Patch Level Notice:

DG/UX for AViiON Systems
Patch Level op-sys-x_5.4R2.01.931008

November 1993

Part Number 017-600051-00

This Patch Level Notice applies to Models:
P001
Q001

Restricted Rights Legend:

Use, duplication, or disclosure by the U.S. Government is
subject to restrictions as set forth in subparagraph (c)(1)(ii)
of the Rights in Technical Data and Computer Software clause at
[DFARS] 252.227-7013 (October 1988).

DATA GENERAL CORPORATION
4400 Computer Drive
Westboro, Massachusetts 01580

Unpublished — all rights reserved under the copyright laws of
the United States.

Copyright © Data General Corporation 1989, 1990, 1991, 1992, 1993.
All Rights Reserved.
Licensed Material — Property of Data General Corporation.
This software is made available solely pursuant to the terms
of a DGC license agreement which governs its use.

DG/UX is a trademark of Data General Corporation.
AViiON is a registered trademark of Data General Corporation.
The X Window System is a trademark of Massachusetts Institute of Technology.
OSF/Motif is a trademark of Open System Foundation.
Ethernet is a registered trademark of Xerox, Inc.
SunOS is a trademark of Sun Microsystems, Inc.
ONC/NFS is a registered trademark of Sun Microsystems, Inc.
UNIX is a registered trademark of UNIX Systems Laboratories

1. Introduction

This Patch Level Notice describes Patch Level op-sys-x_5.4R2.01.931008 for 5.4R2.01 DG/UX™ Systems running on Data General's family of AViiON™ computers. In addition, this notice also includes information not currently available in the product manuals (e.g., information developed after the current manuals were printed, or corrections to current manuals).

This printed notice always accompanies the software. You may print additional copies of this notice after you have installed the product. A copy suitable for line printers can be found in the file /usr/release/op-sys-x_5.4R2.01.931008 .pn. In the event of differences between the printed copy of the notice and the copy on the distribution medium, the printed copy takes precedence.

This Patch Level consists of the following parts:

Part Description	Part Number
DG/UX for AViiON Systems Patch Level op-sys-x_5.4R2.01.931008 Notice	017-600051-00
DG/UX for AViiON Systems Patch Level op-sys-x_5.4R2.01.931008 Media	079-600351-00

2. Product Description

2.1 Individual Patches

For DG/UX Revision 5.4R2.01, Data General releases patches named and numbered on a per product basis. The products included in this convention are, but are not limited to, dgux, tcpip, nfs, X11, X11.lg, aview, and gcc. As needed, Data General will produce and deliver individual patches in response to Software Trouble Reports. Using the product DG/UX Revision 5.4R2.01 the naming convention is:

dgux_5.4R2.01.pmm

where mm refers to the individual patch number for the product. Per product patch numbers are unique and always increase numerically.

During the support period for a product, it may be necessary to release multiple patches that replace the same file. In this case, a later patch will contain all fixes released in previous patches; therefore when you have two patches to the same file, always load the patch with the higher number. The patch with the lower patch number is superseded and will not appear in the next product patch level. In general, however, patches which do not replace previously modified files are separate entities (ie. not cumulative).

2.2 Product Patch Levels

When a sufficient number of individual patches has been generated, they are collected into a patch level on a per product basis. A product patch level is assembled as a single sysadm loadable package. For example, all the current applicable patches for DG/UX Revision 5.4R2.01, are assembled in one package using the following naming convention:

dgux_5.4R2.01.nn

where nn is the patch level number, corresponding to the greatest individual patch number for dgux available in this patch level. Note that the "p" in the individual patch naming convention is dropped in this case. Product patch levels are cumulative, thus you should load only the product patch level file with the greatest number.

2.3 Patch Level op-sys-x

A collection of product patch levels are made available as an op-sys-x patch level for easier distribution. The op-sys-x patch levels are named using a date in the naming convention instead of a revision number. This should better ensure you have the latest patch level. The name is of the form:

op-sys-x_r.r.r.yymmdd

where r.r.r is the release number and yy, mm, and dd correspond to the year, month and day, respectively. This op-sys-x Patch Level is named:

op-sys-x_5.4R2.01.931008

Op-sys-x patch levels are cumulative, thus you should load only the most recent op-sys-x patch level. This op-sys-x patch level is a sysadm loadable tape which contains one product patch level per sysadm loadable package. The packages on this op-sys-x_5.4R2.01.931008 Patch Level are:

Package 1: dgux_5.4R2.01.59
Package 2: tcpip_5.4R2.01.09
Package 3: nfs_5.4R2.01.06
Package 4: X11_5.4R2.01.03
Package 5: networker_5.4R2.01.01

Do not install networker_5.4R2.01.01 if you are running multi-client Networker (Q017A). See section 6.1 for further details.

For each product you have loaded on your system, you are directed to load the corresponding product patch level (package). See the section titled "Installation Instructions" later in this document for specific loading instructions.

Every user is directed to load package number 1, the DG/UX product patch level. After this package has been loaded, the /etc/issue file reads as follows:

DG/UX Operating System Level 5.4R2.01.59

3. Environment

3.1 Hardware

Patch Level op-sys-x_5.4R2.01.931008 of the DG/UX System will run on Data General AViiON series machines with revision E.2 or later of the MC88100 processor and a minimum of 12 MB of main memory, at least 322MB of disk storage, a system console (or graphics monitor for workstations), and a tape drive (for software distribution). On workstations, 16MB of main memory is recommended.

Patch Level op-sys-x_5.4R2.01.931008 of the DG/UX System may also be run on a "diskless" AViiON workstation. This requires a console or workstation monitor, but does not require any disk or tape drive units.

3.2 Software

Your system needs to be running DG/UX 5.4R2.01 System software. Apply this patch ONLY on DG/UX Revision 5.4R2.01.

4. Patches

The subsection headings below correspond to the individual patch numbers that are included in this op-sys-x patch level. Where it appears that a patch has been omitted because the numbering is not consecutive, consider that patch to be superseded and the fix included in a succeeding patch.

For those systems that have loaded individual DG/UX Revision 5.4R2.01 patches or extensions, follow this outline to determine if you need to reload any previously applied single patches.

