

## Patch Kit Notice:

# DG/UX for AViiON Systems Patch Kit op-sys-x\_5.4R2.10.940201

February 1994

Part Number 017-600054-01

This Patch Kit 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Unpublished — all rights reserved under the copyright laws of the United States.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, 1994.

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.

**This patch kit replaces op-sys-x\_5.4R2.10.931210 and is intended to protect your system from improper program execution or data corruption. Please install this patch kit immediately.**

---

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 Kit Notice describes Patch Kit op-sys-x\_5.4R2.10.940201 for 5.4R2.10 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\_5.4R2.10.940201.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 Kit consists of the following parts:

Part Description	Part Number
DG/UX for AViiON Systems Patch Kit op-sys-x_5.4R2.10.940201 Notice for AViiON 88110 Series Computers	017-600054-01
DG/UX for AViiON Systems Patch Kit op-sys-x_5.4R2.10.940201 Tape Media for AViiON 88110 Series Computers	079-600366-01
DG/UX for AViiON Systems Patch Kit op-sys-x_5.4R2.10.940201 CD-ROM Media for AViiON 88110 Series Computers	068-600089-01

## 2. Product Description

### 2.1 Individual Patches

For DG/UX Revision 5.4R2.10, 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 5.4R2.10 the naming convention is:

dgux\_5.4R2.10.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 Kits

When a sufficient number of individual patches has been generated, they are collected into a patch kit 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 5.4R2.10, are assembled in one package using the following naming convention:

dgux\_5.4R2.10.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 Kit op-sys-x

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

op-sys-x\_5.4R2.10.940201

Op-sys-x patch kits are cumulative, thus you should load only the most recent op-sys-x patch kit. This op-sys-x patch kit is a sysadm loadable tape which contains one product patch level per sysadm loadable package. The packages on this op-sys-x\_5.4R2.10.940201 Patch Kit are:

Package 1: dgux\_5.4R2.10.31

Package 2: tcpip\_5.4R2.10.07

Package 3: nfs\_5.4R2.10.01

## 3. Environment

### 3.1 Hardware

Patch Kit op-sys-x\_5.4R2.10.940201 of the DG/UX System will run on Data General AViiON series machines with revision 4.1 or later of the MC88110 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 or CD drive (for software distribution). On workstations, 16MB of main memory is recommended.

Patch Kit op-sys-x\_5.4R2.10.940201 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 5.4R2.10 System software. Apply this patch ONLY on DG/UX Revision 5.4R2.10.

## 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 5.4R2.10 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\_5.4R2.10.p32, then it must be reloaded, because its patch number, p27 is greater than the patch level number 31, dgux\_5.4R2.10.31, 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\_5.4R2.10.p04 is not listed below as being included in this op-sys-x patch level and its number, 04 is less than or equal to the patch level number 31, dgux\_5.4R2.10.31, 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\_5.4R2.10.31**

DG/UX patch level dgux\_5.4R2.10.31 is described below:

##### **4.1.1 dgux\_5.4R2.10.p01**

Patch dgux\_5.4R2.10.p01 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 2.10 system.

##### **4.1.2 dgux\_5.4R2.10.p05**

Patch dgux\_5.4R2.10.p05 corrects a 2000075 (VM\_PANIC\_INVALID\_KERNEL\_ADDRESS) panic from the record lock manager subsystem (RM). The panic can be attributed to continued access to a deallocated record locking node.

##### **4.1.3 dgux\_5.4R2.10.p07**

Patch dgux\_5.4R2.10.p07 corrects a problem with systems which have installed the NVRAM Model 5018VEM[-K] card and have the kernel configured to use the cdm() and nvr() 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.

##### **4.1.4 dgux\_5.4R2.10.p11**

Patch dgux\_5.4R2.10.p11 increases the number of blocks that the kernel resident fsck can process from 600,000 to 4,000,000 blocks. Prior to this enhancement, the user would receive an error from fsck indicating the file system was too large.

#### 4.1.5 dgux\_5.4R2.10.p16

Patch dgux\_5.4R2.10.p16 is a modified VDA255 syac board image that now correctly handles a flushi command immediately followed by a close command. Without this modified board image, the flushi may not complete. The close command is processed next, and if the close command times out, the board is reset. DG/UX may then panic when trying to remove the flushi command from a line that has already been closed.

