DigitalNetworks

RN-DNAS0-00

Digital Network Access Server Software
Version 3.6 BL01
Release Notes
July 2007

This document is the Release Notes for the Network Access Server Software Version 3.6 for Windows 9x/me/2000/NT/XP/2003 Server, Tru64 Unix, and OpenVMS (VAX and Alpha).

Contents

Media Content

The Network Access Server Software CD is now formatted ISO 9660 for all platforms.

The media contains:

1. Network Access Software, binary images for the variants of the DECserver products.
2. Access Server Manager, a Windows 9x/me/2000/NT/XP remote management tool for the DECserver products.
3. Digital Networks Remote Access Security Server supported on Windows NT, Tru64 Unix, and OpenVMS (VAX and Alpha).
4. Digital Networks Remote Access Security Server Manager supported on Windows 9x/me/2000/NT/XP.
5. Documentation for the above software.

OpenVMS and Tru64 Users, Please Read

OpenVMS

The CD-ROM building process made it necessary to take steps to protect the file characteristics during the mastering process. For this release, we put the OpenVMS kits into containers.

The installation savesets are compressed into one saveset and then placed into two self-extracting OpenVMS VAX and an OpenVMS Alpha executables.

Please add the following steps to the installation procedures located in the *Network Access Software Installation Guide*:

- After mounting the CD-ROM, copy the appropriate self-extracting executable for your platform type from the CD-ROM (DNASVAX.EXE, DRASVAX.EXE, DNASAXP.EXE, and DRASAXP.EXE) to a directory on your VMS system.

- Execute the program. The result is DNAS036.BCK and DRAS024.BCK files, an OpenVMS BACKUP saveset.

- Perform a BACKUP DNAS036.BCK/sav *.* and BACKUP DRAS024.BCK/sav *.* to extract its contents.

- Follow the remaining steps as outlined in the installation instructions, but direct the directory path to your current location.

Tru64 Users

The Tru64 kits are now placed in a tar file; note that only DRAS.tar is supported.

Add the following steps to the installation procedures in the *Network Access Software Installation Guide*.

- After mounting the CD-ROM, copy the DRAS.tar file from the DUNIX directory on the CD-ROM to a directory on your DUNIX system.
- Extract the contents of the tar DRAS.tar file. The result is folders containing an installable kit.
- Follow the remaining steps as outlined in the installation instructions, but direct the directory path to your current location.

DNAS Software Release History

Status	Version No.	Type	Release Date
Current Version	3.6	Customer/Software	July 2007
Previous Version	3.5	Customer/Software	March 2007
Previous Version	3.4	Customer/Software	November 2006
Previous Version	3.3	Customer/Software	July 2006
Previous Version	3.2	Customer/Software	June 2005
Previous Version	3.1	Customer/Software	November 2004
Previous Version	3.0	Customer/Software	April 2004

Hardware Compatibility

For DECservers 700-8, 700-16, 900TM: any version of WWENG2.SYS.

For DECservers 708: Version 2.6 BL52 or later of WWENG2.SYS.

For DECservers 716 and 732: Version 2.4 or later of WWENG2.SYS.

For DECserver 90M+: Version 2.6 BL53 or later of MNENG4.SYS.

For DECserver ConX^4: Version 3.1 BL02 or later of MNENG4.SYS.

BOOTPROM Compatibility

To take full advantage of the software features available in this V3.6 release of the Access Server Software the following minimal Boot ROM versions are necessary on the products:

- Version 7.2 or later for the DS700-8, DS700-16, DS900TM.
- Version 2.0 or later for the DECserver 90M+. (Reference the DECserver 90M+ Installation Guide for the details of updating the DS90M+ firmware.)
- Version 7.4 or later for the DECserver 708.
- Version 7.3 or later for the DECserver 716 and DECserver 732.
- Version 2.6 or later for the DECserver ConX^4

If necessary, please contact your service representative for upgrading your Boot ROM version. Some ROM upgrades are not customer or field installable and may require returning the unit to the vendor.

Network Management Software Support

The Access Server supports remote management through the following:

- Remote management CLI interface that you access using Telnet or MOP protcols.
- Windows-based management tool, Access Server Manager.
- clearVISN Network Management Software
- Access Server Software's SNMP agent

Enhancements and Bug Fixes

The V3.6 release of DNAS software includes the following changes:

Enhancements:

- Removed the requirement of assigning a TCP Port of 23 to a Listener having a unique IP Address assigned. The Software now allows any TCP Port number ranging from 1 to 65535 to be assigned.
- Added the ability to save and restore the DECserver characteristics to/from a PCMCIA Flash Rom.