> If previously applied patches, patch levels, or extensions are included in this op-sys-x patch level, then they will be properly overwritten.
>
> If previously applied patches are not included in this op-sys-x patch level AND have an individual patch number greater than the patch level number, then they must be reloaded. For example if you have installed the patch dgux_5.4R2.01.p60, then it must be reloaded, because its patch number, p60 is greater than the patch level number 59, dgux_5.4R2.01.59, for this patch level.
>
> If previously applied patches are not included in this op-sys-x patch level AND have a patch number less than or equal to the patch level number, then these patches have been either superseded by another patch in this op-sys-x patch level or obsoleted and do NOT need to be reloaded. For example, the patch dgux_5.4.2.p06 is not listed below as being included in this op-sys-x patch level and its number, 06 is less than or equal to the patch level number 59, dgux_5.4R2.01.59, therefore it does not need to be reloaded.
>
> If previously applied patches or extensions are not included in this op-sys-x patch level and appear to conflict with this op-sys-x patch level, call the Customer Support Center for assistance.

4.1 Package 1 - Product Patch Level dgux_5.4R2.01.59

DG/UX patch level dgux_5.4R2.01.59 is described below:

4.1.1 dgux_5.4R2.01.p02

Patch dgux_5.4R2.01.p02 corrects a problem with ksh(1) arrays when assigned with the "set -A <array> <value>" syntax. If a one element array is assigned as described, then "print ${#<array>[*]}" returns the number of characters in the array value instead of the number of values in the array. For example, if the array "foo" is set to the one element value of "bar", "print ${#foo[*]}" returns 3 instead of 1.

When installing this patch, be sure you are running the Bourne shell, sh(1), or the C shell, csh(1), and NOT the KornShell, ksh(1).

4.1.2 dgux_5.4R2.01.p04

Patch dgux_5.4R2.01.p04 corrects a problem with the taccess(1) and twrite(1) commands used by Reelexchange. If the /etc/passwd file is close to or larger than approximately 3000 bytes, a portion of Reelexchange's memory is corrupted by taccess(1). When twrite(1) accesses this portion of memory it displays the message "Error: user label nnnnnnn - unknown Label Identifier" errors correctly.

4.1.3 dgux_5.4R2.01.p05

Patch dgux_5.4R2.01.p05 corrects a problem which can lead to the occurrence of a panic 13000057 when using fast recovery file systems. This problem occurred when a data element was not cleared as it should have been during the

handling of a file truncation.

See the Load section for special loading instructions.

4.1.4 dgux_5.4R2.01.p08

Patch dgux_5.4R2.01.p08 corrects a problem which causes a 2000110 panic to occur when a zero length message is sent to a UNIX domain socket. This has been corrected by not allocating or freeing a memory buffer for this message if the length of the message is zero.

4.1.5 dgux_5.4R2.01.p09

Patch dgux_5.4R2.01.p09 corrects a problem where sar is outputting "dgux restarts" instead of meaningful sar output.

4.1.6 dgux_5.4R2.01.p10

Patch dgux_5.4R2.01.p10 is a new release of the firmware for the VLCi Ethernet LAN Controller (CMC-130). It corrects a problem where the firmware would not process a frame correctly if it was larger than the maximum size allowed on the ethernet. Although it may be legal to transfer a frame larger than 1514 bytes on a LAN, it will be discarded by TCP/IP. Sometimes a network failure may cause a frame to be corrupted/extended and this may also appear to be a ethernet frame larger than 1514 bytes to the controller.

Without this patch installed, the VLCi controller will appear to hang if a ethernet frame it received (via broadcast or direct addressing) and can only be recovered by rebooting the kernel. Stopping and starting TCP/IP will not recover the controller.

TCP/IP must be stopped and restarted for this patch to take affect.

4.1.7 dgux_5.4R2.01.p15

Patch dgux_5.4R2.01.p15 corrects a bug in the lfm.a kernel library which caused file record locks to be (incorrectly) released when a file was unlinked or a directory removed. This caused improper program execution.

4.1.8 dgux_5.4R2.01.p17

Patch dgux_5.4R2.01.p17 corrects a problem in the faam.a kernel library which causes a panic code 3000011. This panic occurs because a routine in this library does not properly handle FIFO objects when clearing signal requests.

4.1.9 dgux_5.4R2.01.p19

Patch dgux_5.4R2.01.p19 eliminates a panic from occurring when an NFS server receives a packet from a user that has more than 16 supplementary group IDS. The panic code will most often be 3000032 or 2000075 but other panic codes can occur. Like DG/UX, most UNIX operating systems limit the number of supplementary group IDs to 16. This patch corrects the panic from occurring when communicating with an operating system supporting more than 16 supplementary group IDs.

4.1.10 dgux_5.4R2.01.p20

Patch dgux_5.4R2.01.p20 corrects 2000075 panics which occur as the result of referencing an unwired routine while performing a system shutdown. This problem is corrected by calling the routine in question earlier in the shutdown process.

4.1.11 dgux_5.4R2.01.p21

Patch dgux_5.4R2.01.p21 corrects 41000050 panics which occur as the result of a bug in the su.a kernel library. The panics are due to the dupb() streams routine not checking the streams message datablock reference count prior to incrementing that count.

4.1.12 dgux_5.4R2.01.p22

Patch dgux_5.4R2.01.p22 corrects a problem with installing or upgrading to DG/UX 5.4 Release 2.01 using a remote tape drive. There exists a problem with the stand-alone diskman on the released DG/UX 5.4 Release 2.01 tape. When attempting to load the DG/UX system software over the network with diskman, ifconfig reports the error "invalid subnet mask or broadcast address: ioctl (SIOCGIFFLAGS)" after entering the subnetting network mask for the local host. The ifconfig command fails because diskman creates the network device node with incorrect device numbers. The patch delievers a new diskman for DG/UX 5.4 Release 2.01.

4.1.13 dgux_5.4R2.01.p23

Patch dgux_5.4R2.01.p23 corrects a problem with the runtime dynamic linker, rtld, core dumping if the dlopen(3X) library routine is used to open multiple shared objects at the same time.

