



Table of Contents

1	INTRODUCTION.....	9
1.1	SYSTEM IDENTIFICATION.....	9
1.2	OVERVIEW OF THE DOCUMENT	9
1.3	REFERENCE DOCUMENTS.....	9
1.4	CONVENTIONS AND SYMBOLS.....	11
2	SYSTEM OVERVIEW.....	12
2.1	REMOTE SITE	13
2.2	BASE SITE.....	14
2.3	SYSTEM 9000.....	15
3	OPERATING SYSTEM INSTALLATION AND CONFIGURATION.....	18
3.1	INGEST SERVER.....	19
3.1.1	Connections.....	19
3.1.2	RAID Controller Configuration.....	19
3.1.3	Remote Management Port Configuration.....	20
3.1.4	OS Installation.....	20
3.1.5	Initial Configuration.....	21
3.1.6	Antivirus.....	22
3.2	PROCESSING SERVERS.....	24
3.2.1	Connections.....	24
3.2.2	RAID Controller Configuration.....	24
3.2.3	Remote Management Port Configuration.....	24
3.2.4	OS Installation.....	25
3.2.5	Initial Configuration.....	26
3.2.6	Antivirus.....	27
3.3	NETWORK ATTACHED STORAGE SERVER.....	29
3.3.1	Connections.....	29
3.3.2	RAID Controller Configuration.....	29
3.3.3	Remote Management Port Configuration.....	30
3.3.4	OS Installation.....	30
3.3.5	Initial Configuration.....	31
3.3.6	Antivirus.....	32
3.3.7	Windows Update on Demand.....	32
3.4	OPERATOR WORKSTATION.....	33
3.4.1	Connections.....	33
3.4.2	RAID Controller Configuration.....	33
3.4.3	Remote Management Port Configuration.....	33
3.4.4	OS Installation.....	33
3.4.5	Initial Configuration.....	34
3.4.6	Antivirus.....	35
4	SYSTEM 9000 INSTALLATION AND CONFIGURATION.....	37
4.1	INGEST SERVER.....	38
4.1.1	Installation.....	38
4.1.2	Configuration.....	39
4.2	PROCESSING SERVERS.....	43
4.2.1	Installation.....	43
4.2.2	Configuration.....	45
4.3	OPERATOR WORKSTATION.....	47
4.3.1	Installation.....	47



4.3.2	Configuration.....	49
5	ON-SITE CONFIGURATION AND VERIFICATION.....	51
5.1	NTS/GPS UNIT.....	51
5.1.1	Network Parameters.....	51
5.1.2	NTS Operation.....	52
5.2	NAS SERVER CONFIGURATION.....	52
5.2.1	Network Parameters.....	52
5.2.2	Clock Synchronization.....	52
5.2.3	User Administrator Password.....	53
5.2.4	Remote Management.....	53
5.3	PROCESSING SERVERS CONFIGURATION.....	55
5.3.1	Network Parameters.....	55
5.3.2	Hosts Table.....	57
5.3.3	Clock Synchronization.....	57
5.3.4	Changing the Passwords.....	59
5.3.5	Password less SSH Access.....	59
5.3.6	Orbital Elements Download.....	59
5.3.7	Mounting NAS Storage Drives.....	60
5.3.8	Automatic MODIS Processing.....	61
5.3.9	Remote Management.....	61
5.3.10	Product Sharing Deployment Instructions.....	62
5.4	OPERATOR WORKSTATION CONFIGURATION.....	66
5.4.1	Network Parameters.....	66
5.4.2	Hosts Table.....	68
5.4.3	Clock Synchronization.....	68
5.4.4	Changing the Passwords.....	70
5.4.5	Password less SSH Access.....	70
5.4.6	Orbital Elements Download.....	70
5.4.7	Mounting NAS Storage Drive.....	71
5.4.8	System Alert.....	72
5.5	INGEST SERVER CONFIGURATION.....	73
5.5.1	Network Parameters.....	73
5.5.2	Hosts Table.....	75
5.5.3	Clock Synchronization.....	75
5.5.4	Changing the Passwords.....	76
5.5.5	Password less Access.....	77
5.5.6	Orbital Elements Download.....	77
5.5.7	Remote Management.....	78
5.6	INGEST SERVER VERIFICATION.....	79
5.6.1	Changing VNC Password.....	80
5.6.2	Configure Level 0 Data Distribution.....	80
5.6.3	GSI Ingest Device.....	80
5.6.4	Antenna Controller.....	80
5.6.5	X-Band Receiver.....	81
5.6.6	Antenna Alignment.....	81
5.6.7	Automatic Start-up.....	81
5.7	OPERATOR WORKSTATION VERIFICATION.....	83
5.7.1	Ingest Virtual Screen Access.....	83
5.7.2	Operator Console Access.....	83
6	ADMINISTRATOR TASKS.....	85
6.1	START-UP - REMOTE SITE.....	85
6.1.1	Antenna and Electronics.....	85
6.1.2	UPS Unit.....	85



6.1.3	NTS/GPS Unit.....	85
6.1.4	Network Switch.....	85
6.1.5	X-Band Receiver.....	85
6.1.6	GSI Unit.....	85
6.1.7	IF Fiber Optic Unit.....	86
6.1.8	RS-485 Fiber Optic Unit.....	86
6.1.9	KVM console.....	86
6.1.10	Ingest Server.....	86
6.2	START-UP - BASE SITE.....	86
6.2.1	KVM Switch.....	86
6.2.2	KVM Console.....	87
6.2.3	Network Switch.....	87
6.2.4	LTO drive.....	87
6.2.5	Network Attached Storage Server.....	87
6.2.6	Primary Processing Server.....	87
6.2.7	Backup Processing Server.....	87
6.2.8	Operator Workstation.....	88
6.3	OPERATING SYSTEM SUPPORT.....	88
6.4	ADMINISTRATIVE TASKS.....	88
6.4.1	Ingest Server.....	88
6.4.2	Processing Servers and Workstation.....	90
6.4.3	NAS Server.....	91
6.5	CLOCK SYNCHRONIZATION.....	91
6.5.1	Checking the Ingest Server Clock.....	92
6.5.2	Checking the Operator Workstation Clock.....	92
6.5.3	Checking the Primary Processing Server Clock.....	93
6.5.4	Checking the Backup Processing Server Clock.....	94
6.5.5	Checking the NAS Server Clock.....	95
6.6	SECURITY.....	95
6.7	REMOTE MANAGEMENT.....	95
6.8	ANTIVIRUS.....	96
6.8.1	Manual Scan.....	96
6.8.2	Virus Definitions Download.....	97
7	SOFTWARE MAINTENANCE.....	98
7.1	SYSTEM 9000 SOFTWARE BACKUP.....	98
7.1.1	Backup System 9000 on Ingest Server.....	98
7.1.2	Backup System 9000 on Workstation or Processing Servers.....	99
7.2	INSTALLING A SYSTEM 9000 PATCH.....	99
7.2.1	Install a patch with GPF_install.....	99
7.2.2	Install a patch without GPF_install.....	100
7.3	PROBLEM REPORTING.....	100
7.4	REMOTE MONITORING.....	101
7.5	RED HAT ENTERPRISE LINUX UPDATES.....	101
8	TROUBLESHOOTING.....	103
8.1	SYSTEM ALERT.....	103
8.2	ORBITAL ELEMENTS DOWNLOAD ALERT.....	105
8.3	CHECKING THE ANTENNA CONTROL CHAIN.....	106
8.4	BY-PASSING THE FIBER OPTIC SERIAL LINK.....	107
8.5	CHECKING THE IF CHAIN.....	108
8.6	CHECKING THE IF SIGNAL.....	109
8.7	CHECKING THE DEMODULATED SIGNAL.....	111
8.8	MISCELLANEOUS.....	111
8.8.1	Loss of power to the server rack.....	111



9	HARDWARE MAINTENANCE	112
9.1	REMOTE SITE	112
9.1.1	Radome	112
9.1.2	Working in the Radome	112
9.1.3	Indoor Downlink Electronics	118
9.1.4	NTS/GPS Unit	123
9.1.5	Ingest Server	123
9.1.6	Network Switch	124
9.1.7	KVM Console	124
9.1.8	UPS Unit	124
9.2	BASE SITE	124
9.2.1	Processing Servers	124
9.2.2	LTO Drive	125
9.2.3	Network Attached Storage Server	125
9.2.4	KVM Console and Switch	125
9.2.5	Operator Workstation	125
9.3	PREVENTATIVE MAINTENANCE SCHEDULE	126
A.	ACRONYMS AND ABBREVIATIONS	127
B.	PASSWORD LESS SSH ACCESS.....	129
C.	WEST SITE SYSTEM PARAMETERS	130
D.	EAST SITE SYSTEM PARAMETERS	135

List of Figures

FIGURE 2-1 ESC SYSTEM BLOCK DIAGRAM	12
FIGURE 2-2 REMOTE SITE, HARDWARE COMPONENTS.....	13
FIGURE 2-3 BASE SITE, HARDWARE COMPONENTS.....	14
FIGURE 2-4 SYSTEM DATA FLOW	15
FIGURE 2-5 INGEST VIRTUAL SCREEN	16
FIGURE 2-6 OPERATOR CONSOLE	17

List of Tables

TABLE 1-1 REFERENCE DOCUMENTS.....	10
---	-----------



1 Introduction

This document is intended for the maintenance of the Environmental Sensing Capability (ESC) of the Department of the National Defence (DND) of the Polar Epsilon Project. This document (CDRL-027) describes the tasks necessary to install, configure, and maintain the software as well as maintain, repair, or replace the hardware comprising the ESC. This manual is used in conjunction with the Technical Data Package Manual and the Operator Manual.

1.1 System Identification

Each instance of the ESC is geographically separated into two sites. The earth station components of the ESC are located at the remote site. The operator workstation, and MODIS processing and data storage components are installed at a Canadian Forces Base at which the MetOC is located and initial analysis of the generated oceanographic products by the users occurs. Section 2 provides an overview of the ESC system components.

1.2 Overview of the Document

This document is divided into nine main sections:

- Section 1 defines relations and context for the rest of the document
- Section 2 shows an overview the ESC System
- Section 3 describes the Operating System installation and configuration
- Section 4 describes the System 9000 software installation and configuration
- Section 5 describes the on-site configuration and verification
- Section 6 describes the administrator's tasks
- Section 7 describes the software maintenance
- Section 8 describes the troubleshooting
- Section 9 describes the hardware maintenance

1.3 Reference Documents

Table 1-1 presents a list of reference documents (RD-#). The documents are located in the Manuals folder on the PE-ESC MODIS DVD delivered with the system. New versions of these documents are provided in the Patch Release DVD provided by GI/IES.



Environmental Sensing Capability Polar Epsilon Maintenance Manual



Doc #	Title	Reference Number, File Name, or URL	Issue	Date
RD-01	System Design Description	CDRL-010	1.6	09-08-2016
RD-02	Operators Manual	CDRL-028	1.12	12-20-2016
RD-03	Technical Data Package	CDRL-030	1.11	09-08-2016
RD-04	MODIS Ingestion User Guide	MODIS-Ingestion-User-Guide-2016-09-09-v4.5.pdf	4.5	09-09-2016
RD-05	SeaDAS MODIS Processing User Guide	SeaDAS-MODIS-Processing-User-Guide-2016-12-20-v4.6.pdf	4.6	12-20-2016
RD-06	SeaDAS MODIS Processing User Reference	SeaDAS-MODIS-Processing-User-Reference-2016-12-20-v4.4.pdf	4.4	12-20-2016
RD-07	System Configuration Items; <ul style="list-style-type: none"> • Hardware Configuration Items • Software Configuration Items • System Spare Parts • System Test Equipment 	DND-PE-ES-System-Configuration-Items-2016-09-08.xls	1.0	09-08-2016
RD-09	Maintenance Plan	CDRL-005	2.2	12-04-2014
RD-10	OTRS Customer Guide	OTRS Quick Guide for Customer Interface.pdf		July 4 th , 2012
RD-11	Symantec Antivirus for Linux Client Guide	SAV_Linux_Client.pdf		
RD-12	Symantec Antivirus for Linux Implementation Guide	SAV_Linux_Impl.pdf		
RD-13	Product Sharing Description	DND-PE-Product-Sharing-Description-2016-09-08-v1.1.pdf	1.1	09-08-2016
RD-20	L-3 ESSCO Installation, Operations & Maintenance Manual	L3-ESSCO_IOM_TM10-21.pdf (Also as a Printed Document)	J09-3137	05-18-2010
RD-21	ORMEC G-Series Digital Servodrive Reference	Ormec_Servodrive_Ref.pdf	Rev. B	
RD-22	Network Time Server NTS-150 & NTS-150D User's Manual	nts-150man.pdf	Rev. G	Feb 2005
RD-23	Dell PowerEdge R710 Systems Hardware Owner Manual	PER710_HOM.pdf	Rev. A03	Sep 2009
RD-24	Linksys WebView Switches User Guide	SRW-US_v10_UG_A-Web.pdf		
RD-25	Dell Online Rack UPS 2700W User's Guide	2700_UPS.pdf		June 2009
RD-26	Dell UPS Managements Software Installation and Configuration Guide	UPSManagementSoftware.pdf		May 2009
RD-27	Dell PowerVault LTO4-120HH Tape Drive User's Guide	http://support.dell.com/support/edocs/stor-sys/LTO4120H/IBM/en/ug_en/index.htm		
RD-28	Dell PowerVault NX3000 Systems Hardware Owner's Manual	HOMA00MR.pdf	Rev. A00	Apr 2009
RD-29	Dell PowerVault NX3000 Systems Administrator's Guide	AG_en.pdf	Rev. A00	Mar 2010
RD-30	Dell PowerVault NX3000 Systems Troubleshooting Guide	TG_en.pdf	Rev. A00	Apr 2010
RD-31	Dell Precision Workstation T7500 Setup and Features Information	sfits_en.pdf		Jun 2009

Table 1-1 Reference Documents



(*) *Spare parts procured vary slightly from those listed in the RSPL. Contact the ES LCMM to determine spares availability.*

Note: All OEM documentation listed in Table 1-1 is provided on the final deliverable documentation CD.