This new VDA255 board image also calculates the memory available on the VDC cluster boxes correctly. Previously, tty line flushes/closes could hang due to insufficient space on the VDC.

#### 4.1.6 dgux\_5.4R2.10.p19

Patch dgux\_5.4R2.10.p19 corrects a problem where file access was not being checked before writing a file in a directory or before truncating a file on a DG/UX NFS filesystem when mounted on another vendor's operating system. The problem is not apparent when mounting a DG/UX NFS file system on a DG/UX system.

#### 4.1.7 dgux\_5.4R2.10.p21

DG/UX 5.4R2.10 was released with SVCNMR Rev 4.21. Patch dgux\_5.4R2.10.p21 upgrades the system to SVCNMR Rev 4.27. This patch does not require a rebuild of the DG/UX Kernel.

Patch dgux\_5.4R2.10.p21 corrects potential problems related to SVCNMR Rev 4.21 and AV/Alert including:

- The loss of M3 incident packets when deferred MI is enabled on high end AViiON systems with deferred MI capability. (NASC-12347)

- SVCNMR hanging due to errors from dual-ported hada systems.

- The inability of users to login after disconnecting from RAC sessions in user mode - option 2 under dgsvcmon. (NASC-17296)

- AV/Alert from falsely generating Abrupt shutdown messages during graceful shutdowns such as init 5.

- DG/UX autoreboot remaining enabled in PROM after successive DG/UX panics on AV85/9500 systems.

- Dgs\_sterrr was not properly cleaning up children of the syslog call. The multiple child processes, occurring on Comm errors can use up all existing process table entries crippling the system.

- AV100-400 workstations and the AV4000 server from occasionally crashing when the online sizer runs due to data parity error sensitivity.

This patch also adds the following SVCNMR and AV/Alert enhancements:

- Online Sizing for AV 55/85/9500 family systems, SA-1 JPs and SubFRU information.

- SVCNMR sends an M1 Hardware Configuration packet if the contract number or the system ID has changed.

#### 4.1.8 dgux\_5.4R2.10.p23

Patch dgux\_5.4R2.10.p23 corrects a problem with the select(2) system call. The system call, write(2), when writing to a pipe with a size greater than PIPE\_BUF (default 8192 characters) may have failed to satisfy a read select(2) event on the destination end of the pipe. This is corrected with this patch.

Also included in this patch are the previous fixes :

The OS/2 Streams Trace utility "strace" would not be able to capture the messages to be logged. This problem has been corrected.

A failure in the lock mechanism for Streams occurs 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.

The Streams error logging code was corrected to prevent a deadlock from occurring during the logging process. The changes involved modifying some Streams modules to release locks before calling other Streams functions, thereby avoiding the deadlock situation.

#### 4.1.9 dgux\_5.4R2.10.p24

Patch dgux\_5.4R2.10.p24 corrects a problem with inefficient error handling in the pow(3M) libm routine. Programs that use the pow(3M) routine and were linked with the libm that shipped with DG/UX 5.4 R2.00, R2.01 or R2.10 may perform slower than programs linked with an earlier version of libm. The error handling for this routine has been tuned without losing functionality in the libm contained in this patch.

#### 4.1.10 dgux\_5.4R2.10.p26

Patch dgux\_5.4R2.10.p26 corrects a problem with incorrect results being returned for -MINDOUBLE when linking shared, i.e. using /usr/dglib/libc.so.1.

#### 4.1.11 dgux\_5.4R2.10.p27

Patch dgux\_5.4R2.10.p27 corrects a problem in the att\_kbd streams module which allows all of available streams memory to be used and not released. This may eventually cause a system hang.

#### 4.1.12 dgux\_5.4R2.10.p28

Patch dgux\_5.4R2.10.p28 delivers an enhancement which improves mirror synchronous performance by using 128 block I/O when performing the synchronous operation. When the mirror is located on the CLARiiON, performance can be further enhanced by aligning the starting block of the logical disk containing the mirror image on block boundaries evenly divisible by 128. Additionally when binding disks into a stripe on the CLARiiON with micro code of 5.12 or greater, you should use the default stripe size of 128 sectors for the best mirror synchronous performance.

