the asynchronous interfaces of the same system could be grouped so that a connect request would be routed to any of the currently unused ports. A logical grouping can contain any number of ports from one to all of the ports on the server.

The DECserver Network Access Software allows the DECserver to support RAW TCP. The DECserver unit can be configured to process TCP traffic directly without using Telnet options negotiation. This option is supported for hosts connecting to DECserver TCP listeners.

Port-to-port connections on the same server are also supported.

The system administrator can assign an individual IP address per Telnet Listener. This provides a means to uniquely identify a service per DECserver port, as needed, using standard DNS name resolution. This eliminates the need to specify a TCP port number when connecting to services.

Terminal Device/Session Management Protocol

The DECserver unit also implements and supports the Terminal Device/Session Management Protocol (TD/SMP) to manage multiple sessions at the device level. The DECserver provides the ability to communicate with devices that also implement this protocol (such as VT420, VT330+, or VT340+), and assist in the management of multiple sessions for these devices. By implementing this protocol, the DECserver can permit attached devices to maintain screen and keyboard context for multiple LAT and/or Telnet sessions, as well as allow these devices to run multiple LAT and/or Telnet sessions concurrently.

The DECserver software will support block-mode transfers of up to 2,048 bytes.

WAN Communications for Terminals

For WAN communications, terminal users can connect to remote hosts via Telnet through a TCP/IP router or gateway. In addition, terminal users can connect to a local service node running DECnet, where they can "SET HOST" to a remote system via the DECnet network terminal protocol. If this system has the requisite X.25 or SNA 3270 access routines, a terminal user could communicate to a remote SNA or X.25 host through the appropriate gateway and this intervening host. A DECserver terminal user cannot communicate directly to remote hosts through DECnet routers or X.25/SNA gateways. WAN traffic will not provide the same high level of performance as local terminal connections due to the additional DECnet or Internet protocol overhead. The DECserver units support connections to WANs via modems.

Permanent Characteristics

The DECserver unit maintains permanent characteristics in nonvolatile memory, that are retained even when the power is disconnected. Permanent characteristics are maintained for service and server parameters, as well as per-port parameters. Permanent characteristics can be reset to factory defaults by pressing the software reset button on the hardware unit while plugging in the power cord.

Port Characteristics Configuration

Characteristics governing the operation of an individual port can be displayed by a nonprivileged terminal user interactively from the user's terminal. Many of the characteristics may be set by the user, but certain characteristics are privileged and may only be changed by the Server Manager.

Port parameters that can be set and displayed include: speed, character size, group codes, parity, terminal type, access, autobaud, default protocol, and password protection.

Port Access

Port access is the characteristic that determines how a port may access or be accessed by interactive users and service nodes. A port on a DECserver unit may be configured in different ways depending on the device attached to the port and its intended use. Additionally, different DECserver hardware platforms provide support for different port devices.

- Access Local - Designed for interactive terminals. This allows the device (typically an interactive terminal) attached to the port to CONNECT to LAT or Telnet. Additional example: dial-in modem.
- Access Remote - Designed for application-driven devices such as asynchronous printers that are allocated by a service node process. This allows the implementation of certain shared printers by multiple service nodes. Additional example: dial-out modem.
- Access Dynamic - Designed for devices (such as personal computers or printers with keyboards) that require both local and remote access. Additional example: dial-in/dial-out modem.
- Access None - Designed to allow the Server Manager to disable the use of a port.

With printer support capabilities, the configuration procedure of remote printers needs to be done once and will be automatically reconfigured on system startup. The particular server port must be configured for remote access and set up to match the characteristics of the printer. Improved printer sharing allows a printer on the server to be shared among hosts using LAT and hosts using Telnet.