1.4 Conventions and Symbols

Throughout this document, the keys pressed by the user are shown between []. The symbol [Ctrl-E] means the [E] key is pressed while pressing the key [Ctrl]. The symbol [Space] refers to pressing the space bar.

If you are requested to enter some value or text, the possible choices will be shown between single quotes. If the choice is yours, a placeholder, <my-choice>, is shown. Note that this convention may be used on the commands you are requested to execute.

The commands you are requested to execute are in "Courier New" font when shown on a separate line. When they are embedded in the text, they are shown between single quotes and in the text font.

The following symbols are used throughout this manual:

Y	Year. (2002, 2003, ...)
yy	Last two digits of the year (02, 03, ...)
M	Month of the year (01, 02, ..., 11, 12)
D	Day of the month (01, 02, ..., 30, 31)
h	Hour (01, 02, ..., 23)
m	Minute (01, 02, ..., 58, 59)
s	Second (01, 02, ..., 58, 59)
ddd	Day of year (001, 002, ..., 365)
sid	Satellite ID: eam1 for TERRA and epm1 for AQUA.



2 System Overview

The function of the ESC system is to generate Ocean Color (OC) and Sea Surface Temperature (SST) from the Moderate Resolution Imaging Spectroradiometer (MODIS) instrument of the NASA Earth Observing System (EOS) satellites Aqua and Terra and to make these products available for export to other systems. The MODIS data is available in real-time via the Direct Broadcast (DB) and in a time-delayed fashion via the Internet.

Each instance of the ESC is geographically separated into two sites. The earth station components of ESC are located at the remote site. The operator workstation and the MODIS processing and data storage components are installed at a Canadian Forces Base at which the MetOC is located. A high level, system block diagram of the ES capability is depicted in Figure 2-1.

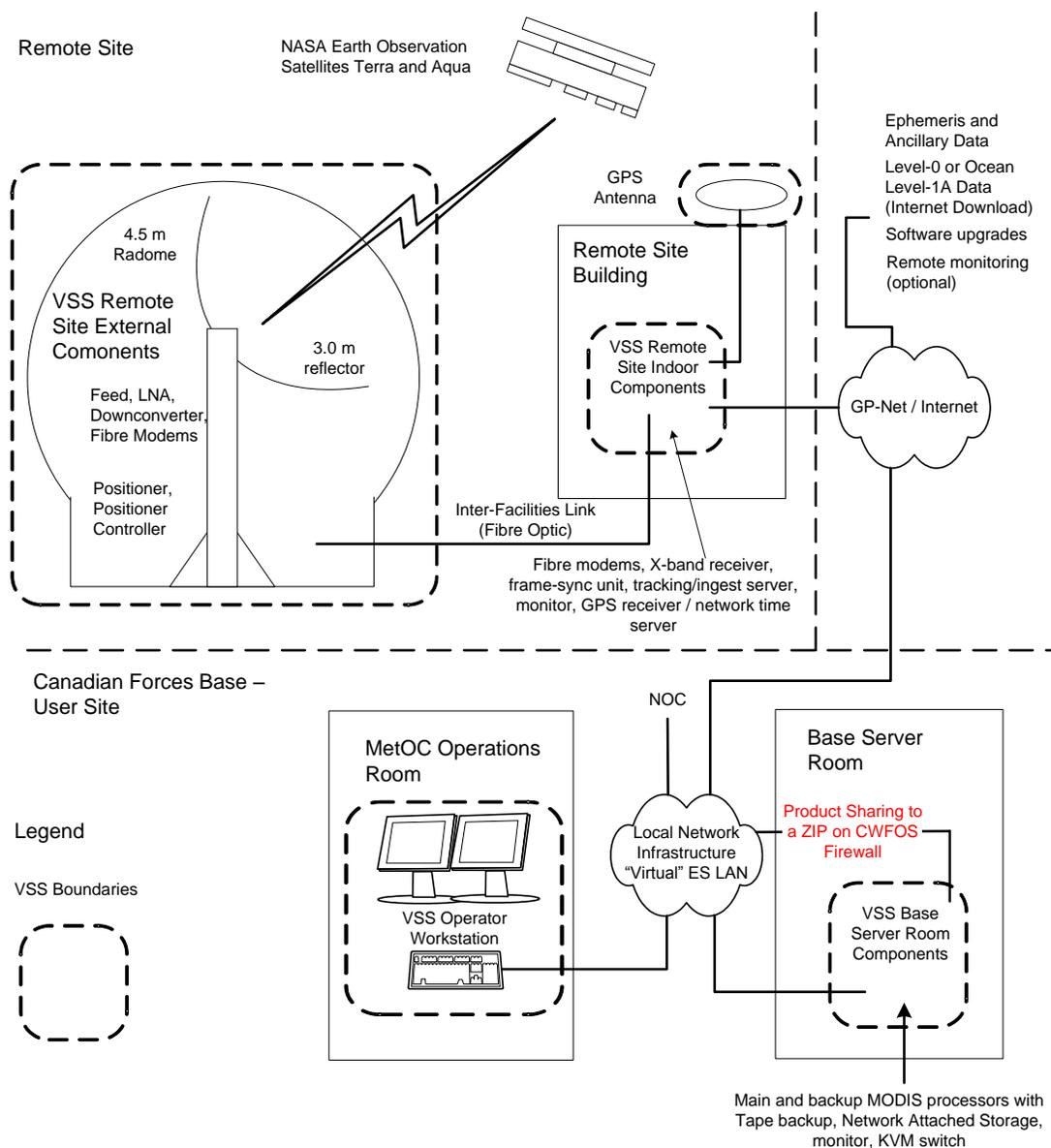


Figure 2-1 ESC System Block Diagram



2.1 Remote Site

The figure below shows a block diagram of the ESC outdoor and indoor components at the remote site with connection between the various components including the connection to the base site via the GP-Net Router.

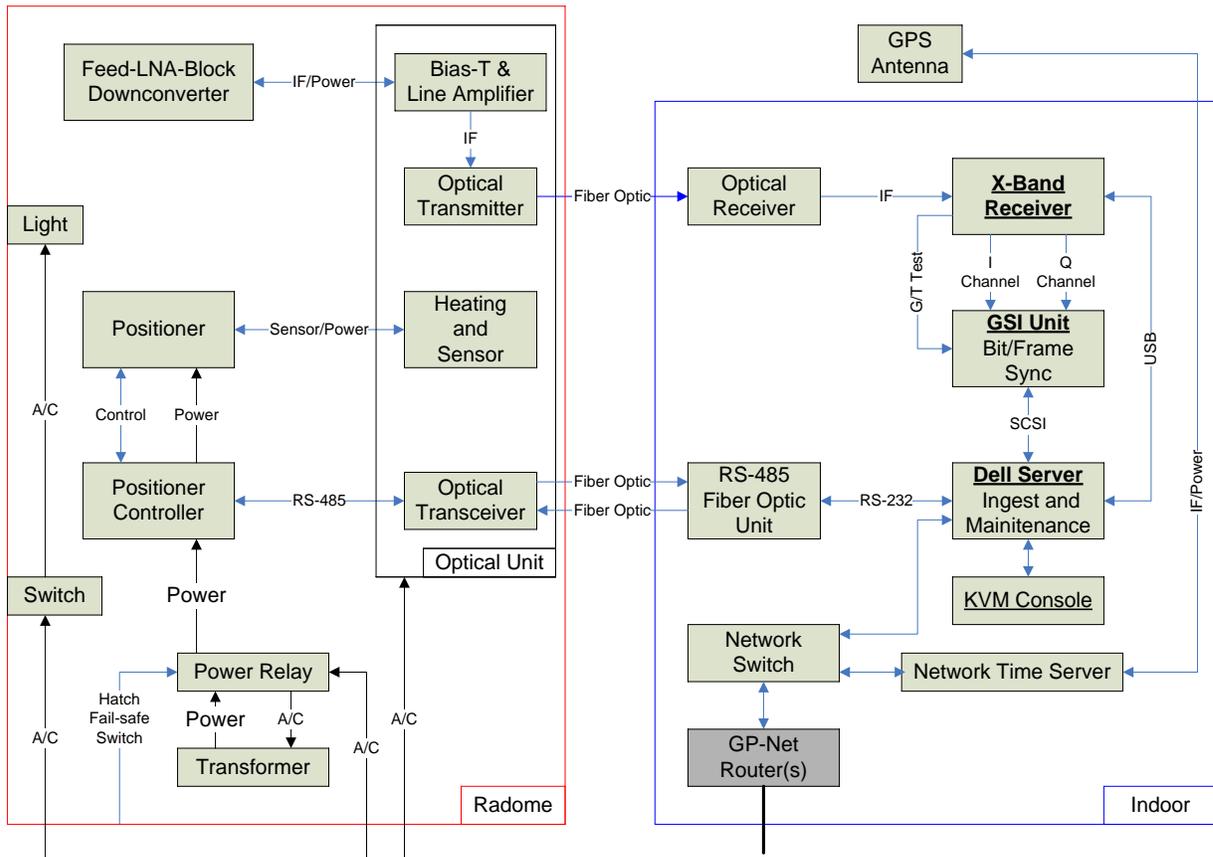


Figure 2-2 Remote Site, Hardware Components



2.2 Base Site

The figure below shows a block diagram of the ESC components at the Canadian Forces Base site with connection between the various components including the connection to the base site via the GP-Net Router.

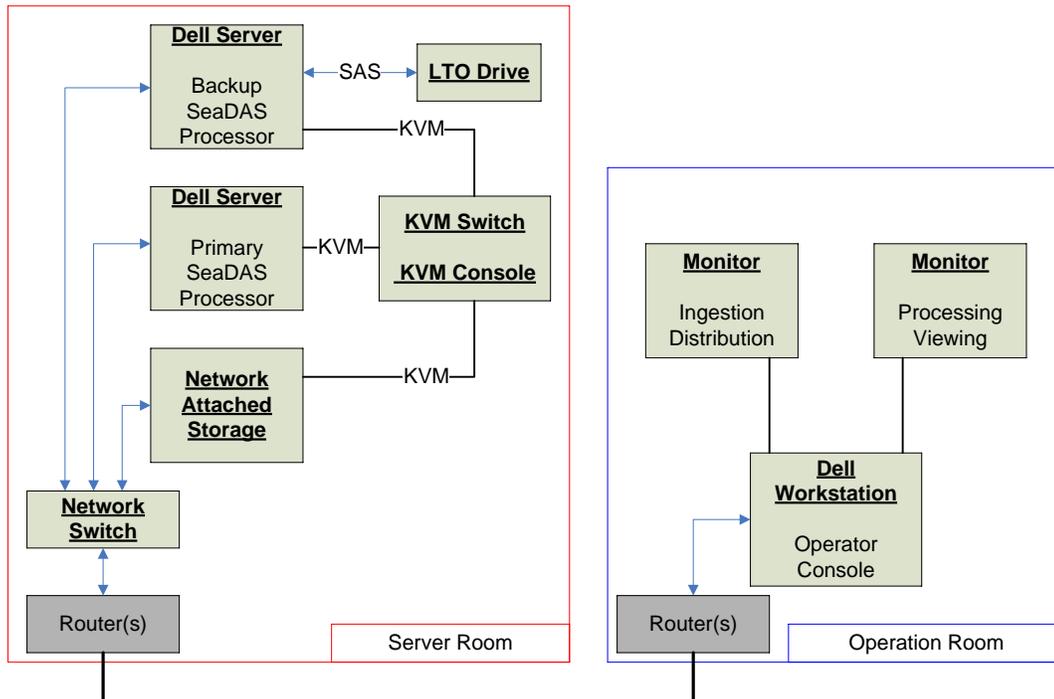


Figure 2-3 Base Site, Hardware Components



2.3 System 9000

The acquisition of the Aqua/Terra DB is done by the ingest processor, which converts the incoming telemetry to level 0 and distributes it to the primary processor. If it fails to distribute to the primary processor, the level 0 data is sent to the secondary processor. The processor receiving the level 0 data generates level 2 and 3 oceanographic products. The operator, via its workstation, monitors and controls the ingestion and the automatic processing. The operator is also responsible for the importation of external level 0 or 1A data and its processing, as well as the exportation of oceanographic products. The data flow of the ESC system is shown in the following figure.