In tuning the CLARiiON stripe size to your application, if you have found that the default stripe size of 128 sectors is not suitable, then you may not see as large of increase in the mirror synchronous performance.

#### 4.1.13 dgux\_5.4R2.10.p30

This patch corrects a data corruption problem that can occur when using DG/UniVerse or executing the system calls below, in the order listed. **THIS PATCH MUST BE INSTALLED TO RESOLVE THIS DATA CORRUPTION PROBLEM AS IT RELATES TO THE FOLLOWING SET OF CIRCUMSTANCES.**

The problem usually occurs when there is a file whose file size is less than the data element size and the system calls below are issued as follows:

1. truncate(2) for some value less than the data element size,
2. lseek(2) past the previous end of file, and
3. write(2) for some value less than the data element size,

In these circumstances, DG/UX fills the next data element with nulls, which can corrupt data in a user's data file or

file system meta data. When the file system meta data is corrupted, the following message usually appears in the file /usr/adm/messages:

"FS tried to read buffer size 1 at logical offset xxxxxxx of the FS identified by fsid yyy (status=4026027)."

Note that special loading instructions for this patch are included in the "Installation Instructions" section of this notice. You will be instructed to run the fsck command with the -y option before rebuilding and rebooting your kernel in order to correct any meta data problems which might exist currently on your system.

Also included in this patch are the following changes:

This patch modifies the NFS server write code path to ensure all incoming requests are buffered. This will collate NFS packets that have been fragmented by a single or multiple IP routers. Without this patch, if the fragmentation is severe enough causing a single 8 KB NFS write request to be broken up into more than 16 IP fragments (i.e. if it was sent through a SL/IP link), DG/UX may panic with a 53000052 panic coed depending on the destination disk device.

This patch implements additional DG/UX NFS performance tuning. This patch should be loaded in conjunction with patch tcpip\_5.4R2.01.p02 to take advantage off all the performance modifications in this patch.

This patch corrects 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.

This patch also closes a small window where a biod server could perform a read ahead on a closed file at the same time the file is being reopened. This reopen race results in a 2000075 nfm panic.

#### 4.1.14 dgux\_5.4R2.10.p31

Patch dgux\_5.4R2.10.p31 corrects a problem where DG/UX could miss an interrupt from the NCR53c710 chip on the "dgsc" controller and experience a SCSI timeout.

This patch fixes a couple of problems that could sometimes cause 53000023 or 53000053 panics. One problem was fixed that caused these panics during SCSI reset/recovery and the other problem caused these panics on multi-initiator systems.

This patch corrects a problem which caused hangs on systems with CLARiiON Tape Arrays, 8mm tape drives, and 4mm tape drives.

This patch fixes a low level SCSI protocol problem which could cause a trespass to fail with an I/O error in a fail-over situation.

Also, this patch fixes a problem where 9-track tape drives would be incorrectly configured as 8mm tape drives.

Finally, this patch fixes a SCSI polling problem that could possibly cause hangs on systems with CLARiiON tape arrays, CLARiiON disk arrays, 8mm tapes, or 4mm tapes.

Also included in this patch are the following enhancements and corrections:

Corrects a problem where an AV5500 with revision 2 of the cypress chip can panic when reporting single bit memory errors. The panic code generated is 2000075.

Correction for a problem that could cause a system hang on a very busy system if the SCSI tape driver attempts to poll a tape device to handle an error situation and the io demon takes a page fault.



Makes changes to the command timeout for certain SCSI tape commands. Previously, some tape commands (status, open, etc) could take up to 5 minutes to complete if the drive unit did not have a tape loaded. The SCSI tape driver would assume the unit was in a REWIND state and retry the command every 2 to 5 seconds for 5 minutes. This replacement module will detect the current state of the tape unit and retry the command only when necessary.

Correction for a problem on the AV8500/9500 (dual 88110 CPU card for SA-1 chassis) systems. The per-jp timer used for profiling does not work correctly after a timer overflow. Symptoms related to this problem are slower performance and possible CPU hogging.