  Command Syntax:

  ```
  SAVE {SERVER} CONFIGURATION
  ```

  Saves the Server's configuration from a removable PCMCIA Flash Card.

  ```
  RESTORE {SERVER} CONFIGURATION
  ```

  Restores the Server's configuration from a removable PCMCIA Flash Card.

  Please note:

  These commands are valid on those servers which support the removable PCMCIA Flash Card.

  Because of the potential differences there may be in configurations in platform types and the version of DNAS Software, this command will fail if the configuration stored on the PCMCIA Flash Card was not stored by an identical platform type or an identical version of DNAS Software as the version running on the server being restored.

  A restore will not change the IP Address and Subnet Mask.

  After being restored the server will need to be initialized before some of the configuration settings will be used.

A show memory now displays the configuration saved. The configuration saved
will not be displayed if:

- A PCMCIA Flash Card is unsupported
- The Flash Card is not present
- The configuration wasn't written
- The manufacturer and device ID can't be read (Intel Series II with write protect enabled doesn't return a manufacturer and device ID).

```
Local> SHOW MEMORY

    Dynamic RAM:                    8 M bytes

    Non-Volatile RAM:               128 K bytes

    Flash RAM:
            Installed:              Yes
            Total size:             2 M bytes
            Boot block:             Valid
    Load Image:
            Name:                   WWENG2
            Size:                   1725584 bytes
            Version:                Network Access SW V3.6 BL01

    Configuration:
            Platform:               DECserver 732
            SW Version:             V3.6 BL01
```

Please note:

An Intel Series 2 Flash Card having the write protect switch enabled will not return the correct data read of the Manufacturer and Device ID. Without the IDs the Software cannot determine the sector size and from where to obtain the configuration data. The last three lines of the show memory displaying the Configuration will be cleared when an Intel Series 2 Flash Card's write protect switch is enabled.

- Added the ability to assign a unique password to a port to be used during a remote access.

Command Syntax:

```
{SET   } PORTS LOGIN PASSWORD{ENABLED }
{DEFINE}                     {DISABLED}  *
{CHANGE}                     {password-string}
```

ENABLED user must enter login password.

DISABLED user is not prompted for a password.

password-string is a quoted string between 1 and 16 characters. A quoted string of no characters, "", clears the characteristic.

Implementation:

The PORTS LOGIN PASSWORD command was expanded to take a quoted string. The LOGIN parameter in the command is no longer optional.

The PORTS LOGIN PASSWORD string,when configured, will be used in place of the SERVER LOGIN PASSWORD string.

The PORTS LOGIN PASSWORD string, when configured ,will be used in conjunction with the SERVER REMOTE PASSWORD string, if so configured.

The pound sign '#' character will still be displayed to prompt for the login password for a local session.

In an effort to remove some confusion when the PORTS LOGIN PASSWORD is being used in conjunction with the SERVER REMOTE PASSWORD, a pound sign '#' prompt will still be used to prompt for the SERVER REMOTE PASSWORD and a single carrot '>' prompt will be displayed to prompt for the PORTS LOGIN PASSWORD string for a remote session.

Bug Fixes:

- An UNKNOWN FLASH DEVICE ID message is displayed during an initialization if the PCMCIA Flash Card write protect switch is set to ENABLED. The software now displays a message indicating the Flash Card is write protected.

The V3.5 release of DNAS software includes the following changes:

Enhancements:

- Device Discovery is a new feature added to DNAS and supported by ASM. This new software feature allows users to easily find and identify DECserver products deployed in their network. This feature eases the task of adding newly deployed or existing DECserver products to the ASM database. In response to a request message from ASM, each DECserver on the user's network responds with its Name, IP address and Product Type. Note: DECservers must be running DNAS V3.5 firmware.
- A FTP client has been added to the DNAS software, which provides users with a third method (in addition to TFTP and MOP) for loading DNAS software and/or the device bootrom. This applies to those DECserver models that support a firmware download into a Flash ROM, currently the DECserver 90M+ and ConX4.
- A ZERO COUNTER command has been added. This allows the user to clear the high counters (except for Highest CPU Used) that are displayed when the SHOW SERVER STATUS command is used.
- A timestamp feature has been added to the Event Notification system. If the real time clock feature of DNAS is active, then date/time is included in the notification messages. If the real time clock feature is not active, then the system uptime is used.