In addition, this patch corrects a problem where a shared application may fail with the error "dynamic linker: prog: symbol not found: func", where prog is the name of the program and func is the name of the function, when the application opens multiple shared library files using the RTLD_LAZY option to dlopen(). The error is reported at runtime when a routine in one shared library attempts to invoke a routine in the other shared library.

4.1.14 dgux_5.4R2.01.p27

Patch dgux_5.4R2.01.p27 corrects a problem with the shell layering program, shl, being unusable due to stty/shl interaction. This patch should be installed on all DG/UX 5.4 R2.01 systems where the shell layering program (shl) will be used.

4.1.15 dgux_5.4R2.01.p29

Patch dgux_5.4R2.01.p29 changes the functionality of admuser(1M) and the sysadm function User -> Login Account -> Modify for the case where an administrator chooses to change the user's home directory. In the past when this option was executed, the files owned by the user whose home directory was being changed were moved and the previous home directory was deleted, regardless of whether it contained other files.

With the application of this patch an attempt is made to copy the files in the old home direcotry owned by this user to the new home directory. As this is a copy operation, the old home directory and its contents are undisturbed by the operation. If removal of files from the old home directory is necessary, it must be done manually.

4.1.16 dgux_5.4R2.01.p31

Patch dgux_5.4R2.01.p31 corrects a problem when reading a CD-ROM containing Rock Ridge format. The problem resulted in a 2000075 panic when the directory structure was being accessed.

4.1.17 dgux_5.4R2.01.p33

Patch dgux_5.4R2.01.p33 corrects a problem whereby a process running on the duart port of the AV/46XX series computer may hang. This patch works around a problem with the duart chip to prevent the hang.

4.1.18 dgux_5.4R2.01.p34

Patch dgux_5.4R2.01.p34 corrects a problem with config not building the conf.c entries correctly causing mismatches on opens of cloneable devices. The typical error will be "race condition between clone open/open on stream". This has been seen when a netware daemon tries to open device /dev/ipx.

4.1.19 dgux_5.4R2.01.p36

Patch dgux_5.4R2.01.p36 corrects several problems in failover operations.

First, this patch addresses some performance problems. Three operations provided by the -o option are noticeably slow when takeaway and/or giveaway databases are large. These operations are sync, give, and take. This patch to admfailoverdisk(1M) corrects a logic error and speeds up these operations.

There have been some reports where the processing of a takeaway database of approximately 200 entries has taken on the order of 20 minutes after a machine failover. These fixes to admfailoverdisk(1M) reduce the time to a matter of seconds, rather than minutes.

Further corrections have been made to the "admfailoverdisk -o take -h host" so that it is no longer 4 to 6 times slower then the analogous "admfailoverdisk -o give -h host" operation.

Second, this patch lifts an artificial limitation placed on the number of physical disks to be failed over. A symptom of this problem is that after a "give" operation to a remote machine, the giveaway and takeaway databases on the remote machine are not correct. The giveaway database contains only a subset of those disks which were failed over and the takeaway database contains the remainder. With this correction the giveaway database now contains all the disks failed over.

Finally, it corrects a problem in the processing of a giveaway or takeaway database when admfailoveridisk -o give or admfailoverdisk -o take are executed. Both of these operations use a routine to sort file systems entries associated with the giveaway/takeaway entries. If the total number of entries with a file system associated with them in a giveaway or takeaway database is greater than or equal to 64, then admfailoverdisk produces a core dump. Part of the information stored in an entry in /etc/failover/giveaway and /etc/failover/takeaway is a logical disk name and piece number. If this logical disk contains a file system, then it is counted against the total of 64. If the logical disk field is a single piece of a multi-piece logical disk, then it also counts against the total. Thus a giveaway file which contains entries for a 6 piece logical disk, on which a file system resides, counts as 6 entries. With the application of this patch, the limit rises to 2048, and the core dump no longer occurs.

4.1.20 dgux_5.4R2.01.p39

Patch dgux_5.4R2.01.p39 corrects a problem with systems which have installed the NVRAM Model 5018VEM[-K] card and have the kernel configured to use the cdm() and nvrd() devices (Cache Device Manager and Non Volatile Ram Driver). The system will appear to hang, but can be interrupted with a hot key sequence to force a panic. User processes may appear to hang and then when a kernel process pends waiting on those hung processes the system will appear to hang.

This patch also corrects LDU downgrades to readonly mode to prevent possible data corruption (attributed to operation of the cdm.a kernel library). The problem is corrected by requiring a buffer lock to be held while testing the current state of the buffer. This will prevent a cache device buffer that is being modified from being cleaned by another thread of control.

4.1.21 dgux_5.4R2.01.p41

This patch corrects a problem which occurs when a print request that specifies a form is made to a printer in a printer class which does not have that form mounted.

If the specified form is not mounted, a request to a printer class that requires that form will be assigned to the first printer in the printer class. If the form is then mounted on the first printer, the request will print. If the form is mounted on some other printer in a printer class, some action to the request, such as lp -i<request-id>, must be done in order for the request to be reassigned to the printer where the form is mounted.

With this patch, lpsched reevaluates all requests to a printer class after a form is mounted. This will reassign a blocked request to the printer in the printer class with the form mounted.

4.1.22 dgux_5.4R2.01.p43

Patch dgux_5.4R2.01.p43 corrects a problem in the ELF environment where the linker miscalculates the size of the dynamic string table which results in linker errors. Programs that have object files that reference _etext, _edata, or _end may run into this problem.

4.1.23 dgux_5.4R2.01.p45

Patch dgux_5.4R2.01.p45 disables the error logging of late collisions on the dgen ethernet device. The late collisions are being reported in error and typically do not indicate a hardware or network problem. This patch also enables the collision backoff algorthim for the dgen (ILACC) ethernet device. This algorthim is used when a collision occurs on the LAN. The ILACC will wait a multiple of IFS (Inter Frame Spaces) before attempting retransmission.

4.1.24 dgux_5.4R2.01.p46

Patch dgux_5.4R2.01.p46 corrects a problem that causes a system to experience a 6000003 panic under heavy usage.