Internet Request for Comments (RFC) Support

The following TCP/IP protocols are supported and adhere to the Internet Request for Comments (RFCs):

- BOOTP (RFC 951 and RFC 1084) and TFTP (RFC 783) protocols together provide a method for downloading the DECserver unit from any host that supports these protocols. BOOTP provides a mechanism whereby the server can identify a host from which it can request a down-load. TFTP provides the data transfer facility used to copy software from the load host to the server.
- Dynamic Host Configuration Protocol (DHCP) (RFC 2131, RFC 2132) is a combination of four IETF RFC's, which together enable automatic and reliable distribution of IP addresses. The DECserver acts as a DHCP proxy on behalf of clients.
- Transmission Control Protocol (TCP) (RFC 793) is the Internet-standard, transport-level protocol that provides the reliable, end-to-end full-duplex stream service that supports many application protocols.
- User Datagram Protocol (UDP) (RFC 768) is an Internet protocol that provides datagram service to application programs, allowing an application program on one machine to send a datagram to an application program on another machine. UDP is necessary for the Domain Name System and Simple Network Management Protocol (SNMP).
- Internet Protocol (IP) (RFC 791) is an Internet-standard protocol that defines the Internet datagram as the unit of information that is passed across the Internet, and provides the universal addressing scheme for hosts and gateways for Internet connectionless, best-effort packet delivery services. IP includes ICMP as an integral part.
- Internet Control Message Protocol (ICMP) (RFC 792) is an Internet network protocol that specifies error and control messages used with the Internet protocols. Packet Internet Groper (PING) tests the reachability of nodes on the user's Internet. ICMP echo requests are sent and replies processed.
- Address Resolution Protocol (ARP) (RFC 826) is an Internet protocol used to perform address resolution to dynamically map or translate an Internet address into the correct physical hardware address.
- Telnet (RFC 854) is the standard Internet application-level protocol for remote terminal connection service. Telnet is a virtual terminal facility that allows a user at one site to establish a TCP connection to a remote system. Telnet makes the local terminal appear as a direct extension of the remote system, allowing the user to conduct a session and run application programs as if the user's terminal was directly connected to the remote system. Both Telnet client and server capabilities are provided:

  TN3270 Terminal Emulation allows users of a DIGITAL ASCII video terminal or PC in terminal emulation mode (VT100, VT200, VT300, VT400 mode) within an Internet network, to interactively access IBM host-based applications developed for IBM 3270 display stations.

  Telnet client provides the ability to connect to any remote TCP port at an Internet address on a LAN or a WAN. Telnet client allows the user to specify a remote computer by Internet address as well as by Domain name.

  Telnet server allows hosts to connect to devices (like printers, host systems, and other serial devices) connected to the DECserver ports.

  Telnet character and binary profile features are available to facilitate using Telnet sessions in interactive or file-transfer modes. Telnet options supported include: status (RFC 859), end-of-record (RFC 885), remote flow control (RFC 1080), echo (RFC 857), timing mark (RFC 860), binary (RFC 856), suppress go ahead (RFC 858), and send location (RFC 779).

  TN3270 serverwide keymapping is a feature that allows the network manager to make up to six customized terminal types and associated keymappings available on the server. An individual port can access any one of these keymappings without using up additional NVRAM. The port user chooses one of the terminal types with the SET PORT TN3270 TERMINAL command.

  Telnet Remote Console allows a user to establish a remote Telnet connection to the management port on

the terminal server, and manage the server as if locally attached. The Telnet Listener 23 can now be assigned to any terminal server port as well as the remote console. Any Telnet Listener (23, 2001-2016) can be assigned to be the remote console.

- Internet Domain Name System (DNS) Support - The Domain Name System provides the translation from system name to Internet address. The DECserver unit will interface to user programs and send queries to Domain name servers for translating Domain names to Internet addresses, and Internet addresses to Domain names (RFCs 1034 and 1035).
- Subnet Addressing (RFC 950)
- Simple Network Management Protocol (SNMP) - The SNMP agent allows the DECserver unit to be managed by an SNMP network management system. Retrieving information from the terminal server is possible by using the SNMP GET and GET-NEXT requests. The SNMP SET operation is fully supported, providing the ability to modify DECserver parameters as well as create and delete applicable table entries. The terminal server can send unsolicited event alarms to specified SNMP management stations via the SNMP TRAP message. Terminal server variables accessible via SNMP (RFC 1157), not a MIB, are defined by the Internet documents: MIB II (RFC 1213), RS-232-like MIB (RFC 1317), and the Character MIB (RFC 1316). Also supported are the AppleTalk MIB (RFC 1243) and the Ethernet-like MIB (RFC 1284).
- Serial Line Internet Protocol (SLIP) - A host computer that supports SLIP can use the DECserver serial port as its network connection. This gives IP hosts, which have no direct Ethernet connection, access to the network and to IP hosts attached to other DECserver serial ports. Any IP application can then be run over the SLIP link (RFC 1055).
- Compressed Serial Line Internet Protocol (CSLIP) (RFC 1144)-CSLIP employs Van Jacobson header compression to increase the performance on serial line connections.
- Point-to-Point Protocol (PPP) (RFC 1331, RFC 1332, RFC 1334, RFC 1378) - A host computer that supports PPP can use the DECserver serial port as its network connection. PPP provides error recovery and is a reliable data link protocol.