Bug Fixes:

- Resolved issue with Event Notification command line prompt. DNAS would accept "SET NOTIF" as a valid command when it should not.

The V3.4 release of DNAS software includes the following changes:

Enhancements:

- Support for the Event Notification System. DECserver Event Notification provides 24/7 monitoring of critical serial device events coupled with an immediate notification whenever an event occurs. Event Notifications can be delivered as email, cell phone, pager, PDA or to any SMTP device. For more informations see chapter 18 of the Management Guide and for command details see the Command Guide.

Bug Fixes:

- In the DHCP protocol messages, the Client ID was not configured the ‘typical way.” The MAC address was part of the Client ID but the device type and the parameter length were not the typical values. (The implementation was not a violation of the standard. It was just different from what most vendors do.) This caused the Microsoft DHCP servers to display an extra ‘0’ byte after the address. This extra byte was also needed when configuring a fixed lease. The fix was to put in the correct device type and adjust the Client ID parameter length in all DHCP messages that contain the Client ID. The end result is that the DHCP server now sees the (6 byte MAC address as the Client ID.

The V3.3 release of DNAS includes the following changes:

Enhancements:

- Support for RFC-2217 an extension to the Telnet protocol for remote configuration of port characteristics.
- Support for SNTP (RFC 2030) added to synchronize the DECserver with NTP servers on the LAN. The feature allows for communication to a primary and secondary NTP server on the LAN through a SNTP unicast client. The internal time is updated based upon the network packets received from the NTP server. Features associated with the time configuration such as daylight savings time and time zone permit the administrator advanced features for maintaining their DECserver.
- Obtain server’s internal characteristics from a DHCP server including IP address, subnet mask and DNS address.
- Wizard Updated to support DHCP.

Bug Fixes:

- On the ConX4 product, there was a problem adding some muticast addresses to the driver database. This resulted in a failure to deliver frames from these multicast addresses to the user.

- Under certain error conditions (e.g. excessive Ethernet collisions) the ConX4 would disable the transmission of Ethernet frames from the device. The only recovery was to reboot the ConX4.
- In certain configurations, the IP address from a ARP packet was not being set correctly in the DECserver. This problem resulted in the loss of communication between the DECserver and the Ethernet network.
- CLEAR/PURGE INTERNET LOCAL, ROOT and ALL is displaying a "Local -425- Internet host not known" if there are no nameserver entries in a database.
- An incorrect value for ifSpeed was being returned for the interfaces.
- The factory default value for Appletalk cache size was incorrect (0) for a ConX^4.
- The system clock was off a little less than a second per minute on the DS90M+ and ConX.
- Edits to the help displays.
- The PURGE INTERNET HOST ALL command returned a HOST_NOT_FOUND error when no hosts were configured and an error message was being displayed. Now returns success with no message. Added Internet Address Learned to the wizard command's internet setup.
- The INIT FACTORY command is now supported for the DS90M+ and ConX.

Restrictions and Limitations

This release of the Access Server Software and Firmware has the following restrictions and limitations:

- The DECserver must have a local IP address at the time TFTP load requests are issued. This Address may come from the DECserver’s NVRAM, for example, a DEFINE INTERNET ADDRESS Command, from the Mini-Monitor, for example, a set IP address command (>>> s ip = nnn.nnn.nnn.nnn), or from a BOOTP or DHCP reply packet. In the case of Directed TFTP, the latter option does not apply.
- If the TFTP server is not located in the same IP LAN subnet (i.e. reachable using ARP), then the DECserver must have a default gateway IP address configured. This address may come from the DECserver’s NVRAM, i.e. a DEFINE INTERNET GATEWAY command, from the Mini-Monitor, for example, the set gateway command (>>> s gw = nnn.nnn.nnn.nnn), or from a BOOTP reply packet. In the case of Directed TFTP, the latter option does not apply.
- The DECserver must have the load image file name configured to perform a TFTP load. Typically the DECserver stores only the filename without any path information or file extension. The fully qualified pathname is typically specified by the BOOTP reply packet. In the case of Directed TFTP, the filename may come from the DECserver’s NVRAM, for example, the DEFINE SERVER SOFTWARE command, or from the Mini-Monitor, for example, the >>> b eth:<filename> Command. It is recommended that the server be configured with a default directory that Contains the DECserver load image files.
- You may receive a timeout status message on the DECserver physical console port. If network connectivity is poor, the firmware will continue to retry, but the download may not ever complete successfully. There is nothing that the user can do at the DECserver to solve this kind of problem, other than to select an alternate load protocol and/or alternate load host if such is available.