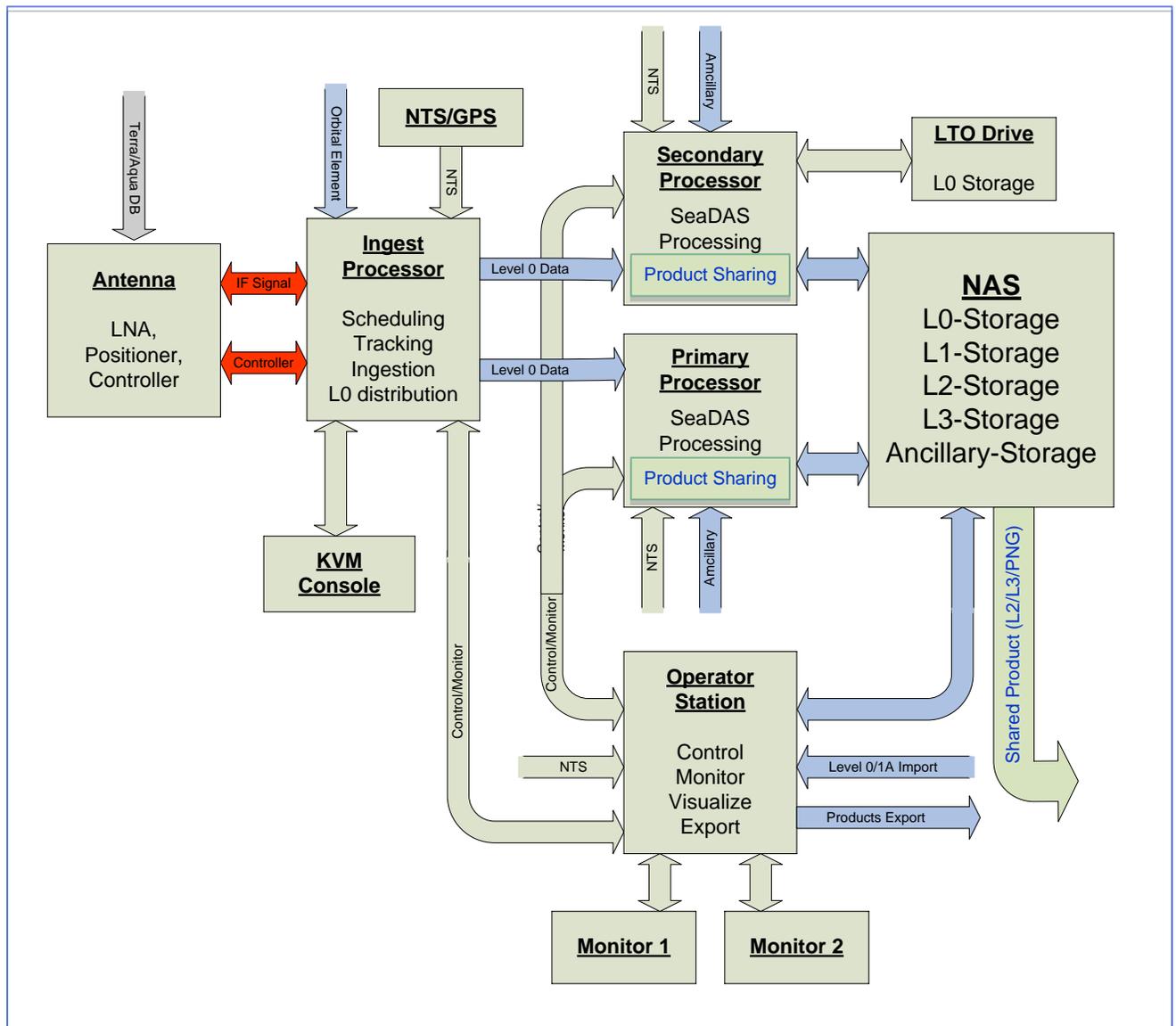


Figure 2-4 System Data Flow

The operations shown in the diagram above include scheduling, tracking satellites, ingestion, Level 0 distribution, MODIS processing, storage to the Network Attached Server (NAS), and shared product distribution. These operations are done through the System 9000 software with the



exception of the shared product distribution. Note that System 9000 contains a MODIS processing layer interfacing with the SeaDAS processing software obtained from NASA. This layer provides a naming convention to ensure unique product names and a storage methodology for easy access to the global products stored on the NAS by both processors and the operator workstation. The software is divided into four main parts:

- Scheduling, tracking, ingestion, and Level 0 data distribution
- MODIS processing
- Shared product distribution
- Operator Console

The scheduling, tracking, ingestion, and distribution are done on the ingest processor located at the remote site. These operations are monitored and controlled via an Ingest Virtual Screen (IVS) displayed on the operator workstation or any computer on the network via a Virtual Network Computing (VNC) viewer. The figure below shows a typical IVS.

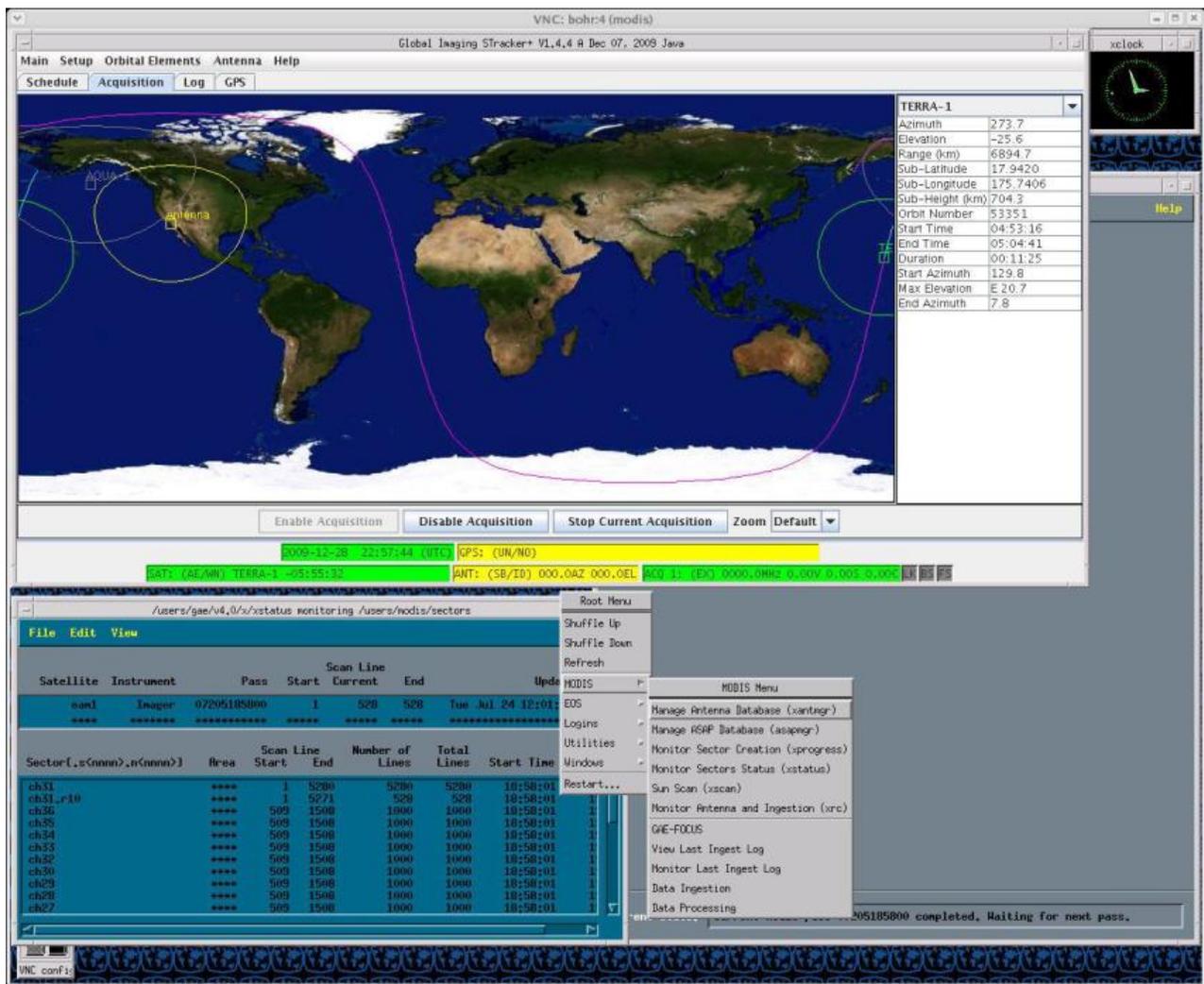


Figure 2-5 Ingest Virtual Screen



The MODIS processing is divided into automatic and manual processing. The automatic processing is done on the primary or the backup MODIS processor. The manual processing is done on the operator workstation. The processing is controlled and monitored via an operator console, shown below, running on the computer performing the processing.

The shared products, generated with either the manual or automatic processing and stored on the NAS are distributed to a Zone Interface Point (ZIP) on the CFWOS firewall with the Product Sharing software. Refer to RD-13 for a description of the Product Sharing software.

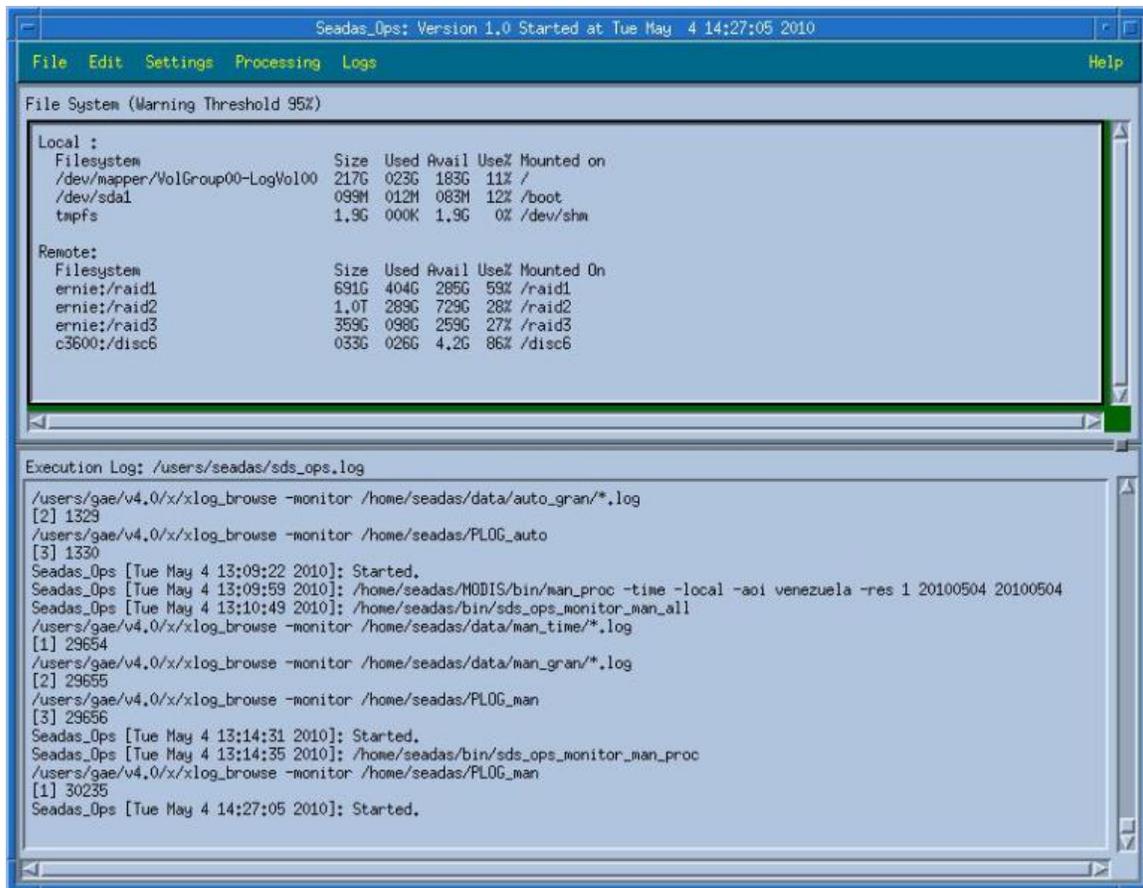


Figure 2-6 Operator Console

The operator console provides menu to enable to perform various tasks. The operator console is described in document RD-02.



3 Operating System Installation and Configuration

This section describes the installation of the Operating Systems (OS) on the various computers of the ESC system and their configurations. The computers are delivered with the OS installed and configured. Therefore, you may skip to the section labelled “System 9000 Installation and Configuration”.

The ESC system has four computer systems each with the following OS:

- Ingest Server running Red Hat Enterprise Linux Version 4 Update 8
- Processing Servers running Red Hat Enterprise Linux 6.7
- Operator Workstation running Red Hat Enterprise Linux 6.7
- Network Attached Storage Server running Windows Storage 2008 Standard

The following assumptions are made throughout this section:

- The equipment comprising the ESC system is powered and running.
- All computers have at least one network connection.
- The LTO tape drive is connected to the secondary or backup processing server.
- The NTS-150 unit is powered and is connected to the network.
- The GPS antenna is mounted on the roof and is connected to the NTS unit.
- The X-Band antenna is installed, powered, and connected to the ingest rack via two fiber optic links: RS-485 and IF signal.



3.1 *Ingest Server*

3.1.1 Connections

Before starting the OS installation, verify that the following connections are present:

- Analog Video and Keyboard/Mouse to the KVM console
- SCSI connection to the ingest unit
- USB connection to the MODIS Mk II Receiver
- USB Dongle
- Serial connection to the RS-485 Fiber Optic unit
- Built-in 1Gbit NIC 1 connected to the network switch

Additionally, confirm that the receiver I/Q channels are connected to the GSI unit and that the receiver is connected to its fiber optic unit.

3.1.2 RAID Controller Configuration

The two drives delivered with the ingest server are mirrored (RAID level 1). In the unlikely event both drives are replaced, you will need to access the RAID controller BIOS to set-up the new drives as RAID level 1. After powering the server, wait for the message

```
Power Edge RAID Controller BIOS
....
Press <Ctrl><E> to Run Configuration Utility
```

Once you have entered [Ctrl-E], the PERC 6/I Integrated BIOS Configuration Utility appears. If needed, use [Ctrl-N] and [Ctrl-P] to show the “VD Mgmt” pane. In this pane you will see the RAID organizational tree showing the “Disk Group” and “Virtual Disk” under one or more RAID controllers. Use the up and down arrow keys to move/highlight the desired item. If “Virtual Disk 0” is already present in the tree, the drives have already been configured. In this case, you can exit the utility by pressing [Esc]. Otherwise, follow these steps:

- Move to “Controller 0” and press [F2] to show the operations menu.
- In this menu, move to “Create New VD” and press [Enter]. The Virtual Disk Management dialog appears:
 - Move to the “RAID Level” window and select RAID Level 1.
 - Move to the first drive in the “Physical Disk Window” and press [Enter] to select. Repeat for the second drive.
 - Move to the “OK” button and press [Enter].
- You should see a “Disk Group 0” and a new “Virtual Disk 0” under “Controller 0”.
- Press [Esc]. Move to the OK button and press [Enter].
- Press [Ctrl-Alt-Del] to reboot.