Correction for a problem on the AV5500 systems where if the system watchdog timer expires and causes a reset and an S 1000 dump is attempted, it will fail with another reset.

Adds support for 45 MHz Iliad board. There is currently only 50 MHz support.

Adds a performance improvement by re-enabling dual instruction issue and removing some of the unneeded instructions added to protect against an 88110 silicon problem. Dual instruction issue facilitates the issue of two instructions in a given clock cycle.

Correction for a memory leak with the sauna disk array inquiry ioctl. This memory leak can cause a soft system hang.

Correction for a problem where when a close is issued for a "no rewind on close" tape device, dgux positions the tape after the first EOF even though the device is opened as Read/Write. DG/UX will now leave you at the current tape position if no filemarks are required. This patch will also change the interrupt priorities for DMA and SCSI on the AV300/400/4000/4300 series of AViiON computers.

Correction for a 60000003 panic seen on systems under heavy usage.

Automatically enables ecc (error correction code) for cypress chip rev 1 or better. This is not enabled in rev 0.

Correction for a timer/prom interaction problem that may cause dgux.installer and customized kernels to hang during the boot process.

Correction for a 57000116 panic by increasing the timeout value on the wait for acknowledgement that the SCSI bus was reset and reinitialized following a SCSI device timeout.

Changes the reporting of soft and hard memory errors to report an address of FFFFFFFF (-1). Without this patch, the address reported would be invalid.

Changed the nested exception handler on 88110 for Flash Basic Pick applications that were hanging.

Correction for a 112000002 panic received on AV5500 systems when an admpdisk command list option is issued.

Correction for an instance of an "fidcr" error. User processes are terminated with a message in /var/adm/messages; "Unexpected fidcr error. Contact Data General. <uid>, <process name>, <address>. The user process is terminated with a "BUS ERROR" message.

#### **4.2 Package 2 - Product Patch Level tcpip\_5.4R2.10.07**

TCP/IP patch level tcpip.4R2.10.09 is described below:

#### 4.2.1 tcpip\_5.4R2.10.p04

Patch tcpip\_5.4R2.10.p04 corrects a problem where telnet and rlogin fail to raise an error condition when reading 0 bytes which resulted from a closed tty. This problem could result in a lingering telnet/rlogin session that doesn't disconnect and becomes cpu bound. This has been seen when there is an abnormal disconnect and when one of the parent process of the telnet/rlogin session has been exec'd as opposed to forked.

#### 4.2.2 tcpip\_5.4R2.10.p05

Patch tcpip\_5.4R2.10.p05 eliminates a vulnerability in sendmail. The CERT Coordination Center has issued a warning (Advisory Number CA-93:16) regarding security holes in the sendmail program of most vendors.

The vulnerability allows unauthorized remote or local users to execute programs as any system user other than root. This vulnerability effects the final destination sendmail host and can be exploited through an intermediate mail machine. Therefore, all sendmail recipient machines within a domain are potentially vulnerable. This patch corrects this problem.

#### 4.2.3 tcpip\_5.4R2.10.p06

Patch tcpip\_5.4R2.10.p06 corrects a RFC775 violation where ftpd failed to return the proper error code and error message when the 'pwd' command failed because of lack of access privileges. This patch will now return the error: "550 Cannot determine current directory. " when the current working directory cannot be determined.

#### 4.2.4 tcpip\_5.4R2.10.p07

Patch tcpip\_5.4R2.10.p07 corrects a problem which causes 2000107 and 2000075 panics. The panic only occurs on a very loaded system and is caused by tcp not properly locking structures accessed by the tcpip read service requests.

This patch also carries forward patches tcpip\_5.4R2.10.p01, tcpip\_5.4R2.10.p02, and tcpip\_5.4R2.10.p03.

Patch tcpip\_5.4R2.10.p01 adds support for a kernel enhancement that will allow the keep alive timer and maximum segment size for TCP/IP to be configurable kernel parameters. The new kernel parameters are TCPKEEPIDLE and TCPMSS. To use, add these variables to the kernel configuration file, rebuild the kernel and reboot.