4.1.25 dgux_5.4R2.01.p48

Patch dgux_5.4R2.01.p48 corrects a 2000075 (VM_PANIC_INVALID_KERNEL_ADDRESS) panic from occurring in the record lock manager subsystem (RM). The panic can be attributed to continued access to a deallocated record locking node.

4.1.26 dgux_5.4R2.01.p49

Patch dgux_5.4R2.01.p49 closes a small window where a biod server could perform a read ahead operation on a closed file at the same time the file is being reopened. This reopen race results in a 2000075 nfm panic.

4.1.27 dgux_5.4R2.01.p50

Patch dgux_5.4R2.01.p50 corrects a time loss problem seen only on AV/53x and AV/46xx systems. The actual rate of time loss varies depending on the system load.

Also included in this patch is the following fix to uc.a from an earlier patch:

This patch corrects a problem in the DG/UX kernel whereby system configurations consisting of 2 GB (Giga-bytes) of main memory or larger may fail to pass device configuration and panic. The kernel or diskman may try to configure VME devices that used to reside within that address range. The patch allows the kernel to size the large memory configuration correctly.

4.1.28 dgux_5.4R2.01.p52

Patch dgux_5.4R2.01.p52 is a patch to the ps library for Oracle RDBMS users. It provides improved performance for two-task applications using the shared memory driver. This patch is appropriate for versions of Oracle later than v6.0.37 or later than v7.0.13. This patch may be installed on any DG/UX 5.4 Release 2.01 system.

4.1.29 dgux_5.4R2.01.p54

Patch dgux_5.4R2.01.p54 corrects a problem in the FDDI device driver where an uninitialized variable could cause 2000075 and 3000032 panics to sometimes occur.

4.1.30 dgux_5.4R2.01.p55

DG/UX 5.4R2.01 was released with SVCMGR Rev 3.01. Patch dgux_5.4R2.01.p55 uprevs the system to SVCMGR Rev 4.24. It is necessary to build a new DG/UX kernel and bounce the system after installation.

4.1.31 CHANGES:

Patch dgux_5.4R2.01.p55 corrects potential problems related to SVCMGR Rev 3.01 and AV/Alert including:

1. Increasing cpu time being consumed by dgsvcmon when modem carrier detect is lost during RAC session. (NASC-16830)
2. The inability of users to login after disconnecting from RAC sessions in user mode - option 2 under dgsvcmon. (NASC-17296)

4.1.32

The following are a set of features that are included in SVCMGR Rev 4.24 which are added by installing patch dgux_5.4R2.01.p55:

1. Hardware Configuration Registration

   Whenever DG/UX is booted, the online hardware sizer is run and a hardware configuration (M1) packet is sent to the designated AV/ALERT Support System as dgsvc_d is initialized. This packet includes: standard header information and a table of hardware part numbers and descriptions.

2. Error Thresholding (device & system level)

   An error thresholding mechanism was built- into SVCMGR that standardizes error reporting and defaults for all soft and certain hard errors. A system-level error thresholding mechanism has also been added to throttle MI call hourly and daily maximums from AV/Alert support systems. A user interface is provided for adjusting these device and system level threshold trip levels.

3. FE Mode Info Packets (M4)

   The M4 FE_Mode Info Packet provides FE/Customer Support information via AV/Alert for: dynamic password expiration, FE_Mode password change, and other future FE_Mode related information.

4. Call Closure Packets (M6)

   Call Closure Packets provide the FE/Customer Support interface for sending call closure information via AV/Alert against MI Incidents (M3). The MI Call Closure Packet is patterened after the FACTS Field Guide and uses the Online Hardware Sizer to ease the FRU replacement selections.

5. Software Applications Packets (M8)

   Software Applications Packets provide a format-free packet for applications to report application-specific information via AV/Alert.

6. HA Features

   High Availability features designed into AViiON System PROM will be supported under SVCMGR interface. These include interfaces for: hardware deconfiguration, deferred MI, and other HA hardware features requiring automated handling or a user interface.

4.1.33 dgux_5.4R2.01.p56

This patch exchanges the interrupt priorities for DMA and SCSI on the AV/300, AV/400, AV/4000 and AV/4300 series of AViiON computers.

Also included in this patch are the following fixes to dev.a from earlier patches: The behavior on the close of a "no rewind on close" tape device has been changed. Currently, DG/UX positions the tape after the first EOF even though the device is opened as Read/Write and no data was written to the tape. DG/UX will now leave you at the current tape position if no filemarks are required.

This patch also corrects a conflict between the SD and OD drivers. Currently, the SD driver may panic during a probedev when Opstar devices are on the SCSI bus. A panic could also occur when Opstar devices are mistakenly deconfigured by referring to them as 'sd' devices, rather than by the name 'od'.

This patch also enables the Read Cache on the Sony WDD-930-01 Opstar drive if it is running the latest firmware.

3rd party Micropolis disks in SCSI-2 mode could not be registered. The drive indicated it performed SCSI-2 Command Tagged Queuing, but when DG/UX attempted to send a tagged command, the drive rejected it and the operation failed. Currently, DG/UX checks the inquiry block to determine if Tagged Queue Commands are supported. DG/UX now verifies that this feature is actually enabled in the Control Mode Page instead of assuming that Tagged Queuing is enabled. If DG/UX detects that Tagged Queuing is off but the drive indicates that it supports this feature, an attempt will be made to turn it on. If that attempt fails, tagged commands will not be sent to the drive.

3rd party Seagate and IBM disks in SCSI-2 mode would see the error 'unable to flush buffer' when data was written to them. These errors would eventually cause the filesystem to be downgraded to read-only mode. This problem was occurred because these drives have shallower queues in them than DG drives. When the queue filled up with commands, subsequent commands were rejected with the QueueFull status which DG/UX didn't expected. This status was incorrectly interpreted as the "EBUSY" status so the command was actually retried. Now, when DG/UX detects the QueueFull status, it will adjust the drive's command queue information so the disk's queue will not be flooded.

DG/UX would sometimes panic with a panic code of 2000075 or 3000032 if a close to a tape device was issued while a SCSI bus reset was in progress.