3.1.3 Remote Management Port Configuration

The remote management port allows the administrator to access the integrated Dell Remote Access Controller (iDRAC) and manage the machine hardware. The iDRAC shares access on any NIC port on the machine. This section describes the steps to set an IP address for the iDRAC as well as a login name and password for remote access. This iDRAC user has administrator privileges.

After powering the server, wait for the message

```
iDRAC6 Configuration Utility 1.45
...
Press <Ctrl><E> for remote access setup within 5 seconds...
```

Once you have typed [Ctrl-E], the iDRAC Configuration Utility appears. Use the up and down arrow keys to move/highlight the desired item. Follow these steps:

- Move to "LAN Parameters" and press [Enter]. In this dialog:
 - Move to "Host Name" and press [Enter]. Type 'Admin' and press [Enter].
 - Move to "IPV4 Address Source" and set it to "Static". Use the space bar to toggle between "Static" and "DHCP".
 - Move to "IPV4 Address". Move the first dotted octet of the IP address and set it. Repeat for the other octets.
 - Move the "Subnet mask" and set it.
 - Move to "Default Gateway" and set it.
 - Move to "DNS Server" and set it.
 - Press [Esc] to exit this dialog.
- Move to "LAN User Configuration" and press [Enter]. In this dialog:
 - Move the "Account User Name" and enter "Admin".
 - Move to "Enter Password" and set it.
 - Move to "Confirm Password" and repeat it.
 - Press [Esc] to exit this dialog.
- Press [Esc] to exit. Move to "Save Changes and exit" and press [Enter]. The boot will continue automatically.

3.1.4 OS Installation

This section describes the operating system installation. Immediately after powering the server, insert the installation DVD marked "Red Hat Enterprise Linux Version 4 for 32-bit x86". The server will boot from the DVD. Follow these steps:

- When requested, select the installation in graphical mode.
- Skip the verification of the CD media.
- Click "Next" to skip the welcome screen.
- Select "English (English)" for the language.
- Select "U.S. English" for the keyboard.
- Select "Install" if the presence of an OS on the drives is detected.
- Select "Automatic Partitioning".
 - Click on "Remove all partitions on the system".



- Select “sda 237822 MB ...”
- Select “Review (and modify if needed) the partitions created”. The swap should be about 2Gbytes greater than the memory on the machine.
- Click “Next”.
- Click “Yes” to continue.
- Click “Next” to select the default. Otherwise, make appropriate changes.
- Click “Next” in Boot Loader Configuration.
- In the Network Configuration:
 - Highlight and click on “eth0...”
 - Click “Edit”
 - Un-select “Configure DHCP”.
 - Select “Activate on boot”.
 - Enter the IP address and the network mask.
 - Enter the hostname.
 - Enter the gateway, primary DNS, and other DNS if desired.
 - Click Next.
- In the Firewall Configuration:
 - Select “Enable Firewall”.
 - Select “Remote Login (SSH)”.
 - Select “Active” when enabling SELinux.
 - Click Next.
- Click “Next” in Additional Language Support.
- In the Network Time Server:
 - Click on the appropriate city on the map.
 - Click on either of the following for the appropriate time zone settings:
 - America/Vancouver – Pacific Time – West British Columbia
 - America/Halifax Atlantic Time – Nova Scotia
 - Select “System Clock uses UTC”.
 - Click “Next”.
- Set the root password.
- In Package Installation Defaults:
 - Select “Customize software packages to install”.
 - Click “Next”.
 - Scroll to bottom and select “Everything”.
 - Click “Next”.
- Click “Reboot” when done with the installation.

3.1.5 Initial Configuration

An initial configuration menu appears on the first boot after the OS has been installed. Follow these steps:

- Click “Next” to skip the welcome screen.
- Click “Next” to accept the License Agreement.
- In Date and Time:
- Click on the “Network Time Protocol” panel.



- Select “Enable Network Time Protocol”.
- Enter the IP address of each Network Time Source and click “Add”.
- Click “Show Advanced Options”.
- Select “Use Local Tim Source”.
- You can also set the time zone with the “Timezone” panel.
- Click “Next”.
- Select the display to 1024 x 1280 and 32 million colors and click “Next”.
- In “Red Hat Login”, select “Tell me why I need to register...” and click “Next”.
- In “Why register”, select “I cannot complete...” and click “Next”.
- Click “Next” to skip “System User”.
- Click “Next” to skip “Additional CDs”.
- Click “Next”.

A login prompt will appear. The server is now ready for the System 9000 software installation and configuration.

3.1.6 Antivirus

To install the Symantec antivirus software on Linux, log in as user root at the server or workstation console.

- Insert the DVD or USB Flash Drive labelled GI-MODIS.
- If a DVD or USB icon does not appear, double-click on the Computer icon and double-click on the DVD or USB icon.
- With the cursor on the background, press the right-mouse button, move to “Open Terminal” and release the button. A terminal window appears. The commands are entered in this window.
- In this terminal window, type the command ‘df -h’ to find the name under which the DVD installation media has been mounted: /media/<device>. Replace <device> with the appropriate value whenever it is mentioned in this document.
- Execute the following commands:

```
cd /root
export SAV_DIR=/media/<device>/Symantec/Linux
cp $SAV_DIR/sav*.bash /root
chmod 744 sav*.bash
./sav-install.bash $SAV_DIR/sav-linux-1.0.9-13.tgz
umount /media/<device>
```

- Disable the auto protection (to keep performance up):

(lines beginning with # are comments, lines in *Italic* are the program responses)

```
# Check status
/opt/Symantec/symantec_antivirus/sav info -a
Enabled #--> Auto Protect is Enabled

# Disable Auto Protect
/opt/Symantec/symantec_antivirus/sav autoprotect -d
/opt/Symantec/symantec_antivirus/sav info -a
```



Disabled # --> Auto Protection is disabled

- Check definition update time:

```
# Check Update of Virus Definitions Download
/opt/Symantec/symantec_antivirus/sav liveupdate -v
Frequency:      Weekly - Fri at 20:00
Missed Events:  Enabled
State:          Enabled
```

- Manual Scanning:

```
# Manual Scanning
/opt/Symantec/symantec_antivirus/sav manualscan -s <directory>
# --> Reports no info to terminal, check
/var/symantec/Logs/<date>.log
# It is up to each site to come up with a schedule to
# perform the manual scans on a routine basis.
```

- Running Daemons:

```
# Daemons: symcfgd and rtvscand services
# Both are running by default.
# REQUIRED FOR MANUAL SCAN!
# rtvscand is actually the scan engine.
```



3.2 Processing Servers

3.2.1 Connections

Before starting the OS installation, verify that the following connections are present:

- Analog Video and Keyboard/Mouse to the KVM switch
- USB Dongle
- Built-in 1Gb NIC 1 connected to the network switch
- LTO drive connected to the backup processor

3.2.2 RAID Controller Configuration

The two drives delivered with the processing server are mirrored (RAID level 1). In the unlikely event both drives are replaced, you will need to access the RAID controller BIOS to set-up the new drives as RAID level 1. After powering the server, wait for the message

```
Power Edge RAID Controller BIOS
....
Press <Ctrl><E> to Run Configuration Utility
```

Once you have entered [Ctrl-E], the PERC 6/I Integrated BIOS Configuration Utility appears. If needed, use [Ctrl-N] and [Ctrl-P] to show the “VD Mgmt” pane. In this pane you will see the RAID organizational tree showing the “Disk Group” and “Virtual Disk” under one or more RAID controllers. Use the up and down arrow keys to move/highlight the desired item. If “Virtual Disk 0” is already present in the tree, the drives have already been configured. In this case, you can exit the utility by pressing [Esc]. Otherwise, follow these steps:

- Move to “Controller 0” and press [F2] to show the operations menu.
- In this menu, move to “Create New VD” and press [Enter]. The Virtual Disk Management dialog appears:
 - Move to the “RAID Level” window and select RAID Level 1.
 - Move to the first drive in the “Physical Disk Window” and press [Enter] to select. Repeat for the second drive.
 - Move to the “OK” button and press [Enter].
- You should see a “Disk Group 0” and a new “Virtual Disk 0” under “Controller 0”.
- Press [Esc]. Move to the OK button and press [Enter].
- Press [Ctrl-Alt-Del] to reboot.

3.2.3 Remote Management Port Configuration

The remote management port allows the administrator to access the integrated Dell Remote Access Controller (iDRAC) and manage the machine hardware. The iDRAC shares access on any NIC port on the machine. This section describes the steps to set an IP address for the iDRAC as well as a login name and password for remote access. This iDRAC user has administrator privileges.



After powering the server, wait for the message

iDRAC6 Configuration Utility 1.45

...

Press <Ctrl><E> for remote access setup within 5 seconds...

Once you have typed [Ctrl-E], the iDRAC Configuration Utility appears. Use the up and down arrow keys to move/highlight the desired item. Follow these steps:

- Move to "LAN Parameters" and press [Enter]. In this dialog:
 - Move to "Host Name" and press [Enter]. Type 'Admin' and press [Enter].
 - Move to "IPV4 Address Source" and set it to "Static". Use the space bar to toggle between "Static" and "DHCP".
 - Move to "IPV4 Address". Move the first dotted octet of the IP address and set it. Repeat for the other octets.
 - Move the "Subnet mask" and set it.
 - Move to "Default Gateway" and set it.
 - Move to "DNS Server" and set it.
 - Press [Esc] to exit this dialog.
- Move to "LAN User Configuration" and press [Enter]. In this dialog:
 - Move the "Account User Name" and enter "Admin".
 - Move to "Enter Password" and set it.
 - Move to "Confirm Password" and repeat it.
 - Press [Esc] to exit this dialog.
- Press [Esc] to exit. Move to "Save Changes and exit" and press [Enter]. The boot will continue automatically.

3.2.4 OS Installation

This section describes the operating system installation on the processing servers. Immediately after powering the server, insert the DVD marked "Red Hat Enterprise Linux 6.7 (64-bit) Installation Disc". After the hardware has been initialized, a *Welcome to RHEL 6.7* screen appears. Select *Install or Upgrade an Existing System* and press [Enter]. At the next screen, select *Skip* to skip the testing of the DVD and press [Enter]. Wait approximately 60 seconds for the *RHEL 6* screen to appear and click *Next*, in the lower right corner of the screen, to proceed with the installation steps shown below along with the defaults:

Steps	Default
• Language	English
• Keyboard	U.S. English
• Devices	Select <i>Basic Storage Devices</i>
• Installation	Select <i>Fresh Installation</i>
• Hostname & Network	Enter the hostname Click <i>Configure Network</i> Highlight <i>em1</i> and click <i>Edit</i> Select <i>Connect automatically</i>



Select *IPv4 Settings*

Select *Manual* as the Method:

Click *Add*.

Enter IP address. Press [Tab]

Enter Netmask. Press [Tab]

Enter Gateway. Press [Tab]

Enter DNS server(s)

Click *Apply*

Click *Close*

Click Next

- Time Zone Select time zone for your location. Click *Next*.
- Root Password Enter and confirm the root password. Click *Next*.
- Partitioning Select *Replace Existing Linux System(s)*
Click *Review and modify partitioning layout*
Click *Next*.
The Partitions Menu appears.
Modify as desired. Click *Next* when done.
Click *Write changes to disk* if requested.
(It will take several minutes to format the drive)
- Boot Loader Use the defaults. Click *Next*.
- Software Select *Software Development W/S* and click *Next*.
(It will take several minutes to install the RPMs)

Click *Reboot* to reboot the machine once the installation is finished.

3.2.5 Initial Configuration

An initial configuration menu appears on the first boot after the OS has been installed. Click *Forward* to proceed with the steps necessary to make your system ready to use:

- License Information Agree and click *Forward*
- Set Up Software Updates Select *No, I prefer to register at a later time*.
Click *Forward*
- Create User Click *Forward*. This step can be done at a later time
- Date and Time Click *Synchronize date and time over the network*
Remove current NTS entries.
Add local NTS IP address.
Click *Advanced Options*
Select *Speed up initial synchronization*
Click *Forward*
- Kernel Dump Use defaults or define as desired. Click *Finish*.
Click *Yes* to use these settings.
Click *OK* to reboot.

Once the machine has booted, log in as user root at the console login screen. The GNOME Environment appears. Next, move the cursor on the background, press the right-mouse button to



display the menu, move to “Open Terminal” and release the button. A terminal window appears. Enter the following command to register this machine for Red Hat Updates:

```
subscription-manager register --username <u> --password <p> --auto-attach
```

where <u> and <p> are the user name and password respectively of your Red Hat account.

The server is now ready for the System 9000 software installation and configuration.

3.2.6 Antivirus

To install the Symantec antivirus software on Linux, log in as user root at the server or workstation console.