The current default for the keep alive timer is 7200 seconds (2 hours). The value of the keep alive timer represents the number of seconds an endpoint is idle before the first keeplive probe is sent. With this patch, the value of the keep alive timer 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. 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, the limits will be used.

This patch also adds a kernel enhancement that will allow the maximum segment size (MSS) for TCP/IP to be a configurable kernel parameter. The value of the maximum segment size represents the amount of data TCP will send in one packet. 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. 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

**WARNING!!!** Setting the TCPKEEPIDLE 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.

Patch tcpip\_5.4R2.10.p02 implements additional DG/UX NFS performance tuning. This patch should be loaded in conjunction with patch dgux\_5.4R2.10.p14 to take advantage off all the performance modifications in this patch.

Patch tcpip\_5.4R2.10.p03 corrects a couple of deadlocks that have been discovered. The first deadlock is a tcp deadlock caused by a violation of the TCP locking hierarchy by the function tcp\_drop(). This violation manifests as a deadlock if a connection is being accepted by an application process at the same time that connection is being reset by the peer. The fix involves modifying tcp\_drop() to conform to the TCP locking design. The second deadlock is caused by a problem in inso.a. This deadlock is caused by a three-way race between the server application accepting a new connection, the peer resetting that same connection, and tcp\_fasttimo servicing delayed acknowledgments.

These problems are timing issues where the window for this to occur is very small. The problem requires at least a dual processor or better for the deadlock to manifest itself.

#### 4.3 Package 3 - Product Patch Level nfs\_5.4R2.10.p01

NFS Patch Level nfs\_5.4R2.10.p06 is described below:

##### 4.3.1 nfs\_5.4R2.10.p01

Patch nfs\_5.4R2.10.p01 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.

Note that this patch delivers 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
```

## 5. Files

A list of files for each product package included in patch kit op-sys-x\_5.4R2.10.940201 is contained in a file in the /usr/release directory. To be able to back out of this patch kit, these files should be saved prior to loading this patch kit.

#### Package 1 - Product Patch Level dgux\_5.4R2.10.31

```
/dgux.installer
/etc/svcmgr.rclinktab.proto
/etc/svcmgr.rcrmtab.proto
/sbin/setup.d/root/dgux_5.4R2.10.p21__r.svcmgr.do
/usr/dglib/libc.so.1
/usr/etc/master.d/dgux
/usr/lib/libm.a
/usr/lib/tcload/models/syac/VDA255
/usr/sbin/dgs_streerr
```

/usr/sbin/dgs\_syslog  
/usr/sbin/dgsvc\_bthresh  
/usr/sbin/dgsvc\_d  
/usr/sbin/dgsvc\_down  
/usr/sbin/dgsvc\_inetd  
/usr/sbin/dgsvc\_mid  
/usr/sbin/dgsvc\_pwd  
/usr/sbin/dgsvc\_sizer  
/usr/sbin/dgsvc\_timd  
/usr/sbin/dgsvcmom  
/usr/sbin/init.d/rc.dgrmserv  
/usr/sbin/init.d/rc.dgserv  
/usr/sbin/svcmgr  
/usr/src/uts/aviion/lb/bm.a  
/usr/src/uts/aviion/lb/cdm.a  
/usr/src/uts/aviion/lb/conf.a  
/usr/src/uts/aviion/lb/dev.a  
/usr/src/uts/aviion/lb/ffm.a  
/usr/src/uts/aviion/lb/fsck.a  
/usr/src/uts/aviion/lb/klog.a  
/usr/src/uts/aviion/lb/lbm.a  
/usr/src/uts/aviion/lb/lfm.a  
/usr/src/uts/aviion/lb/nc.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/pm.a  
/usr/src/uts/aviion/lb/rm.a  
/usr/src/uts/aviion/lb/sc.a  
/usr/src/uts/aviion/lb/sci.a  
/usr/src/uts/aviion/lb/sfm.a  
/usr/src/uts/aviion/lb/ts.a  
/usr/src/uts/aviion/lb/uc.a  
/usr/src/uts/aviion/lb/vm.a  
/usr/src/uts/aviion/lb/vmc.a  
/usr/src/uts/aviion/lb/vp.a  
/usr/stand/diskman

**Package 2 - Product Patch Level tcpip\_5.4R.2.10.07**

/usr/bin/ftpd  
/usr/bin/mailq  
/usr/bin/newaliases  
/usr/bin/rlogin  
/usr/bin/sendmail  
/usr/bin/smtplib  
/usr/bin/telnet  
/usr/etc/master.d/tcpip  
/usr/src/uts/aviion/lb/conf.a  
/usr/src/uts/aviion/lb/inet.a  
/usr/src/uts/aviion/lb/inso.a  
/usr/src/uts/aviion/lb/tcp.a  
/usr/src/uts/aviion/lb/udp.a

Package 3 - Product Patch Level nfs\_5.4R.2.10.01

/usr/sbin/pcnfsd

## 6. Installation Instructions

### 6.1 Loading the Patch Kit

This patch kit consists of those packages listed in the section titled "Patch Kit op-sys-x", which contain the files as listed by package in the "FILES" Section of this document. **IMPORTANT: LOAD ONLY THE PACKAGES THAT APPLY TO YOUR SYSTEM.**

To back out of this op-sys-x patch kit, 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 KIT TO AVOID OVERWRITING A PROGRAM THAT IS CURRENTLY RUNNING.**

This op-sys-x patch kit will load on any DG/UX 5.4R.2.10 system.

Before loading the patch kit, execute the following steps to boot standalone diskman and run fsck on all file systems:

Bring your system down to the SCM:

```
# cd /
# shutdown -g0 -y
# halt -q
```

Boot the tape:

```
SCM> b st(ncsc(),4)
```

Register your disks by selecting "Physical Disk Management Menu" from the Diskman Main Menu. Then select "Register, Deregister or List Registered Physical Disks" from the Physical Disk Management Menu. Select the option "Register a Physical Disk" to register each of your system disks. To run fsck on your file systems, choose the option "File System Management Menu" from the Diskman Main Menu, then choose the option "Check a File System" from the File System Management Menu. Perform this step on all file systems, including root and usr. When you're finished, exit diskman to return to the SCM, and boot your system to run level 1.

### 6.2 Loading the op-sys-x Patch Kit from Tape

The following instructions assume that your tape drive is configured at SCSI ID 4.

To load the op-sys-x patch kit, 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/usr/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 Patch Kit from CD-ROM

The following instructions assume that your CD-ROM drive is configured at SCSI ID 4.

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

1. Insert the CD-ROM and register the CD-ROM device via diskman or with the admpdisk command:

```
# admpdisk -o register '<CD-ROM_device>'
```

2. Create a mount point and mount the file system:

```
# mkdir /release
# mount -o ro /dev/dsk/+release /release
```

3. Run sysadm to install the patch kit:

```
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] /release/op-sys-x_5.4R2.10.940201
Package Name(s): [all]
List file names while loading? [no]
OK to perform operation? [yes]
Loading DG/UX Operating System...
*Loading package: <package name> .....
*Package "<package name>" has been loaded.
Updating proto root (/srv/release/PRIMARY/usr/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.

### 6.4 Loading the op-sys-x Patch Kit from a Directory

If the op-sys-x Patch Kit 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_kit
# cd /var/tmp/patch_kit
# tar xvf <path_name>/op-sys-x_5.4R2.10.940201
```

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

```
#sysadm loadpackage
Release Medium: [/dev/rmt/0] /var/tmp/patch_kit
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/usr/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 tape which can be applied on any AViiON system with a tape drive, follow the steps below:

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

## 6.5 Installing the Patch Kit

### 6.5.1 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 steps:

```
# sysadm setuppackage
Package Name(s): [all] (Type "?" to see packages to setup)
OK to perform operation? [yes]
Setting up dgux_5.4R2.10.p21 in MY_HOST root.
Setting up patch: dgux_5.4R2.10.p21.
Package dgux_5.4R2.10.p21 has been successfully set up in MY_HOST root.
Package setup for dgux_5.4R2.10.p21 is complete.
```

### 6.5.2 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.