The 9 Track tape drive may not read EOF/EOM correctly causing multi-tape reelexchange restores to pull the tape off of the tape reel. The st (SCSI Tape) driver was modified to give EOF precedence over EOM.

The sd driver has been modified to recognize the TEN-X Multi-platter OCU device and assign that device a large (100 second) timeout value. This is designed to reduce the likelihood that certain optical disk jukeboxes will experience disconnect timeouts and SCSI resets.

The dev_scsi_poll_deregister_device routine has been modified to be WIRED in memory. If a tape drive is being deconfigured, and it takes a page fault, DG/UX will panic. This wiring directive will avoid the panic.

DG/UX may hang or panic when a tape unit is deconfigured. When the tape unit is deconfigured, it releases wired memory that may have already been released.

The sd driver has a bug where it doesn't record sar statistics for extended read/write operations. The extended read/write commands are used for large disk devices, so this addresses a problem where no sar data is collected for block addresses above 2**21.

This patch also increases the bus-request timeout for the insc adapter. The 2GB 3.5"" disk drive (Models 6841 & 6842) runs idle-time functions which include servo adjustments to account for thermal changes in the drive. If the IO rate to the drive is heavy, the drive may have to hold off a request for a short period of time (2 to 4 seconds) so

that the calibration operation can be completed. A timeout value in the insc adapter driver was too small to allow this operation to be done without timing out, so the value was enlarged to 5 seconds.

This patch corrects a problem where the JB and OD drivers were using adapter retries. This was causing the original request sense information from a device error to be lost.

This patch also corrects a problem where Opstar would imtermittantly fail when making a file system with sysadm. The error "unable to create MO file system on <file_system> using MOMFKS" would be returned. This failure occured when both "sar" and "diskman" attempted to open the device simultaneously.

4.1.34 dgux_5.4R2.01.p57

Patch dgux_5.4R2.01.p57 corrects a problem where a signal structure could be freed while a valid pointer to the structure still existed. This led to the signal structure free list being corrupted.

Also included in this patch is a correction for a problem that occurs when using the sigstack() call. Sigstack did not properly change the signal stack to the user provided signal stack address, instead the original stack was used.

4.1.35 dgux_5.4R2.01.p58

Patch dgux_5.4R2.01.p58 corrects a problem where protection violations (SIGBUS signal) do not point to the generating instruction on the 88100 when running in serialized mode.

Also included in this patch are the following fixes:

Correction for a problem where a system dump to a Logical Disk corrupts a small part of the dump image. The corruption occurrs due to the overflow of the sc_static_stack. This only occurs with a system dump to disk, not to tape.

Correction for a problem where the register contents of the destination register, which is obtained from the siginfo data structure, is reset to zero in an application that binds in a SIGILL signal handler. This causes a problem in the case where the destination register is the same register as either rS1 or rS2 because the address calculation is corrupted. This occurs for all type of ld.usr, st.usr and xmem.usr opcodes.

Correction for a bug in the sc.a kernel library which causes the system to enter an infinite loop, thereby resulting in a soft system hang.

4.1.36 dgux_5.4R2.01.p59

Patch dgux_5.4R2.01.p59 changes the Streams error logging code to prevent a deadlock from occuring during the logging process. The changes involved modifying some Streams modules to release locks before calling other Streams functions, thereby avoiding the deadlock situation.

Also included in this patch are the previous fixes :

A previous fix changed the lock mechanism for Streams when a process is accessing a FIFO via a stat(2) system call. The current lock mechanism would not ensure that the stream is open and valid in all cases and a panic may occur if the FIFO was recently closed. This patch corrects poll(2) to correctly handle the system call restart. The system call restart is a per system call dependent feature that enables selective system calls to be transparently retried if a signal was caught during the duration of the system call. This patch enables poll(2) to be restartable.

The second correction was for the occurance of a DG/UX panic with a 2000075 panic. This panic occurred because of incorrect handling of M_FLUSH messages in the streams code.

The third problem corrected is seen as either a 2000075 panic occurs or lpsched hangs. These occur as the result of two processes obtaining locks on one end of a pipe, followed by one of the processes releasing its lock and deleting

the end of the pipe it held.

The fourth problem corrected is also seen as a 2000075 panic, when a streams module is removed from a FIFO stream. This occurs due to a design flaw in the sfm.a kernel library whereby the I_PUSH and I_POP streams ioctl calls behave incorrectly when inserting and removing streams modules.

The fifth problem corrected is a streams locking problem whereby both ends of a stream pipe may need to be locked, but the DG/UX kernel does not guarantee that a process will be able to obtain both locks. Two processes may obtain a lock on each end of the stream pipe, causing a process deadlock until one of the processes terminates or releases the lock, or in the more severe case, the kernel may panic if one of the processes deletes the pipe while the other process holds the lock on the other end of the pipe. This typically causes a 2000075 panic.

The sixth problem corrected by this patch occurs if the system runs out of STREAMS queuepairs while attempting to initialize a new streamhead, the open will fail but the streamhead open count will not be reset and the streamhead will not be deleted. Subsequent opens to the same device will cause a panic because the streamhead will appear to be open when it is not. This may indicate that the kernel parameter NQUEUE needs to be increased as well as installing this patch.

4.2 Package 2 - Product Patch Level tcpip_5.4R2.01.09

TCP/IP patch level tcpip.4R2.01.09 is described below:

4.2.1 tcpip_5.4R2.01.p01

Patch tcpip_5.4R2.01.p01 adds the initgroup() call to ftpd. This will allow for the initialization of a ftp user's supplementary group list. See the initgroups(3C) man page for more details.

This patch also modifies the check of autlogin's username/password in the .netrc file. Now, the lookup of autologin's username/password will be based on the specified destination rather than converting system alias names back to the primary system name.

4.2.2 tcpip_5.4R2.01.p03

Patch tcpip_5.4R2.01.p03 is a release of an updated ping command. This command is based on the BSD 4.4 ping command. Please see the man page for ping(1) included in this patch for details.