- Insert the DVD or USB Flash Drive labelled GI-MODIS.
- If a DVD or USB icon does not appear, double-click on the Computer icon and double-click on the DVD or USB icon.
- With the cursor on the background, press the right-mouse button, move to “Open Terminal” and release the button. A terminal window appears. The commands are entered in this window.
- In this terminal window, type the command ‘df -h’ to find the name under which the DVD installation media has been mounted: /media/<device>. Replace <device> with the appropriate value whenever it is mentioned in this document.
- Execute the following commands:

```
cd /root
export SAV_DIR=/media/<device>/Symantec/Linux
cp $SAV_DIR/sav*.bash /root
chmod 744 sav*.bash
./sav-install.bash $SAV_DIR/sav-linux-1.0.9-13.tgz
umount /media/<device>
```

- Disable the auto protection (to keep performance up):

(lines beginning with # are comments, lines in *Italic* are the program responses)

```
# Check status
/opt/Symantec/symantec_antivirus/sav info -a
Enabled #--> Auto Protect is Enabled

# Disable Auto Protect
/opt/Symantec/symantec_antivirus/sav autoprotect -d
/opt/Symantec/symantec_antivirus/sav info -a
Disabled # --> Auto Protection is disabled
```

- Check definition update time:

```
# Check Update of Virus Definitions Download
/opt/Symantec/symantec_antivirus/sav liveupdate -v
Frequency: Weekly - Fri at 20:00
Missed Events: Enabled
State: Enabled
```



- Manual Scanning:

```
# Manual Scanning
# /opt/Symantec/symantec_antivirus/sav manualscan -s <directory>
# --> Reports no info to terminal, check
# /var/symantec/Logs/<date>.log
# It is up to each site to come up with a schedule to
# perform the manual scans on a routine basis.
```

- Running Daemons:

```
# Daemons: symcfgd and rtvscand services
# Both are running by default.
# REQUIRED FOR MANUAL SCAN!
# rtvscand is actually the scan engine.
```



3.3 Network Attached Storage Server

3.3.1 Connections

Before starting the OS installation, verify that the following connections are present:

- Analog Video and Keyboard/Mouse to the KVM console
- USB Dongle
- Built-in 1Gb NIC 1 connected to the network switch

3.3.2 RAID Controller Configuration

Six drives are delivered with the NAS server. The two smaller drives are mirrored (RAID level 1) and contain a root partition and a small storage partition. The four bigger drives are configured at RAID level 5 and contain one storage partition. In the unlikely event both root drives or all four storage drives are replaced at once, you will need to access the RAID controller BIOS to set-up the new drives as RAID level 1. After powering the server, wait for the message

Power Edge RAID Controller BIOS

....

Press <Ctrl><E> to Run Configuration Utility

Once you have entered [Ctrl-E], the PERC 6/I Integrated BIOS Configuration Utility appears. If needed, use [Ctrl-N] and [Ctrl-P] to show the “VD Mgmt” pane. In this pane you will see the RAID organizational tree showing the “Disk Group” and “Virtual Disk” under one or more RAID controllers. Use the up and down arrow keys to move/highlight the desired item. If “Virtual Disk 0” and “Virtual Disk 1” are already present in the tree, the root drives and the data drives have already been configured. In this case, you can exit the utility by pressing [Esc]. Otherwise, follow these steps:

- If “Virtual Disk 0” is not present:
 - Move to “Controller 0” and press [F2] to show the operations menu.
 - In this menu, move to “Create New VD” and press [Enter]. The Virtual Disk Management dialog appears.
 - To configure the root drives:
 - Move to the “RAID Level” window and select RAID Level 1.
 - Move to the first drive in the “Physical Disk Window” and press [Enter] to select. Repeat for the second drive. **Note: select the 146 Gbytes drives.**
 - Move to the “OK” button and press [Enter].
 - You should see “Virtual Disk 0” under “Controller 0”.
- If “Virtual Disk 1” is not present:
 - Move to “Controller 0” and press [F2] to show the operations menu.
 - In this menu, move to “Create New VD” and press [Enter]. The Virtual Disk Management dialog appears.
 - To configure the storage drives:
 - Move to the “RAID Level” window and select RAID Level 5.
 - Move to the first drive in the “Physical Disk Window” and press [Enter] to select. Repeat for the three other drives. **Note: select the 450 Gbytes drives.**



- Move to the “OK” button and press [Enter].
- You should see “Virtual Disk 1” under “Controller 0”.
- Press [Esc]. Move to the OK button and press [Enter].
- Press [Ctrl-Alt-Del] to reboot.

3.3.3 Remote Management Port Configuration

The remote management port allows the administrator to access the integrated Dell Remote Access Controller (iDRAC) and manage the machine hardware. The iDRAC shares access on any NIC port on the machine. This section describes the steps to set an IP address for the iDRAC as well as a login name and password for remote access. This iDRAC user has administrator privileges.

After powering the server, wait for the message

```
iDRAC6 Configuration Utility 1.45
...
Press <Ctrl><E> for remote access setup within 5 seconds...
```

Once you have typed [Ctrl-E], the iDRAC Configuration Utility appears. Use the up and down arrow keys to move/highlight the desired item. Follow these steps:

- Move to "LAN Parameters" and press [Enter]. In this dialog:
 - Move to “Host Name” and press [Enter]. Type ‘Admin’ and press [Enter].
 - Move to “IPV4 Address Source” and set it to “Static”. Use the space bar to toggle between “Static” and “DHCP”.
 - Move to “IPV4 Address”. Move the first dotted octet of the IP address and set it. Repeat for the other octets.
 - Move the “Subnet mask” and set it.
 - Move to “Default Gateway” and set it.
 - Move to “DNS Server” and set it.
 - Press [Esc] to exit this dialog.
- Move to “LAN User Configuration” and press [Enter]. In this dialog:
 - Move the “Account User Name” and enter “Admin”.
 - Move to “Enter Password” and set it.
 - Move to “Confirm Password” and repeat it.
 - Press [Esc] to exit this dialog.
- Press [Esc] to exit. Move to “Save Changes and exit” and press [Enter]. The boot will continue automatically.

3.3.4 OS Installation

This section describes the operating system installation. Immediately after powering the server, insert the re-installation DVD marked “Microsoft Windows Storage Server 2008 Standard with Service pack 2” and follow the instructions. Note that the root drive is split into two partitions (C and D) of approximately equal size.



3.3.5 Initial Configuration

After the OS installation, the NAS server must be configured to make the second partition of the root disk and the entire storage disk accessible from the processing servers and the operator workstation.

3.3.5.1 Storage Disk

If the storage disk is not formatted, log on as Administrator and follow these steps:

- Click on “Start”.
- Go to “Administrator Tools” and start “Server Manager”.
- Expand “Storage” in the left-hand panel and select “Disk Management”. You will be reminded to format the storage disk.
- Right-click on the box representing the storage drive and select “Create Simple Volume”.
- Enter the volume name when requested and use the default value for everything else.
- Finishing the wizard starts the formatting. A couple of hours are required to format a large drive.
- Once the drive is formatted, reboot the NAS server to make the storage drive information visible on the upper-right section of the desktop background.

3.3.5.2 Share Drives

The second partition of the root disc is drive D and is about 68 GB. The storage disk partition is drive F and is about 1.2 TB. The two drives need to be made sharable to enable remote access. If the drives are not already shared, follow these steps:

- Click on “Start”.
- Click on “Computer”.
- Click on drive D or F.
- Right-click on the drive and click “Share...”.
 - If the drive is already marked as shared, click “OK”. Otherwise
 - Otherwise, click “Advanced Sharing...”.
 - Click in the “Share this folder” box.
 - Replace the drive letter D or F with nas0 or nas1 respectively.
 - Click “Permissions”.
 - The group “Everyone” should already be selected.
 - Click on “Full Control” to enable. All the boxes under the “Allow” column should be selected.
 - Click OK to exit.
 - Click OK exit.
- Click “Close” to exit.

Next create folder “SEADAS” in the D and F drives. The NAS server is now ready for remote storage on the processing servers and the operator workstation.



3.3.6 Antivirus

To install Symantec Endpoint Protection Antivirus software for Windows follows these steps:

- Insert the DVD or USB Flash Drive labelled GI-MODIS.
- Copy Symantec_Endpoint_Protection_11.0.6A_Xplat_EN_DVD.zip in the folder /Symantec/Win32 to the desktop.
- Double-click on the Symantec Endpoint Protection ZIP icon.
- A window appears. Click Extract in this window.
- Select "Endpoint Client" and follow the instructions.
- Reboot once the installation is complete.

3.3.7 Windows Update on Demand

By default, the Windows updates are downloaded and installed automatically. Follow the steps below to change the setting to an “on demand” installation:

- Open the “Control Panel” in the Start menu.
- Double-click on the “Windows Update” icon.
 - Click “Change Settings”
 - Under “Important Updates”, select “Download updates but let me choose whether to install them”.
 - Click OK.



3.4 Operator Workstation

3.4.1 Connections

Before starting the OS installation, verify that the following connections are present:

- Keyboard and Mouse to workstation.
- DP to DVI cables from video card to both monitors.
- USB Dongle
- Built-in 1Gbit NIC 1 connected to the network switch

3.4.2 RAID Controller Configuration

The workstation does not have a RAID controller. Instead, the workstation has two 250 GB drives, which have been configured as one partition to maximize the space available for the local products.

3.4.3 Remote Management Port Configuration

The workstation does not have a remote management port. However, it is best suited for remote management of the ingest server, the processing servers, and the NAS server.

3.4.4 OS Installation

This section describes the operating system installation on the operator workstation. Immediately after powering the workstation, insert the DVD marked “Red Hat Enterprise Linux 6.4 (64-bit) Installation Disc”. After the hardware has been initialized, a *Welcome to RHEL 6.7* screen appears. Select *Install or Upgrade an Existing System* and press [Enter]. At the next screen, select *Skip* to skip the testing of the DVD and press [Enter]. Wait approximately 60 seconds for the *RHEL 6* screen to appear and click *Next*, in the lower right corner of the screen, to proceed with the installation steps shown below along with the defaults:

Steps	Default
• Language	English
• Keyboard	U.S. English
• Devices	Select <i>Basic Storage Devices</i>
• Installation	Select <i>Fresh Installation</i>
• Hostname & Network	Enter the hostname
	Click <i>Configure Network</i>
	Highlight <i>em1</i> and click <i>Edit</i>
	Select <i>Connect automatically</i>
	Select <i>IPv4 Settings</i>
	Select <i>Manual</i> as the Method:
	Click <i>Add</i> .
	Enter IP address. Press [Tab]
	Enter Netmask. Press [Tab]
	Enter Gateway. Press [Tab]
	Enter DNS server(s)
	Click <i>Apply</i>
	Click <i>Close</i>



- Time Zone *Click Next*
Select time zone for your location. *Click Next.*
- Root Password Enter and confirm the root password. *Click Next.*
- Partitioning Select *Replace Existing Linux System(s)*
Click *Review and modify partitioning layout*
Click *Next.*
The Partitions Menu appears.
Modify as desired. *Click Next* when done.
Click *Write changes to disk* if requested.
(It will take several minutes to format the drive)
- Boot Loader Use the defaults. *Click Next.*
- Software Select *Software Development W/S* and click *Next.*
(It will take several minutes to install the RPMs)

Click *Reboot* to reboot the machine once the installation is finished.

3.4.5 Initial Configuration

An initial configuration menu appears on the first boot after the OS has been installed. Click *Forward* to proceed with the steps necessary to make your system ready to use:

- License Information Agree and click *Forward*
- Set Up Software Updates Select *No, I prefer to register at a later time.*
Click *Forward*
- Create User Click *Forward*. This step can be done at a later time
- Date and Time Click *Synchronize date and time over the network*
Remove current NTS entries.
Add local NTS IP address.
Click *Advanced Options*
Select *Speed up initial synchronization*
Click *Forward*
- Kernel Dump Use defaults or define as desired. Click *Finish.*
Click *Yes* to use these settings.
Click *OK* to reboot.

Once the machine has booted, log in as user root at the console login screen. The GNOME Environment appears. Next, move the cursor on the background, press the right-mouse button to display the menu, move to “Open Terminal” and release the button. A terminal window appears. Enter the following command to register this machine for Red Hat Updates:

```
subscription-manager register --username <u> --password <p> --auto-attach
```

where <u> and <p> are the user name and password respectively of your Red Hat account.

The server is now ready for the System 9000 software installation and configuration.



3.4.6 Antivirus

To install the Symantec antivirus software on Linux, log in as user root at the server or workstation console.

- Insert the DVD or USB Flash Drive labelled GI-MODIS.
- If a DVD or USB icon does not appear, double-click on the Computer icon and double-click on the DVD or USB icon.
- With the cursor on the background, press the right-mouse button, move to “Open Terminal” and release the button. A terminal window appears. The commands are entered in this window.
- In this terminal window, type the command ‘df -h’ to find the name under which the DVD installation media has been mounted: /media/<device>. Replace <device> with the appropriate value whenever it is mentioned in this document.

- Execute the following commands:

```
cd /root
export SAV_DIR=/media/<device>/Symantec/Linux
cp $SAV_DIR/sav*.bash /root
chmod 744 sav*.bash
./sav-install.bash $SAV_DIR/sav-linux-1.0.9-13.tgz
umount /media/<device>
```

- Disable the auto protection (to keep performance up):

(lines beginning with # are comments, lines in *Italic* are the program responses)

```
# Check status
/opt/Symantec/symantec_antivirus/sav info -a
Enabled #--> Auto Protect is Enabled

# Disable Auto Protect
/opt/Symantec/symantec_antivirus/sav autoprotect -d
/opt/Symantec/symantec_antivirus/sav info -a
Disabled # --> Auto Protection is disabled
```

- Check definition update time:

```
# Check Update of Virus Definitions Download
/opt/Symantec/symantec_antivirus/sav liveupdate -v
Frequency: Weekly - Fri at 20:00
Missed Events: Enabled
State: Enabled
```

- Manual Scanning:

```
# Manual Scanning
# /opt/Symantec/symantec_antivirus/sav manualscan -s <directory>
# --> Reports no info to terminal, check
/var/symantec/Logs/<date>.log
# It is up to each site to come up with a schedule to
# perform the manual scans on a routine basis.
```



- Running Daemons:

```
# Daemons: symcfgd and rtvscand services  
# Both are running by default.  
# REQUIRED FOR MANUAL SCAN!  
# rtvscand is actually the scan engine.
```



4 System 9000 Installation and Configuration

This section describes the installation and configuration of the System 9000 software on the various computers of the ESC system. The computers are delivered with the System 9000 software already installed and configured. Therefore, you may skip to the section labelled “On-site Configuration and Verification”.