  Link Control Protocol (LCP) (RFC 1331)-The following LCP options are settable:

  * Maximum Receive Unit-Specifies the maximum sized datagram that both the remote node and the server would like to receive over the link.
  * Async Character Control Map-Specifies which characters require byte stuffing.
  * Password Authentication Protocol (PAP) (RFC 1334) -Provides dial-in security via a PAP packet.
  * Protocol Field Compression-Compresses the HDLC protocol field from two bytes to one.
  * Address and Control Field Compression-Compresses the HDLC address and control fields causing them to be omitted from the frame.

  Internet Protocol Control Protocol (IPCP) (RFC 1332) and PPP IPCP Extensions for Name Server Addresses (RFC 1877), which is the Internet-standard protocol that lets the DECserver pass primary and secondary DNS and WINS name server addresses to PPP dial-in clients-The following IPCP options are settable:

  * IP Addresses-Negotiates IP addresses for both ends of the link and used if the attached device does not support IP Address negotiation.
  * IP Compression Protocol-Supports Van Jacobson's TCP/IP Header Compression (RFC 1144).
  * IP Address-Negotiates IP address for each end of the link.

  AppleTalk Control Protocol (ATCP) (RFC 1378)-The following ATCP options are fixed:

  * AppleTalk Address-Negotiates AppleTalk address for each end of the link.
  * Routing Protocol-Negotiates which routing protocols may be used over the link. Only RTMP and NONE are supported.

* Suppress Broadcast-Peer may request that the server not forward broadcast traffic to the attached host.
* Default Router-Allows the server to inform the attached host what the address is for the default router.
* Zone Information - Allows the server to inform the attached host what the name is for the default zone.

Internet Packet Exchange Control Protocol (IPXCP) (RFC 1552) - The following IPXCP options are supported: Network Address, Node Address, and Routing Protocol. Only RIP and NONE are supported.

- Remote Authentication Dial-In User Service (RADIUS) (RFC 2138, RFC 2139) is an Internet-standard protocol that decribes an open protocol for communicating authentication, authorization, and accounting data between remote access servers and shared authentication servers.
- Call Back Control Protocol (CBCP) is the Microsoft mechanism for supporting dial-back during authentication for Windows 95.

DECserver Operation

The DECserver ROM-based firmware provides the necessary maintenance operation protocols for downloading DECserver software from a TCP/IP host via BOOTP/TFTP, or from a Phase IV or Phase V DECnet load host over the Ethernet into server memory. The DECserver software contains provisions to be loaded from nonvolatile memory (Flash RAM) incorporated in some of the DECserver hardware platforms. All self-test diagnostics are in DECserver ROM and are executed on power-up prior to downloading the server. In the event of a bugcheck caused by a fatal error, the unit will normally attempt to upline dump server memory to the load host. The upline dump is via either BOOTP/TFTP or MOP. Following this, the unit will automatically initialize itself and invoke a download.

The DECserver Network Access Software supports the following modes of operation. Hardware dependencies are noted below:

Hardware	Support Mode of Operation
All DECservers	XON/XOFF flow control
	Block mode transfers up to 2,048 bytes
	Abiltiy to pass break character and error notification
	Data transparency mode
	Digital personal computer file transfers
All DECservers except DECserver 900MC	Data leads only
	DSR/DTR flow control
	Automatic line-speed detection
	Abiltiy to assist in multiple-session management by TD/SMP
	Split-speed (transmit and receive) terminal operation
	DSR logout (automatically disconnects sessions if the terminal is powered down)
	Signal check (checks signal status before and during a session)
	Long break logout (causes the access server to disconnect sessions if RxD is deasserted more than several seconds)
All DECservers except DECserver 90 series	CTS/RTS flow control

DECserver 700-08, 900GM, and 900MC only	Full modem control
	Modem fallback features

Communications-DECserver 90TL and DECserver 90M Hardware Dependent

The DECserver 90TL and DECserver 90M servers support the simultaneous operation of up to eight asynchronous devices at speeds from 75 b/s to 57.6 Kb/s. The DECserver 700-08, DECserver 700-16, and DECserver 900 support the simultaneous operation of up to 8, 16, or 32 asynchronous devices, respectively, at speeds from 75 b/s to 115.2 Kb/s.