4.2.3 tcpip_5.4R2.01.p04

Patch tcpip_5.4R2.01.p04 adds the -e option to telnet providing the capability of specifying an escape character string on the command line. The escape character string must follow the -e option as a separate argument and must be enclosed in double quotes. For example, if one does not want an escape sequence, specify a null string as the argument to the -e option, i.e. telnet -e "".

4.2.4 tcpip_5.4R2.01.p06

Patch tcpip_5.4R2.01.p06 corrects a problem with the select() satsify on a connection confirmation. TCP connect confirmations incorrectly satisfy select()s with read intent. This could lead to a recv() incorrectly receiving an EAGAIN error.

4.2.5 tcpip_5.4R2.01.p07

Patch tcpip_5.4R2.01.p07 adds a kernel enhancement that will allow the maximum segment size (MSS) for TCP/IP to be a configurable kernel parameter. The current method for determining the default maximum segment size depends upon the location of the peer. If the peer is on a directly connected network, the MTU from the network

interface is used to calculate the TCP MSS. If the peer is non-local, the TCP MSS is calculated using IP_MSS(576) as the MTU (i.e. TCP MSS will be 536). With this patch, the TCP MSS value can be specified directly. When configuring a new kernel with "sysadm newdgux", specify the new TCP/IP kernel variable TCPMSS and give it the desired maximum segment size value in bytes. Rebuild, install and reboot the new kernel to obtain this new feature.

The kernel configuration variable TCPMSS represents the amount of data TCP will send in one packet. The minimum value for TCPMSS is 0 which means that TCP will use the current default method of determining the maximum segment size. Its maximum value will be 65536 bytes.

Also included in this patch is an earlier released patch that adds a kernel enhancement that will allow the keep alive timer for TCP/IP to be a configurable kernel parameter. The current default for the keep alive timer is 7200 seconds (2 hours). With this patch, the value can be adjusted. When configuring a new kernel with "sysadm newdgux", specify the new TCP/IP kernel variable TCPKEEPIDLE and give it the desired timeout value, in seconds. Rebuild, install and reboot the new kernel to obtain this new feature.

The kernel configuration variable TCPKEEPIDLE represents the number of seconds an endpoint is idle before the first keepalive probe is sent. The minimum value for TCPKEEPIDLE is 75 seconds (a probe interval) and the maximum value is 65535 seconds. These limits are silently enforced and if exceeded will be used.

WARNING!!! Setting the TCPKEEPIDLE timer and TCPMSS will be supported by a different mechanism in DGUX 5.4 Release 3.00. There are no plans to support the mechanism implemented in this patch in any later revision of DG/UX.

4.2.6 tcpip_5.4R2.01.p08

Patch tcpip_5.4R2.01.p08 is a new release of the bootp server daemon for DG/UX TCP/IP. Please see the man pages for booptd(1M) for more information. This is the initial release of this software.

4.2.7 tcpip_5.4R2.01.p09

Patch tcpip_5.4R2.01.p09 corrects a problem with tftpd service timeout/failures in environments with excessive simultaneous tftp service requests (i.e. diskless client boot operations, Xterminal boot operations, etc.). This patch allows the tftpd daemon to handle more simultaneous requests before timing out. The patch provides performance enhancements which enusre that the intitial tftp read requests are answered before they are retransmitted to avoid the spawning of additional tftpd processes.

4.3 Package 3 - Product Patch Level nfs_5.4R2.01.p06

NFS Patch Level nfs_5.4R2.01.p06 is described below:

4.3.1 nfs_5.4R2.01.p01

Patch nfs_5.4R2.01.p01 changes the way in which rpc.lockd accesses the TCP/IP transport system to send lock messages to clients and servers. Previously, rpc.lockd would allocate and try to bind to a privledged UPD port to generate the lock message for each new client. This operation may take several seconds if for some reason the system currently running has all of the privledged ports in use (ports numbered between 600 and 1023 are privledged). Netstat can be used to list all of the ports currently in use.

Rpc.lockd has been changed to allocate one privledged port and use it for all messages thereby avoiding this condition.

This problem may show up as a "spinning or run-away lockd".

4.3.2 nfs_5.4R2.01.p02

Patch nfs_5.4R2.01.p02 corrects a problem where the rusersd daemon fails to return a list users when the login terminal name is of type tty[pqrs] and the environment variable DISPLAY has been set to ":0.0" The rusersd daemon now determines logins in the same manner as the who() command does.

4.3.3 nfs_5.4R2.01.p04

Patch nfs_5.4R2.01.p04 corrects a problem whereby rpc.statd will not execute the wait(2) system call to clean up children processes that were forked to handle lock recovery for remote clients. This will result in defunct processes to accumulate over time, eventually preventing users from logging into the system.

4.3.4 nfs_5.4R2.01.p06

Patch nfs_5.4.2.p06 corrects a problem where PCNFSD would incorrectly hold /dev/console open. On a B1 trusted system this prevented users from logging onto /dev/console more than once.

It also resolves a problem where finger would fail with the error:
finger: can't stat /dev/PC-NFS login

Note that this patch delievers revision 2.00 of PCNFSD. PCNFSD has been qualified with NFS Client for Lan Workplace. The uncompiled lwpnfs daemon included in the NFS client for Lan Workplace is not supported. In addition, BSD printing is no longer supported in this revision.

In order to access a printer on the server you must export the /usr/spool/pcnfs directory to group everyone. PCNFSD will use this directory to store your print jobs. Failure to export this directory will result in the error:
"Invalid remote device" when trying to link a printer.

Also note, that in order for a user with a UID less than 101 to link a file system to a local drive, the following entry must be in the file /etc/pcnfsd.conf, (create one if it does not already exist) :
uidrange 0-65555

Otherwise the user will receive an authentication error when trying to execute a net link command.

4.4 Package 4 - Product Patch Level X11_5.4R2.01.p03

X11 Patch Level X11_5.4R2.01.p03 is described below:

4.4.1 X11_5.4R2.01.p01

Patch X11_5.4R2.01.p01 correct/supplies the following:

1. When certain GC algebra functions were used and a pixmap was used to redisplay an exposed area of the screen, the foreground and background had the same color.
2. Oracle CASE*Designer would crash after choosing an option on the main menu bar.
3. All MIT patches up to and including patch # 2830.