The ESC has three computer systems running the System 9000 software:

- Ingest Server performing the MODIS tracking and ingestion.
- Primary/Backup Processing Servers performing the automatic MODIS processing.
- Operator Workstation performing the manual processing as well as control and monitoring operations.

The System 9000 software contains the necessary programs to track the MODIS satellites, TERRA and AQUA, to ingest the MODIS telemetry and to perform the SeaDAS MODIS processing. System 9000 is delivered on two DVDs labelled GI-MODIS (SeaDAS 6.4) and GI-MODIS (SeaDAS 7.3) respectively. Either DVD can be used to install System 9000 on the ingest server. Both DVDs are needed to Install System 9000, SeaDAS 6.4, and SeaDAS 7.3 on the operator workstation and the processing servers.

Once a computer has booted, a login screen appears on the console. In the case of the processing servers, you will need to select the processing server from the KVM console. Press [Ctrl] twice to show the KVM menu. In this menu, select the server you wish to view and press [Enter].

The following sections describe the installation on the three computer systems: Ingest Server, Processing Servers, and Operator Workstation. Enter ‘root’ to log in as user root. The System 9000 installation and configuration are done as user root.

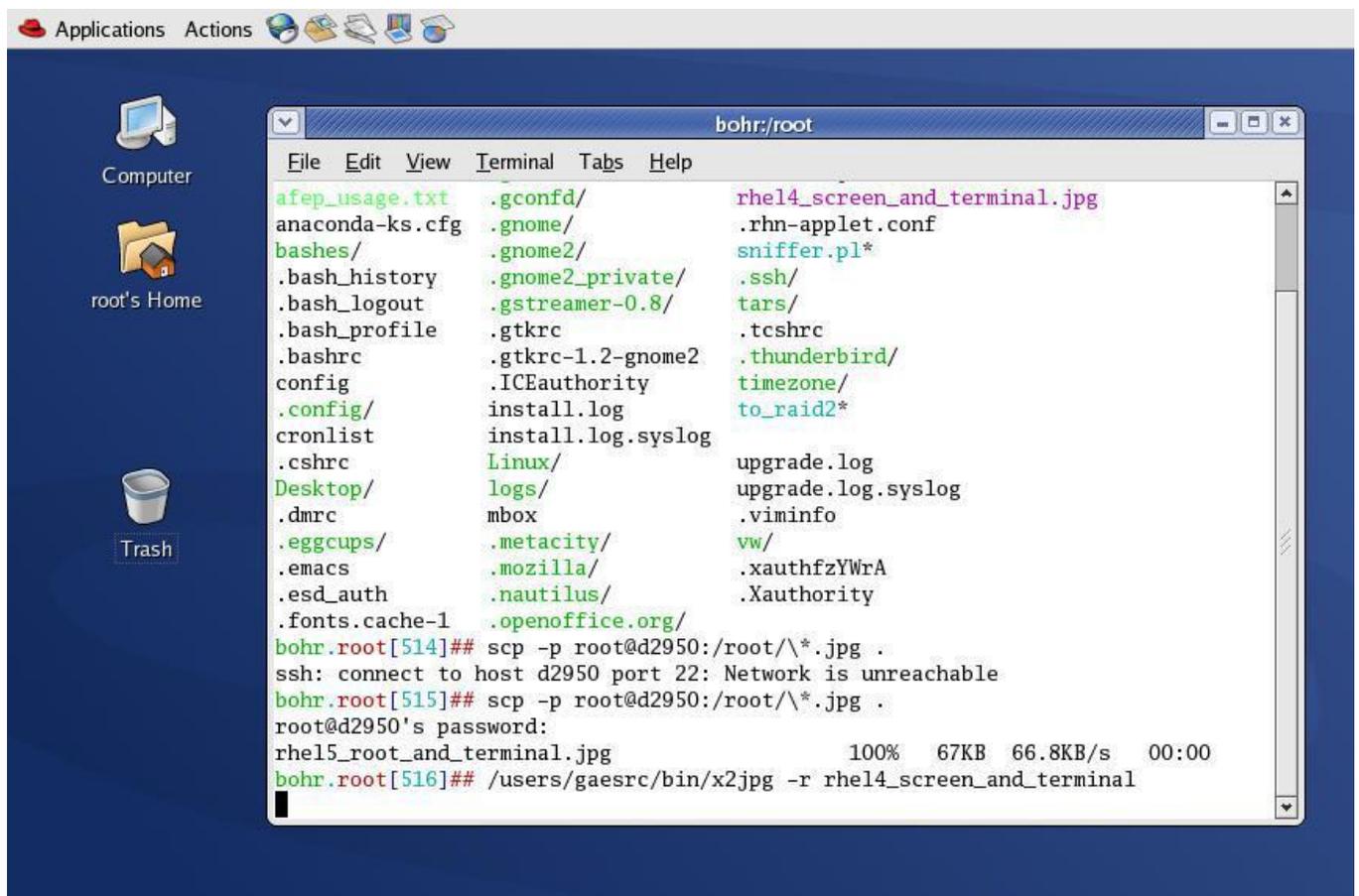


4.1 Ingest Server

4.1.1 Installation

This section describes the installation of the software on the ingest server. The ingestion is performed by user modis. An additional user named gae, containing generic tools and databases, is also installed. User gae does the automatic daily update of the orbital elements. Note that the software requires a USB license dongle. A red LED on the dongle identifies an active license dongle.

The installation begins with a log in as user root at the console login screen. The GNOME Environment appears. Next, move the cursor on the background, press the right-mouse button, move to “Open Terminal” and release the button. A terminal window appears. The commands will be entered in this window.



To install System 9000, follow these steps:

- Insert the DVD labelled GI-MODIS (SeaDAS 6.4).
- If a DVD icon does not appear, double-click on the Computer icon and double-click on the DVD.
- In the terminal window, type the command ‘df -h’ to find the name under which the DVD installation media has been mounted: /media/<device>. Replace <device> with the



appropriate value whenever it is mentioned in this document.

- Execute the following commands:

```
cp /media/<device>/Install_S9000 /tmp
cd /tmp

./Install_S9000 -d /media/<device> -system
./Install_S9000 -d /media/<device> -ingest modis
umount /media/<device>
```

The first Install_S9000 command performs the following steps:

- Install the GNU configuration files.
- Update /root/.bashrc and /root/.emacs.
- Install additional RPMs (64-bit Linux only).

The second Install_S9000 command performs the following steps:

- Create user gae and install its software.
- Create user satops and install its software.
- Create user modis and install its software.
- Install the license files.
- Install patches if delivered with installation media.
- Configure user gae (Section 4.1.2.1).
Enter 'y' when the following is requested.
Run /users/gae/GAE_setup to configure? (y or n):
- Skip user satops configuration.
Enter 'n' when the following is requested.
Run /users/satops/SATOP_setup to configure? (y or n):
- Configure user modis (Section 4.1.2.2).
Enter 'y' when the following is requested.
Run /users/gae/SETUP/ingest_user to configure? (y or n):

4.1.2 Configuration

The software configuration is done in three parts: Generic, telemetry-specific, and site-specific. The generic and telemetry-specific parts are described below. Once you are done, refer to Section 5 for the site-specific configuration.

4.1.2.1 *Generic*

The generic configuration is done with the script /users/gae/GAE_setup called by the installation script and consists of the following steps:

- Install the resource files for the various X programs in /usr/lib/X11/app-defaults.
- Create a generic C-shell login source file /users/gae/.gaelogin.
- Set-up the Orbital Elements download and update:
 - Enter 'nasa', 'celestrak', or 'gi' to download the orbital elements from NASA, Celestrak, or Global Imaging respectively. Use 'nasa' if ingesting or processing the MODIS satellites.



- Enter the hour and minute at which the daily orbital elements download and update will occur. A cron job for user gae will be set. Use the command ‘crontab –u gae –l’ to view the job.
 - Start the storage-directory cycling program (sd_cycle).
 - For RHEL 4/5, the entry ‘sdcy’ is added to the file /etc/inittab to launch sd_cycle at boot time and respawn it when terminated.
 - For RHEL 6, the file sdcy.conf is added to the folder /etc/init to launch sd_cycle at boot time and respawn it when terminated.
 - Enter “y” when asked if there are GSI units attached to this machine to create the GSI device file and set the device permissions.
 - For RHEL 4/5
 - Add the entry sdvp to the file /etc/inittab to execute the script set_dev_perm once at boot time to create the device names
 - Add the entry sdip to the file /etc/inittab to execute the script set_dev_perm at regular interval to set the permissions.
 - For RHEL 6
 - Add the file sdvp.conf to the folder /etc/init to execute the script set_dev_perm once at boot time to create the device names
 - Add the file sdip.conf to the folder /etc/init to execute the script set_dev_perm at regular interval to set the permissions.
- The script set_dev_perm generates the proper ingest device names and sets the permissions for various devices: USB-to-Serial device, Stream Tape device, etc.
- Install the software package for the USB license dongle.
 - There is no Serial GPS delivered with this system. Enter ‘n’ when requested.

4.1.2.2 Telemetry-Specific

The telemetry-specific configuration is done with the command

```
/users/gae/SETUP/ingest_user modis
```

called by the installation script and consists of the following steps:

- Enter “modis” when requested which user is doing the tracking.
 - Enter “y” when requested to confirm user modis is doing the tracking.
- Enter “y” when requested to configure the antenna/downlink database:
 - Check/Set the antenna location:
 - Enter the antenna latitude.
 - Enter the antenna longitude.
 - Enter the antenna elevation.
 - The new values are displayed. Enter ‘y’ if they are correct. If not, enter ‘n’ to repeat the process.
 - Check/Set the ingest, receiver, and controller device:
 - Enter the ingest device name.
 - Enter the type of receiver interface.
 - Enter the receiver device name.
 - Enter the controller device name.
 - The new values are displayed. Enter ‘y’ if they are correct. If not, enter ‘n’ to repeat



the process.

- Check/Set the HOME AZ/EL offset and motors:
 - The factory values for these parameters are listed in a pre-configuration sheet delivered with the system.
 - Enter the elevation HOME offset and motor type.
 - Enter the azimuth HOME offset and motor type.
 - The new values are displayed. Enter 'y' if they are correct. If not, enter 'n' to repeat the process.
- The antenna/downlink database file is updated to reflect the new values.
- Install STracker+ software on user modis:
 - Install the JAVA version used by STracker.
 - Ignore the comments concerning the Serial GPS.
 - Set the default area of interest used by the tracking program.

This step requires 'vi' editing experience.
- Set VNC password.
- Add user modis to group uucp to get read and write access to USB devices.
- Automatic start of IVS VNC server (command 'vnc-ivs -start')
 - For RHEL 4/5, add the entry xv24 to the file /etc/inittab to execute the script vnc-ivs once.
 - For RHEL 6, add the file xv24.conf to the folder /etc/init to execute the script vnc-ivs once.
- When requested, enter 'y' to configure the MODIS level 0 data distribution (script 10_dist):
 - Transfer mode:
 - Enter 'ftp' or 'scp' for the transfer mode. If you enter FTP, the VSFTP daemon must be installed on the destination computers. If you enter SCP, password-less access for user modis on the ingest server to the user on the destination machines must be set-up. Refer to Appendix B for details on password-less access.
 - Distribution options:
 - Enter 'either' or 'both' for the distribution mode. Use 'either' if the second destination is a backup processor.
 - Enter 'oldest' or 'newest' for the distribution order. Use 'oldest' as distribution order to ensure proper temporal processing.
 - Enter 'terra', 'aqua', or 'none' for priority. Use 'none' as priority to ensure proper temporal processing.
 - First remote destination:
 - IP address or hostname. Enter 'ps1', which should be an alias in the hosts table for the primary processor.
 - User name. Enter 'seadas' to send the data to the user doing the SeaDAS MODIS processing.
 - Password. Note that the metacharacters must be escaped. Needed only with FTP transfer mode.
 - Destination path. Enter '/users/seadas/level0'.
 - Second remote destination:
 - Enter 'y' when requested to add a second destination.
 - IP address or hostname. Enter 'ps2', which should be an alias in the hosts table for



- the secondary or backup processor.
- User name. Enter 'seadas' to send the data to the user doing the SeaDAS MODIS processing.
- Password. Note that the metacharacters must be escaped. Needed only with FTP transfer mode.
- Destination path. Enter '/users/seadas/level0'.
- The script l0_dist is updated to reflect the new values.
- Start MODIS L0 Distribution (script l0_dist)
 - For RHEL 4/5, add entry l0dd the file /etc/inittab to start l0_dist at boot time and respawn it when terminated.
 - For RHEL 6, add l0dd.conf to the folder /etc/init to start l0_dist at boot time and respawn it when terminated.
- Enter "y" when requested to log in as user modis to test the log in sequence. Type 'exit' to exit the log in.

Next, refer to Section 5 for site-specific configuration.