- If your TFTP server host operating system uses case-sensitive file names, be sure that the filenames of the DECserver load images match the name the DECserver requests via TFTP. Note that the DECserver will typically request a file by name only, with no path or file extension Information. Use the restricted mode of TFTP daemon on UNIX systems with the restricted file system pointing to the directory in which the DECserver load images exist. In the DECserver ROM Mini-Monitor, you may specify a long pathname for the load image (e.g. /usr/tftpboot/MNENG2). When you define the load image name in DECserver NVRAM, you are restricted to 9 characters. While it is possible to use a quoted string to provide a path name, the length is restrictive (e.g. /u/t/MNENG2 is too long).

Any other problems than those listed above should be reported to our Technical Support Staff.

MIB and RFC Information

IETF STANDARDS MIB SUPPORT

RFC No.	Title
RFC 1243	Definitions of Managed Objects for the AppleTalk
RFC 1213	Management Information Base (MIB-II) for Internet protocol suite management
RFC 1158	Obsolete MIB-II for backward compatibility
RFC 1316	Definitions of Managed Objects for Character Stream Devices, the Character MIB
RFC 1317	Definitions of Managed Objects for RS232-like Hardware Devices, the RS-232-like MIB
RFC 1284	Definitions of Managed Objects for Ethernet
RFC 1471	Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol
RFC 1473	Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol
RFC 2030	Simple Network Time Protocol Client (SNTP)
RFC 2217	Telnet COM Port Control Option
DEC-DECserver-Accounting	Definitions of Managed Objects for the DECserver Accounting Objects

RADIUS SUPPORT

RFC No.	Title
RFC 2138	Remote Authentication Dial-In User Service (RADIUS)
RFC 2139	RADIUS Accounting protocol enhancement that reports a number of termination reason codes to the RADIUS server when user sessions are completed.

SNMP SUPPORT

RFC No.	Title
RFC 1155	Structure for Management for TCP/IP-Based Protocols
RFC 1157	Simple Network Management Protocol (SNMP)

SNMP TRAP SUPPORT

Cold Start, Line up, Line Down, Authentication

Documentation

Documentation files contained within the media:

The manuals are in Adobe Acrobat Reader (.PDF) format. The latest version of the Acrobat Reader, as well as updates, may be obtained from the Adobe Systems Internet web site: http://www.adobe.com/products/acrobat/.

Document	Title
MG-DNAS0-00.pdf	*Network Access Software Management Guide*
CG-DNAS0-00.pdf	*Network Access Software Commands Reference Guide*
PG-DNAS0-00.pdf	*Network Access Software Problem Solving Guide*
IG-DNAS0-00.pdf	*Network Access Software Installation Guide*
RN-DNAS0-00.pdf	*Network Access Software Release Notes*
MG-DRAS0-00.pdf	*Digital Networks Remote Access Security User's Guide*
IG-DRAS0-00.pdf	*Digital Networks Remote Access Security Installation Guide*

Description of Documents

Document	Description
Digital Networks Remote Access Security User's Guide	Explains how to use Digital Network's Remote Access Security (DRAS) to manage a DRAS server and its database.
Digital Networks Remote Access Security Installation Guide	Explains how to install Digital Network's Remote Access Security (DRAS) and its management software.
Network Access Software Management Guide	Details the tasks you perform to configure and manage your access server.
Network Access Software Command Reference Guide	Describes the commands to operate and manage the access server.
Network Access Software Problem Solving Guide	Describes problem-solving tools and procedures for the various access servers.
Release Notes	This document. Provides the latest information about the access server. The release notes are available with the software distribution kit and are stored in the load host directory with the other software distribution files.
Access Server Manager Online Help	Help is available for the Access server Manager using its on-line help. Help describes how to perform management and configuration tasks.

Accessing Online Information

Support Services

To locate product-specific information, information about our other products, or product warranty information refer to the following Digital Networks web sites at:

http://www.digitalnetworks.net/

To contact us by mail:

Digital Networks
20 N. Wentworth Ave.
Londonderry NH. 03053-7438
USA

To contact us by phone:

Digital Networks' U.S. headquarters is open Monday - Friday, 8:00am - 5:00pm EST.

Sales HOTLINE: (603) 216-6066
Customer Service: (603) 216-6064
Corporate Telephone: (877) 341-9594

Digital Networks, 20 N. Wentworth Ave. Londonderry NH. 03053-7438

Web site: **http://www.digitalnetworks.net**