4.4.2 X11_5.4R2.01.p02

Corrects a qsort problem that manifests itself as a segmentation fault when running ESRI's Arc/Info application.

4.4.3 X11_5.4R2.01.p03

Patch X11_5.4R2.01.p03 corrects a problem in which text areas do not display properly and some text areas are unreadable when running SoftPC with windows on a monochrome workstation.

4.5 Package 5 - Product Patch Level networker_5.4R2.01.p01

NETWORKER Patch Level networker_5.4R2.01.p01 is described below:

4.5.1 networker_5.4R2.01.p01

Patch networker_5.4R2.01.p01 corrects a number of problems in the single client version of Legato NetWorker. This patch should not be applied if you are running multi-client Networker (Q017A).

A problem in the savegroup command which causes it to dump core if any of the clients in the group are not AViiON systems.

A problem with recovery in the Motif interface which causes it to hang after prompting the user on a name conflict.

A problem which prevents NetWorker from using more than 150MB on QIC-525 tapes.

A problem with recovery in the Motif interface which caused it to appear to hang, due to a lenghy delay afte the completion of a recover operation.

A problem which prevented raw disks from being archived with NetWorker. Raw disks (both logical and physical) can now be archived by simply including their paths in a save set list. As with file systems, NetWorker will retrieve underlying physical device characteristics and use that information to perform intelligent scheduling among raw disks on the same client. Raw disks located on disk arrays or on separate physical devices may be archived concurrently, while raw disks located on the same physical device (which is not a disk array) are archived sequentially.

5. Files

A list of files for each product package included in patch level op-sys-x_5.4R2.01.931008 is contained in a file in the /usr/release directory. To be able to back out of this patch level, these files should be saved prior to loading this patch level.

Package 1 - Product Patch Level dgux_5.4R2.01.59

/etc/svcmgr.rclinktab.proto
/etc/svcmgr.rcrmtab.proto
/sbin/setup.d/root/dgux_5.4R2.01.p55_r.svcmgr.do
/usr/bin/admfailoverdisk
/usr/bin/admuser
/usr/bin/failoverd
/usr/bin/ksh
/usr/bin/sar
/usr/bin/shl
/usr/bin/xc

/usr/catman/a_man/man1/admuser.1m.z
/usr/catman/a_man/man1/dgs_strerr.1m.z
/usr/catman/a_man/man1/dgs_syslog.1m.z
/usr/catman/a_man/man1/dgsvc_d.1m.z
/usr/catman/a_man/man1/dgsvc_inetd.1m.z
/usr/catman/a_man/man1/dgsvc_mid.1m.z
/usr/catman/a_man/man1/dgsvc_pwd.1m.z
/usr/catman/a_man/man1/dgsvc_sizer.1m.z
/usr/catman/a_man/man1/dgsvc_timd.1m.z
/usr/catman/a_man/man1/dgsvcmon.1m.z
/usr/catman/a_man/man1/svcmgr.1m.z
/usr/dglib/libc.so.1
/usr/etc/master.d/dgux
/usr/etc/master.d/odg
/usr/lib/lan/cmc130.bin
/usr/lib/lp/lpsched
/usr/lib/sysadm/C/menus/Usermgmt.menu
/usr/options/dgux_5.4R2.01.59.name
/usr/release/dgux_5.4R2.01.59.fl
/usr/release/op-sys-x_5.4R2.01.931008.pn
/usr/sbin/.dft_threshold
/usr/sbin/config
/usr/sbin/dgs_strerr
/usr/sbin/dgs_syslog
/usr/sbin/dgsvc_bthresh
/usr/sbin/dgsvc_d
/usr/sbin/dgsvc_inetd
/usr/sbin/dgsvc_mid
/usr/sbin/dgsvc_pwd
/usr/sbin/dgsvc_sizer
/usr/sbin/dgsvc_timd
/usr/sbin/dgsvcmon
/usr/sbin/init.d/rc.dgrmserv
/usr/sbin/init.d/rc.dgserv
/usr/sbin/setup.d/usr/dgux__2.u.sysadm.do
/usr/sbin/svcmgr
/usr/sde/m88kdguxelf/usr/bin/ld
/usr/src/uts/aviion/cf/Libs.odg
/usr/src/uts/aviion/cf/system.odg.proto
/usr/src/uts/aviion/lb/ts.a
/usr/src/uts/aviion/lb/cdm.a
/usr/src/uts/aviion/lb/dev.a
/usr/src/uts/aviion/lb/dgen.a
/usr/src/uts/aviion/lb/dl.a
/usr/src/uts/aviion/lb/ffm.a
/usr/src/uts/aviion/lb/hfm.a
/usr/src/uts/aviion/lb/ilacc.a
/usr/src/uts/aviion/lb/init.a
/usr/src/uts/aviion/lb/nfm.a
/usr/src/uts/aviion/lb/odg.a
/usr/src/uts/aviion/lb/pdep.a
/usr/src/uts/aviion/lb/pefn.a
/usr/src/uts/aviion/lb/pm.a
/usr/src/uts/aviion/lb/ps.a

/usr/src/uts/aviion/lb/rm.a
/usr/src/uts/aviion/lb/rpc.a
/usr/src/uts/aviion/lb/sc.a
/usr/src/uts/aviion/lb/sfm.a
/usr/src/uts/aviion/lb/so.a
/usr/src/uts/aviion/lb/su.a
/usr/src/uts/aviion/lb/uc.a
/usr/src/uts/aviion/lb/uc.a
/usr/src/uts/aviion/lb/vmc.a
/usr/stand/diskman

Package 2 - Product Patch Level tcpip_5.4R.2.01.09

/etc/bootptab.proto
/sbin/setup.d/root/bootp__1.r.proto.do
/usr/bin/admbootpclient
/usr/bin/bootpd
/usr/bin/ftp
/usr/bin/ftpd
/usr/bin/inetd
/usr/bin/ping
/usr/bin/telnet
/usr/bin/tftpd
/usr/catman/a_man/man1/admbootpclient.1m.z
/usr/catman/a_man/man1/bootpd.1m.z
/usr/catman/a_man/man1/ping.1m.z
/usr/etc/master.d/tcpip
/usr/options/tcpip_5.4R2.01.p09.name
/usr/release/tcpip_5.4R2.01.p09.fl
/usr/release/op-sys-x_5.4R2.01.931008.pn
/usr/src/uts/aviion/lb/conf.a
/usr/src/uts/aviion/lb/inso.a
/usr/src/uts/aviion/lb/tcp.a