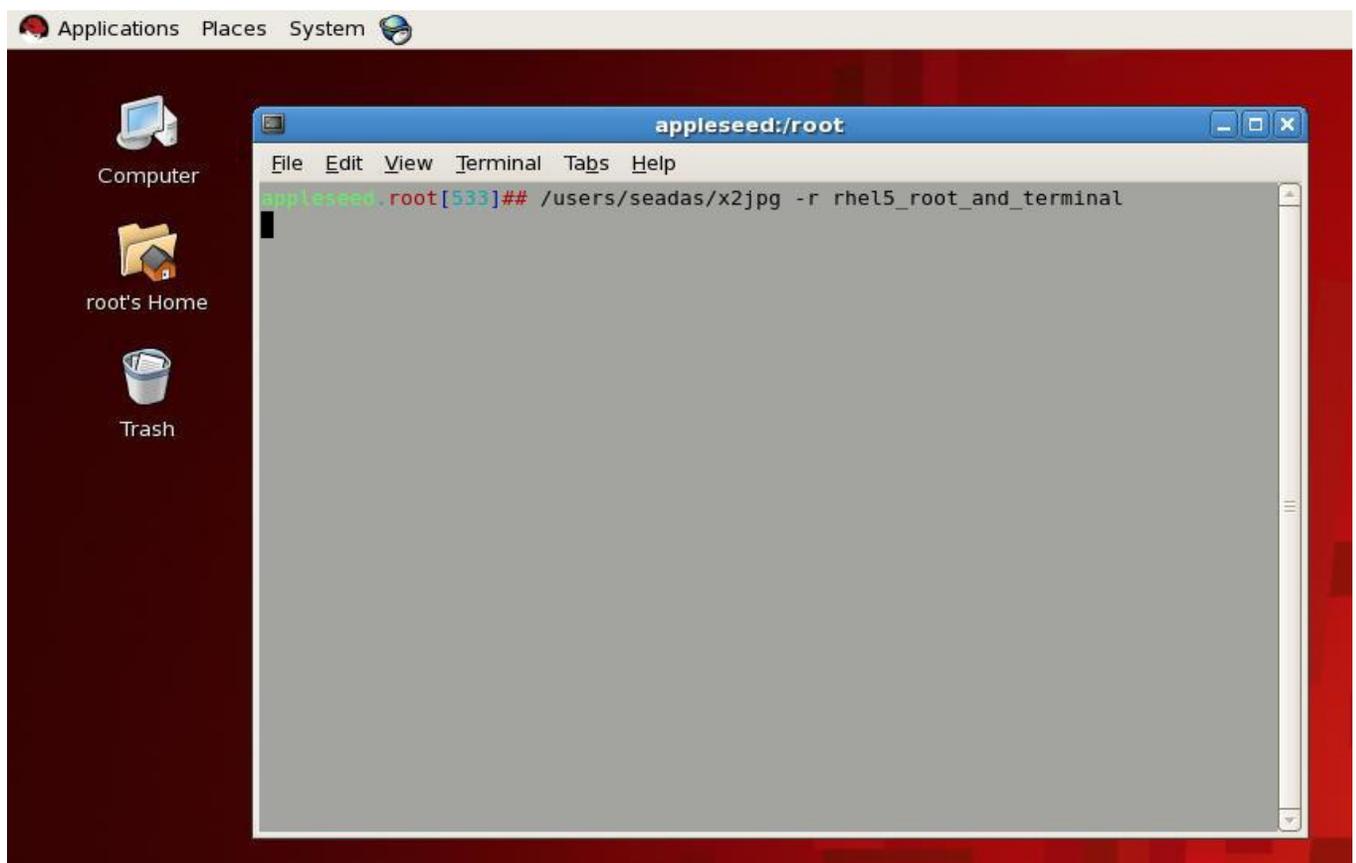
4.2 Processing Servers

The software installation assumes that the NAS server is running and has been properly configured to remotely mount its storage drives.

4.2.1 Installation

This section describes the installation of the software on the processing servers. The processing is performed by user seadas. An additional user named gae, containing generic tools and databases, is also installed. User gae does the automatic daily update of the orbital elements. Note that the software requires a USB license dongle. A red LED on the dongle identifies an active license dongle.

The installation begins with a log in as user root at the console login screen. The GNOME Environment appears. Next, move the cursor on the background, press the right-mouse button, move to “Open Terminal” and release the button. A terminal window appears. The commands will be entered in this window.



To install System 9000 and SeaDAS 6.4, follow these steps:

- Insert the DVD labelled GI-MODIS (SeaDAS 6.4).
- If a DVD icon does not appear, double-click on the Computer icon and double-click on the DVD icon.



- With the cursor on the background, press the right-mouse button, move to “Open Terminal” and release the button. A terminal window appears. The commands are entered in this window.
- In this terminal window, type the command ‘df -h’ to find the name under which the DVD installation media has been mounted: /media/<device>. Replace <device> with the appropriate value whenever it is mentioned in this document.
- Execute the following commands:

```
cp /media/<device>/Install_S9000 /tmp
cd /tmp

./Install_S9000 -d /media/<device> -system
./Install_S9000 -d /media/<device> -process SeaDAS
umount /media/<device>
```

The first Install_S9000 command performs the following steps:

- Install the GNU configuration files.
- Update /root/.bashrc and /root/.emacs.
- Install additional RPMs (64-bit Linux only).

The second Install_S9000 command performs the following steps:

- Create user gae and install its software.
- Create user seadas and install its software.
- Copy the license files to /users/gae/product.
- Install patches if delivered with installation media.
- Configure user gae (Section 4.2.2.1).
Enter ‘y’ when the following is requested.
Run /users/gae/GAE_setup to configure? (y or n):
- Configure user gae (Section 4.2.2.2).
Enter ‘y’ when the following is requested.
Run /users/seadas/SEADAS_setup to configure? (y or n):
- Install NASA SeaDAS 6.4 software.

To install SeaDAS 7.3, follow these steps:

- Insert the DVD labelled GI-MODIS (SeaDAS 7.3).
- If a DVD icon does not appear, double-click on the Computer icon and double-click on the DVD.
- With the cursor on the background, press the right-mouse button, move to “Open Terminal” and release the button. A terminal window appears. The commands are entered in this window.
- In this terminal window, type the command ‘df -h’ to find the name under which the DVD installation media has been mounted: /media/<device>. Replace <device> with the appropriate value whenever it is mentioned in this document.



- Execute the following commands:

```
cp /media/<device>/Install_S9000 /tmp
cd /tmp

./Install_S9000 -d /media/<device> -process SeaDAS

umount /media/<device>
```

The Install_S9000 command performs the following steps:

- Skip user gae installation.
Enter 'n' when the following is requested.
User gae exists. Continue with user installation? (y or n)
- Skip user seadas installation.
Enter 'n' when the following is requested.
User seadas exists. Continue with user installation? (y or n)
- Copy the license files to /users/gae/product.
- Install patches if delivered with installation media.
- Skip user gae configuration.
Enter 'n' when the following is requested.
Run /users/gae/GAE_setup to configure? (y or n):
- Skip user seadas configuration.
Enter 'n' when the following is requested.
Run /users/seadas/SEADAS_setup to configure? (y or n):
- Install NASA SeaDAS 7.3 software.

4.2.2 Configuration

The software configuration is done in three parts: Generic, processing-specific, and site-specific. The generic and processing-specific parts are described below. Once you are done, refer to Section 5 for the site-specific configuration.

4.2.2.1 Generic

The generic-specific configuration is done with the script /users/gae/GAE_setup called by the installation script and consists of the following steps:

- Install the resource files for the various X programs in /usr/lib/X11/app-defaults.
- Create a generic C-shell login source file /users/gae/.gaelogin.
- Set-up the Orbital Elements download and update:
 - Enter 'nasa', 'celestrak', or 'gi' to download the orbital elements from NASA, Celestrak, or Global Imaging respectively. Use 'nasa' if ingesting or processing the MODIS satellites.
 - Enter the hour and minute at which the daily orbital elements download and update will occur. A cron job for user gae will be set. Use the command 'crontab -u gae -l' to view the job.
- Start the storage-directory cycling program (sd_cycle).
 - For RHEL 4/5, the entry 'sdcy' is added to the file /etc/inittab to launch sd_cycle at boot time and respawn it when terminated.



- For RHEL 6, the file `sdcy.conf` is added to the folder `/etc/init` to launch `sd_cycle` at boot time and respawn it when terminated.
- Enter “n” when asked if there are GSI units attached to this machine.
- Install the software package for the USB license dongle.
- There is no Serial GPS delivered with this system. Enter ‘n’ when requested.

4.2.2.2 *Processing-Specific*

The processing-specific configuration is done with the script `/users/seadas/SEADAS_setup` called by the installation script and consists of the following steps:

- Disable the tty requirement for sudo in `/etc/sudoers`.
- Enter ‘y’ when asked if this is a processing server because the processing server does perform the automatic processing.
 - Start the Very Secure FTP daemon (`vsftpd`).
 - Move the launch icons from `/users/seadas/Desktop` to `/users/seadas/Desktop_Saved`.
 - Automatic SeaDAS MODIS processing in background (`auto_proc`)
 - For RHEL 4/5, add entry `auto` to the file `/etc/inittab` to start the script `auto_proc` at boot time and respawn it when terminated.
 - For RHEL 6, add the file `asmp.conf` to the folder `/etc/init` to start the script `auto_proc` at boot time and respawn it when terminated.
- Install and setup the X11 `XVFB` package.
- If an LTO tape storage device is connected to the machine, add a command to `/etc/rc.local` to set the permissions for the device (`/dev/st0`).
- Inform the user about global storage via NFS.

Next, refer to Section 5 for site-specific configuration.



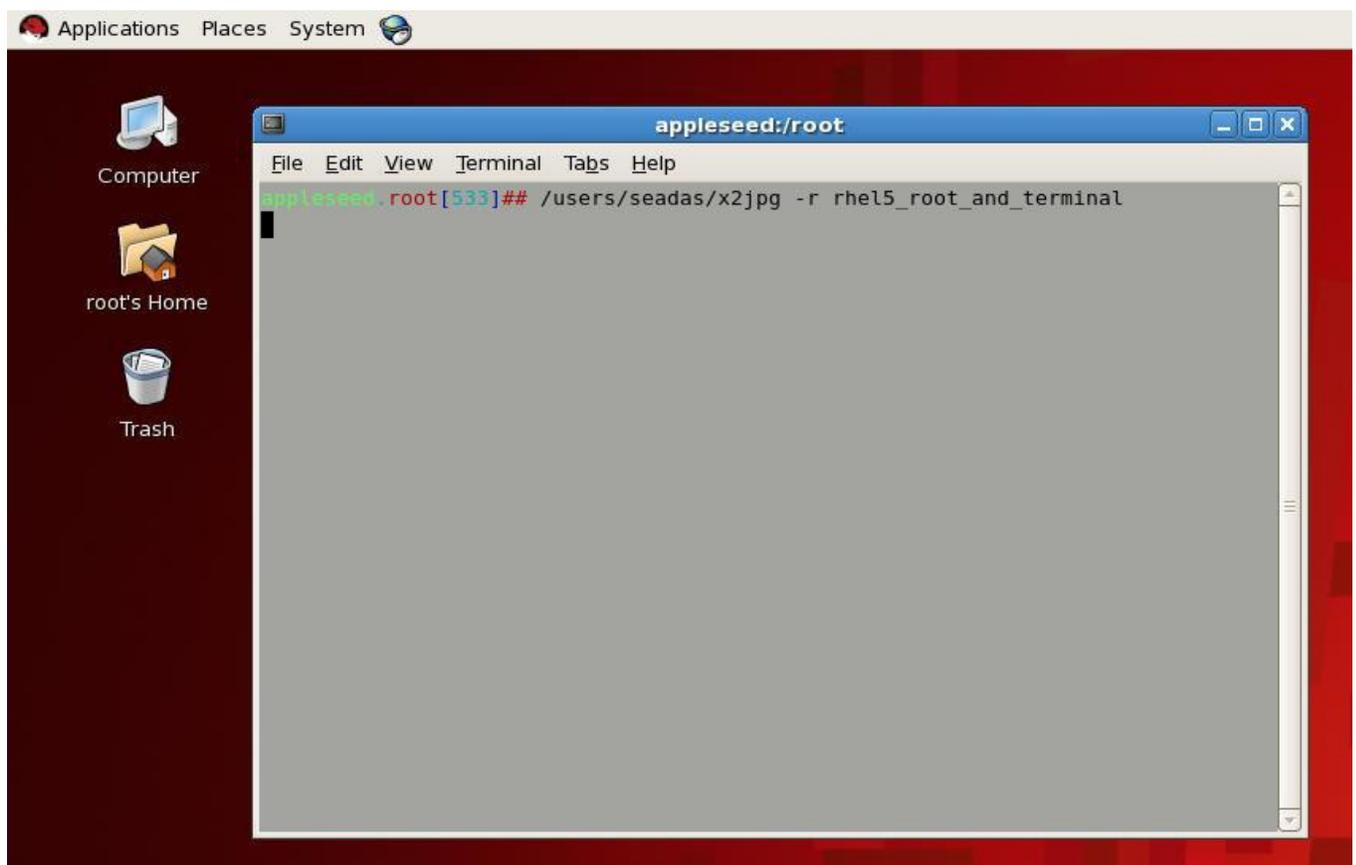
4.3 Operator Workstation

The software installation assumes that the NAS server is running and has been properly configured to remotely mount its storage drives.

4.3.1 Installation

This section describes the installation of the software on the processing servers. The processing is performed by user seadas. An additional user named gae, containing generic tools and databases, is also installed. User gae does the automatic daily update of the orbital elements. Note that the software requires a USB license dongle. A red LED on the dongle identifies an active license dongle.

The installation begins with a log in as user root at the console login screen. The GNOME Environment appears. Next, move the cursor on the background, press the right-mouse button, move to “Open Terminal” and release the button. A terminal window appears. The commands will be entered in this window.



To install System 9000 and SeaDAS 6.4, follow these steps:

- Insert the DVD labelled GI-MODIS (SeaDAS 6.4).
- If a DVD icon does not appear, double-click on the Computer icon and double-click on the DVD icon.



- With the cursor on the background, press the right-mouse button, move to “Open Terminal” and release the button. A terminal window appears. The commands are entered in this window.
- In this terminal window, type the command ‘df -h’ to find the name under which the DVD installation media has been mounted: /media/<device>. Replace <device> with the appropriate value whenever it is mentioned in this document.
- Execute the following commands:

```
cp /media/<device>/Install_S9000 /tmp
cd /tmp

./Install_S9000 -d /media/<device> -system
./Install_S9000 -d /media/<device> -process SeaDAS
umount /media/<device>
```

The first Install_S9000 command performs the following steps:

- Install the GNU configuration files.
- Update /root/.bashrc and /root/.emacs.
- Install additional RPMs (64-bit Linux only).