The DECserver 90TL and DECserver 90M servers use the DEC-423-A electrical interface standard for local connections, which is compatible with the DEC EIA/TIA-232-E/CCITT V.24/V.28 interface, and supports eight asynchronous devices operating at speeds up to 57.6 Kb/s with DTR/DSR (Data Terminal Ready/Data Terminal Set Ready) signaling. The DECserver 90TL and DECserver 90M can sustain an aggregate character throughput of 30,000 characters per second. The DECserver 90TL and DECserver 90M hardware have eight MJ8 connectors integral to the box. Each port can be individually configured in various modes.

The DECserver 90TL and DECserver 90M DSR and DTR signals can be used to control some modems. The control signals required between a communications server and a modem are determined by the modem and, in some cases, Telecommunications Utility regulations. To provide satisfactory operation, the modem must be configured as follows:

- DSR - The modem must assert DSR when it has connected to an open telephone line and the modem is ready to establish an outgoing call.
- The modem must de-assert DSR when it is not connected to an open telephone line.
- DTR - When DTR is asserted by the server, the modem must be put into a state of readiness for receiving an incoming call, or the modem must be made ready to initiate an outgoing call. When DTR is deasserted, the modem must disconnect from the telephone line and prevent subsequent connections to the telephone line.

Modems that cannot be configured in this way are not compatible with the DECserver 90TL and DECserver 90M servers.

The DECserver 90TL and DECserver 90M servers can operate with a modem that is speed buffering only if the modem and server are configured for XON/XOFF flow control and the data is nonbinary. For binary data communications with a modem that is speed buffering and not configured for XON/XOFF flow control, a communications server with CTS/RTS flow control is needed (such as the DECserver 700).

To run DECserver Network Access Software in a DECserver 90TL server, a DSRVE-SK memory upgrade kit must be installed to increase the available memory to 4 MB. The DSRVE-SK memory upgrade kit is no longer available. Therefore, only DECserver 90TL units that have been previously upgraded can operate DNAS V2.3 software. DECserver 90TL units that have not been upgraded must run DECserver 90TL software.

Communications-DECserver 700/DECserver 900TM Hardware Dependent

The DECserver 700 server is available in two models: the DECserver 700-16 and the DECserver 700-08. The DECserver 700-16 provides attachment for 16 asynchronous devices via MJ8 connectors (also referred to as RJ45 connectors). The DECserver 700-08 hardware has 8 DB25 male connectors integral to the box. The DECserver 900TM provides attachment for 32 asynchronous devices via MJ8 connectors (also referred to as RJ45 connectors). The DECserver 700-16 and DECserver 900TM conform to the DEC-423 electrical interface standard for local connections, and support 2 user-selectable modem signaling options: CTS/RTS/DSR/DTR or RI/DCD/DSRS/DTR. DEC-423 is a superset of EIA-423-A/CCITT V1.0 with some exceptions, and supports longer cable runs and higher signaling speeds. Both DECserver 700 models also support asynchronous devices with interfaces that conform to the DEC EIA/TIA-232-E/CCITT V.24/V.28 interface.

Communications-DECserver 900GM Hardware Dependent

The DECserver 900GM server is configured with 4, 68-pin high-density CHAMP connectors. The DECserver 900GM provides attachment for between 16 - 32 (4-8 per port) devices depending on how the user configures each port. When connecting 8 devices, a port can be configured to conform to the DEC-423 electrical interface standard for local connections, and support 2 user-selectable modem signaling options CTS/RTS /DSR/DTR or RI/DCD/DSRS/DTR. DEC-423 is a superset of EIA-423-A/CCITT V1.0 with some exceptions, and supports longer cable runs and higher signaling speeds. The DECserver 900GM also supports devices that conform to the DEC EIA/TIA-232-E/CCITT V.24/V.28 interface. The DECserver 900GM kit also includes 68-pin to 50-pin adapters for each port that provide a standard TELCO interface for connecting into building wiring.

When connecting into 50-pin TELCO environments only DTR/DSR control signals are supported.