Package 3 - Product Patch Level nfs_5.4R.2.01.06

/usr/options/nfs_5.4R2.01.p06.name
/usr/release/nfs_5.4R2.01.p06.fl
/usr/release/op-sys-x_5.4R2.01.931008.pn
/usr/sbin/dg_lock_mgr
/usr/sbin/pcnfsd
/usr/sbin/rpc.lockd
/usr/sbin/rpc.statd
/usr/sbin/rusersd

Package 4 - Product Patch Level X11_5.4R.2.01.03

/usr/options/X11_5.4R2.01.p03.name
/usr/release/X11_5.4R2.01.p03.fl
/usr/release/op-sys-x_5.4R2.01.931008.pn
/usr/opt/X11/bin/Xdg
/usr/opt/X11/bin/Xdg
/usr/opt/X11/lib/libXm.so.2

Package 5 - Product Patch Level networker_5.4R.2.01.01

/usr/opt/networker/bin/compressasm
/usr/opt/networker/bin/logasm
/usr/opt/networker/bin/mailasm
/usr/opt/networker/bin/mbackup
/usr/opt/networker/bin/mrecover
/usr/opt/networker/bin/nsrindexasm
/usr/opt/networker/bin/nsrmmdbasm
/usr/opt/networker/bin/nullasm
/usr/opt/networker/bin/rawasm
/usr/opt/networker/bin/recover
/usr/opt/networker/bin/save
/usr/opt/networker/bin/savefs
/usr/opt/networker/bin/savegroup
/usr/opt/networker/bin/uasm
/usr/opt/networker/bin/xlateasm
/usr/opt/networker/sbin/nsrd
/usr/opt/networker/sbin/nsrmmd
/usr/opt/networker/sbin/scanner
/usr/options/networker_5.4R2.01.p01.name
/usr/release/networker_5.4R2.01.p01.fl
/usr/release/op-sys-x_5.4R2.01.931008.pn

6. Installation Instructions

6.1 Loading the Patch Level

This op-sys-x patch level is in sysadm loadpackage format and consists of those packages listed in the section titled "Patch Level op-sys-x" containing the files as listed by package in the section titled "FILES" Section of this document. IMPORTANT, LOAD ONLY THE PACKAGES THAT APPLY TO YOUR SYSTEM.

To back out of this op-sys-x patch level, files listed in the section titled "Files" should be saved to another name or backed up before proceeding. YOU SHOULD BE IN RUN LEVEL 1 WHEN LOADING THIS op-sys-x PATCH LEVEL TO AVOID OVERWRITING A PROGRAM THAT IS CURRENTLY RUNNING.

This op-sys-x patch level will load on any DG/UX 5.4R2.01 system.

6.2 Loading the op-sys-x Patch Level from Tape

To load the op-sys-x patch level, perform the following steps:

```
Warning: Do not select "all" at Package Name(s): [all], if you
     are selecting individual packages.  Load only the
         packages you need.
         Type a "?" to choose the packages that interest you.

#sysadm loadpackage
Release Medium: [/dev/rmt/0] /dev/rmt/<tape_device>
Is /dev/rmt/<tape_device> ready? [yes]
Package Name(s): [all]
List file names while loading? [no]
OK to perform operation?  [yes]
*Positioning the tape to load: <package name> .....
```

*Loading package: <package name> .....
*Package "<package name>" has been loaded.
Updating proto root (/srv/release/PRIMARY/root/root.proto).
Updating MY_HOST root (/srv/release/PRIMARY/root/MY_HOST).
Package load is finished.
The selected packages have been loaded.

* These lines are repeated for each package selected for loading.

6.3 Loading the op-sys-x Patch Level from a Directory

If the op-sys-x Patch Level is delivered as a tar format file which consists of images that are sysadm loadable, you will need to extract the images into an empty directory. To extract these images from a provided file, perform the following steps:

```
# mkdir -p /var/tmp/patch_level
# cd /var/tmp/patch_level
# tar xvf <path_name>/op-sys-x_5.4R2.01.931008
```

To load the patch level from this directory structure, perform the following steps:

```
#sysadm loadpackage
Release Medium: [/dev/rmt/0] /var/tmp/patch_level
Package Name(s): [all]
List file names while loading? [no]
OK to perform operation? [yes]
*Loading package: <package name> .....
*Package "<package name>" has been loaded.
Updating proto root (/srv/release/PRIMARY/root/root.proto).
Updating MY_HOST root (/srv/release/PRIMARY/root/MY_HOST).
Package load is finished.
The selected packages have been loaded.
```

* These lines are repeated for each package selected for loading.

To create a sysadm loadable patch tape which can be applied on any AViiON system with a tape drive, follow the steps below:

```
# cd /var/tmp/patch_level
# ./Docs/MakeTape /dev/rmt/<tape_device>
```

6.4 Installing the Patch Level

6.4.1 setuppackage

After loading the package using sysadm loadpackage, you must set up a patch by running sysadm setuppackage.

To setup the patch, perform the following setups:

```
# sysadm setuppackage
```

```
Package Name(s): [all] (Type "?" to see packages to setup)
OK to perform operation? [yes]
Setting up dgux in MY_HOST root.
Setting up patch: dgux_5.4.1.p26.
Setting up patch: dgux_5.4.1.p58
Package dgux has been successfully set up in MY_HOST root.
Package setup for dgux is complete.
```

6.4.2 Building a New Kernel

See Chapter 4 of the *Managing the DG/UX System* manual for instructions on reconfiguring the system. Use **sysadm newdgux** to build a new kernel. If you are a diskless server, your client kernels must be rebuilt or the new **dgux.diskless** in **/usr/stand** must be hard linked to the appropriate client's root area.

--- End of Patch Level Notice ---