When connecting four devices per port, each connection can support the following control signals RTS/CTS/DSR/ DCD/SMI/DTR/RI/DSRS.

Communications-Decserver 900MC Hardware Dependent

The DECserver 900MC is configured with eight MJ8 connectors. Each connector supports an integral V.34 33.6Kb/s modem. Both MP8 and MP6 phone cables are supported.

Restrictions on DECserver Usage

While terminal connections using the DECserver unit have been designed to simulate direct terminal connections as much as possible, a few differences exist because of the nature of the product. Under most circumstances, these differences are not noticed by terminal users or service node application programs. However, applications that are directly dependent on the following functions may not operate as with a direct connection:

- Applications that depend on reading or setting the terminal speed, character size, and parity by manipulating system data structures
- Applications that depend on an extremely fast response time (typically less than 200 ms) to operate
- Applications that use an alternate terminal driver in the service node
- Applications that expect incoming connections to have fixed device names

HARDWARE REQUIREMENTS

DECserver units not equipped with flash RAM rely on network hosts to load the server software image. Supported load host processors for Open-VMS and DIGITAL UNIX include most VAX, MicroVAX, VAXstation, VAXserver and Alpha models. RISC-based processors include most Personal DECstation, DECstation, and DECsystem models. In addition, load host kits are available for Windows NT and Windows 95 systems.

The following processors are not supported as load hosts: MicroVAX I, VAXstation I, VAX-11/725, VAX-11/782, and VAXstation 8000.

DECserver Hardware

The following DECconnect cables and accessories are available for the DECserver 700:

- H8584-AA MP8 to MMJ adapter
- H8585-AB MJ8 to DB25, low-speed modem adapter
- H8585-AC MJ8 to DB25, high-speed modem adapter
- H8585-AA MJ8 to DB9, adapter for PC interconnect
- DW29-AA AUI-to-ThinWire Ethernet adapter module option

The DECserver hardware requires both a transceiver drop cable and Ethernet connection (H4005 or DELNI) to connect to a Thickwire Ethernet physical channel. The DECserver 700 supports both Thickwire and twisted-pair connections integral to the box. The DECserver 900TM supports Thickwire Ethernet and 10Base-T twisted-pair Ethernet when coupled with its optional docking station.

Both the DECserver 90TL and DECserver 90M servers support ThinWire con- nections integral to the box. The DECserver 90M also supports a 10Base-T connection integral to the box. The DECserver 90TL and DECserver 90M can be connected to a ThickWire Ethernet using an Ethernet transceiver connection, transceiver drop cable, and a repeater (such as a DEMPR or DESPR). Alternatively, the DECserver 90TL and DECserver 90M can be mounted in a DEChub 90 backplane and connected to the Thickwire backplane using a DECbridge 90 or DECrepeater 90FA.

OPTIONAL HARDWARE

Terminals Supported

The DECserver Network Access Software supports the following DIGITAL terminal devices that have keyboards:

- LA12, LA34, LA35, LA36, LA38, LA120
- All VTxxx terminals

Supported terminal parameters are:

- Character size: 7 or 8 bits per character
- Parity: Even, Odd, or None

The automatic line-speed detection (Autobaud) feature is supported for either 7-bit characters with even parity, or 8-bit characters with no parity.

The DECserver Network Access Software also supports DIGITAL Asian terminal device variants when accessed from OpenVMS/Hanzi systems. Refer to the OpenVMS VAX Operating System Software Product Description (SPD 25.01.xx) for a complete listing of supported devices.

Note: This product will also operate on non-DIGITAL terminal devices or personal computers such as terminals supporting VT100 or VT200 like characteristics, and personal computers supporting IBM PC, IBM PC/XT, and IBM PC/AT characteristics.

Printers Supported

The DECserver Network Access Software supports the following DIGITAL asynchronous printers when accessed from OpenVMS systems: All LJ, LA, LQP, LXY, LN0, LG, and DTC printing devices.

The DECserver Network Access Software also supports DIGITAL Asian printer device variants when accessed from OpenVMS/Hanzi systems. Refer to the OpenVMS VAX Operating System Software Product Description (SPD 25.01.xx) for a complete listing of supported devices.

Disk Space Requirements

- For OpenVMS (VAX and Alpha):

  Disk space required 8,500 for blocks use (permanent):

- For ULTRIX:

  Disk space required 4,500 KB for installation and permanent:

- For Microsoft Windows:

  Disk space required 3.4 MB for installation and permanent:

- For UNIX:

  Disk space required 5,000 KB for installation and permanent:

- For DIGITAL UNIX:

  Disk space required 4,500 KB for installation and permanent:

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

CLUSTER ENVIRONMENT

This layered product is fully supported when installed on any valid and licensed VAXcluster[1] configuration without restrictions. The HARDWARE REQUIREMENTS section of this product's Software Product Description details any special hardware required by this product.

SOFTWARE REQUIREMENTS

DECserver units not equipped with Flash RAM rely on network hosts to download the server software image. Supported operating systems include OpenVMS VAX, OpenVMS Alpha, DECnet/OSI for OpenVMS, ULTRIX, Windows NT, Windows 95, DIGITAL UNIX, as well as many generic UNIX operating systems. The following table list the minimum version of these operating systems that are supported load hosts. In general, all later versions of these operating systems can provide load host support. However, support for all later versions is not guaranteed.

Operating System /Software	Miminum Version Required
DECnet OSI for OpenVMS operating system	Version 5.5
DIGITAL UNIX operating system	Version 1.0
Microsoft Windows 95 operating system	Not applicable
Microsoft Windows NToperating system	Version 3.51

Version 5.x VAXcluster configurations are fully described in the VAXcluster Software Product Description (SPD 29.78.xx) and include CI, Ethernet, and Mixed Interconnect configurations.

Operating System/Software	Miminum Version Required
MOP software	Version 4.2 (included with ULTRIX operating system)
OpenVMS VAX operating system	Version 5.0
ULTRIX operating system	Version 4.0

For UNIX systems:

The following generic operating systems are supported. Complete support cannot be granted on systems where customization has taken place. In addition, some UNIX implementations, other than those in the following list, may operate successfully, but no support is implied.

BOOTP/TFTP-One of the following:

Operating_System	Version
SunOS	Release 4.0
DIGITAL UNIX	Version 1.0
IBM AIX	Version 3.1.1
SCO UNIX System V	Release 3.2 V2.0 /386
HP-UX	Version 8.0

Some System V systems, such as HP-UX and SCO, may not support the upline dump of server memory.

OpenVMS Tailoring:

For OpenVMS Version 5.x systems, the following OpenVMS classes are required for full functionality of this layered product:

- OpenVMS required saveset
- Network support
- Utilities

GROWTH CONSIDERATIONS

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

DISTRIBUTION MEDIA

For all platforms: Multiple Operating system CD-ROM

ORDERING INFORMATION

Software License: QM-0LWAA-BA

Software Media with documentation on CD-ROM: QB-0LWAA-WA

Software Documentation (Hardcopy): Softcopy documentation is provided with the CD-ROM. Hardcopy documentation: QA-0LWAK-GZ

Software Product Services: QT-0LWA*-**

Update License: QM-0LWAA-BB[1]

*Denotes variant fields. For additional information on available licenses, services, and media, refer to the appropriate price book.

1 A software license for DNAS is included with all DECserver 90M, DECserver 700, and DECserver 900 units. This license is not version specific. Customers with such units do not need to purchase a license for DNAS or an update license for later version of DNAS software. Early versions of the DECserver 700 were sold with DECserver 700 software. These units can be upgraded to run DNAS software with the purchase of a update license. In most cases these DECservers will require a memory upgrade to 4MB of DRAM as well. Option number DSRVW-UB includes both the 4MB SIMM memory and the update license.

SOFTWARE LICENSING

This software is furnished under the licensing provisions of Cabletron Syystems Standard Terms and Conditions. For more information about Cabletron's Systems licensing terms and policies, contact your local Cabletron Systems office.

The DECserver Network Access software license applies to the DECserver unit on which the server software runs, not to service host node CPUs in the network.

This product does not provide support for the OpenVMS License Management Facility. A Product Authorization Key (PAK) is not required for installation or use of this version of the product.

SOFTWARE PRODUCT SERVICES

A variety of service options are available from DIGITAL. For more information, contact your local DIGITAL office.

SOFTWARE WARRANTY

Warranty for this software product is provided by DIGITAL with the purchase of a license for the product as defined in the "Networks Products Warranty and Service Information".

The above information is valid at time of release. Please contact your local Cabletron Systems office for the most up-to-date information.