The second Install_S9000 command performs the following steps:

- Create user gae and install its software.
- Create user seadas and install its software.
- Copy the license files to /users/gae/product.
- Install patches if delivered with installation media.
- Configure user gae (Section 4.3.2.1).
Enter ‘y’ when the following is requested.
Run /users/gae/GAE_setup to configure? (y or n):
- Configure user gae (Section 4.3.2.2).
Enter ‘y’ when the following is requested.
Run /users/seadas/SEADAS_setup to configure? (y or n):
- Install NASA SeaDAS 6.4 software.

To install SeaDAS 7.3, follow these steps:

- Insert the DVD labelled GI-MODIS (SeaDAS 7.3).
- If a DVD icon does not appear, double-click on the Computer icon and double-click on the DVD.
- With the cursor on the background, press the right-mouse button, move to “Open Terminal” and release the button. A terminal window appears. The commands are entered in this window.
- In this terminal window, type the command ‘df -h’ to find the name under which the DVD installation media has been mounted: /media/<device>. Replace <device> with the appropriate value whenever it is mentioned in this document.



- Execute the following commands:

```
cp /media/<device>/Install_S9000 /tmp
cd /tmp

./Install_S9000 -d /media/<device> -process SeaDAS

umount /media/<device>
```

The Install_S9000 command performs the following steps:

- Skip user gae installation.
Enter 'n' when the following is requested.
User gae exists. Continue with user installation? (y or n)
- Skip user seadas installation.
Enter 'n' when the following is requested.
User seadas exists. Continue with user installation? (y or n)
- Copy the license files to /users/gae/product.
- Install patches if delivered with installation media.
- Skip user gae configuration.
Enter 'n' when the following is requested.
Run /users/gae/GAE_setup to configure? (y or n):
- Skip user seadas configuration.
Enter 'n' when the following is requested.
Run /users/seadas/SEADAS_setup to configure? (y or n):
- Install NASA SeaDAS 7.3 software.

4.3.2 Configuration

The software configuration is done in three parts: Generic, processing-specific, and site-specific. The generic and processing-specific parts are described below. Once you are done, refer to Section 5 for the site-specific configuration.

4.3.2.1 Generic

The generic-specific configuration is done with the script /users/gae/GAE_setup called by the installation script and consists of the following steps:

- Install the resource files for the various X programs in /usr/lib/X11/app-defaults.
- Create a generic C-shell login source file /users/gae/.gaelogin.
- Set-up the Orbital Elements download and update:
 - Enter 'nasa', 'celestrak', or 'gi' to download the orbital elements from NASA, Celestrak, or Global Imaging respectively. Use 'nasa' if ingesting or processing the MODIS satellites
 - Enter the hour and minute at which the daily orbital elements download and update will occur. A cron job for user gae will be set. Use the command 'crontab -u gae -l' to view the job.
- Start the storage-directory cycling program (sd_cycle).
 - For RHEL 4/5, the entry 'sdcy' is added to the file /etc/inittab to launch sd_cycle at boot time and respawn it when terminated.



- For RHEL 6, the file `sdcy.conf` is added to the folder `/etc/init` to launch `sd_cycle` at boot time and respawn it when terminated.
- Enter “n” when asked if there are GSI units attached to this machine.
- Install the software package for the USB license dongle.
- There is no Serial GPS delivered with this system. Enter ‘n’ when requested.

4.3.2.2 Processing-Specific

The processing-specific configuration is done with the script `/users/seadas/SEADAS_setup` called by the installation script and consists of the following steps:

- Disable the tty requirement for sudo in `/etc/sudoers`.
- Enter ‘n’ when asked if this is a processing server because the operator workstation does not perform the automatic processing.
- Add the automatic system alert script `sds_ops_system_alert` as a cron job of user `seadas`. The script will run every 5 minutes to alert the operator of system problems.
- If an LTO tape storage device is connected to the machine, add a command to `/etc/rc.local` to set the permissions for the device (`/dev/st0`).
- Inform the user about global storage via NFS.

Next, refer to Section 5 for site-specific configuration.



5 On-site Configuration and Verification

The system is delivered with pre-configured computers. However, site-specific configuration such as network parameters, hosts table, and NTS parameters may be required. Once the site-specific configuration is complete, each computer should be verified before the automatic processes are enabled. Some of these tasks require editing ASCII (text) files. The instructions mention the vi editor, but you can use any other text editor.

The following sections describe the on-site configuration and verification of the ESC system:

- NTS/GPS unit
- NAS server
- Processing servers and operator workstation
- Ingest server
- Processing servers
- Operator workstation

5.1 NTS/GPS Unit

This section assumes that the NTS-150 is connected to the network switch and that the GPS antenna is on the roof and is also connected to the unit.

5.1.1 Network Parameters

The NTS-150 network parameters can be configured via a telnet connection or the serial port of the NTS-150 unit. The system has been delivered pre-configured. It may be possible to telnet to the NTS-150 with the command 'telnet nts' on the ingest workstation. Log in as user operator with password mercury. Display the current network setting by entering:

```
F100 ic
```

Set the new network settings by entering the following string with the appropriate values inserted:

```
F100 IP:<NTS-IP-Address> SM:<Subnet-Mask> G:<Default-Gateway>
```

Enter "y" when prompted. The unit will reboot with the network settings. Once you have set the network parameters for the ingest server, try to connect to the NTS-150 again.

If you cannot telnet to the NTS-150, connect a portable PC, running Windows-XP, to the serial port of the unit with the null modem cable provided with the unit. Use the Hyper Link program to connect to the NTS unit. If you are not running Windows-XP, simply find this program or a similar communication program. Set your communication program to: 9600, 8, N, 1. Log in as user operator and password mercury. Display the current network setting by entering:

```
F100 ic
```

Set the new network settings by entering the following string with the appropriate values inserted:

```
F100 IP:<NTS-IP-Address> SM:<Subnet-Mask> G:<Default-Gateway>
```

Enter "y" when prompted. The unit will reboot with the network settings. Disconnect the computer, and cycle the power on the NTS-150 unit to ensure a 100-Mbps connection.



- Click “Synchronize with an Internet Server”, if not selected.
- Select the IP address in the list of time servers.
- Replace with the NTS-150 IP address.
- Click “Update Now”. Wait for an answer.
- Click “OK”.
- Click “OK”.

5.2.3 User Administrator Password

To modify the user Administrator password, follow these steps:

- Click “Start”.
- Click “Control Panel”.
- Double-click on the “User Accounts” icon.
- Click on “Internet Time” tab.
- Click on “Change your password”.
 - Enter old password.
 - Enter new password.
 - Confirm the new password.
 - Click “Change Password”.

If you modify the password for user Administrator on the NAS you will need to replace the old password with the new password in the file /etc/fstab of the processing servers (Section 5.3.7) and the operator workstation (Section 5.4.7).

5.2.4 Remote Management

To change the Remote Management network parameters and password on a server, reboot the server. During the reboot process, wait for the message

```
iDRAC6 Configuration Utility 1.45
...
Press <Ctrl><E> for remote access setup within 5 seconds...
```

Once you have typed [Ctrl-E], the iDRAC Configuration Utility appears. Use the up and down arrow keys to move/highlight the desired item. Follow these steps:

- Move to "LAN Parameters" and press [Enter]. In this dialog:
 - Move to “IPV4 Address”. Move the first dotted octet of the IP address and set it. Repeat for the other octets.
 - Move the “Subnet mask” and set it.
 - Move to “Default Gateway” and set it.
 - Move to “DNS Server” and set it.
 - Press [Esc] to exit this dialog.
- Move to “LAN User Configuration” and press [Enter]. In this dialog:
 - Move to “Enter Password” and set it.
 - Move to “Confirm Password” and repeat it.



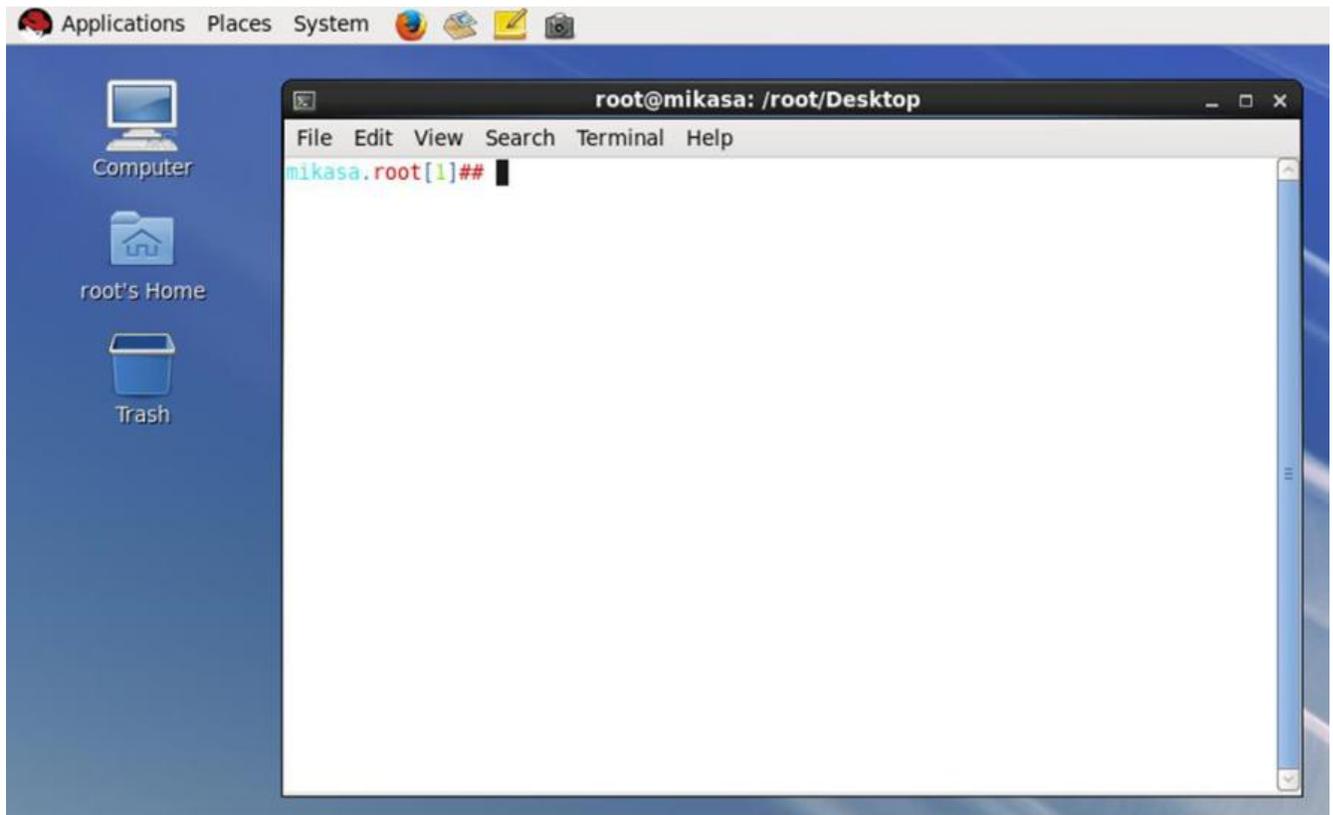
-
- Press [Esc] to exit this dialog.
 - Press [Esc] to exit. Move to “Save Changes and exit” and press [Enter]. The boot will continue automatically.

You can manage the server remotely from any Internet browser on any computer on the network with the URL <http://<iDRAC-IP-address>>. At the prompt, enter the iDRAC user name (Admin) and its password.



5.3 Processing Servers Configuration

This section describes the on-site configuration of each processing server running Red Hat Linux. The instructions in this section assume you are logged in as user root on the console of the server. If you are not user root on the console, log off by clicking the “Log Out” function under the “System” menu. In the dialog, click “Log Out” to log out. Enter ‘root’ at the prompt. The GNOME Environment appears. Next, move the cursor on the background, press the right-mouse button, move to “Open Terminal” and release the button. A terminal window appears. The commands will be entered in this window.

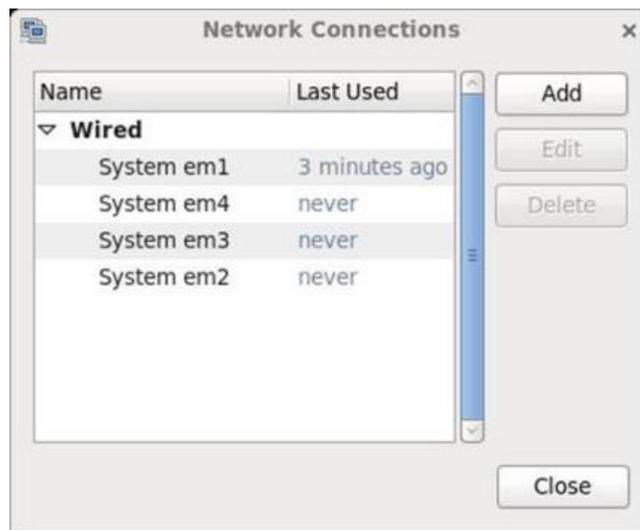


5.3.1 Network Parameters

Execute the command

```
/usr/bin/nm-connection-editor
```

to define the network parameters. The following dialog window appears:



Highlight “System em1” and click “Edit”. The following dialog appears:



Follow these steps:

- Select “Connect automatically”
- Select “Available to all users”
- Display the “IPv4 Settings” panel



- Select “Manual” for “Method”
- Set Address, Netmask, and Gateway
- Set DNS servers
- Select “Require IPv4 addressing for this connection to complete”
- If required, configure the routes
- Click “Apply” to save your changes and exit this dialog
- Click “Close” to close the “Network Connections” dialog.

Execute the following command for your changes to take effect:

```
service network force-reload
```

An easy way to check Internet access is to launch a Web browser and try a Web page.

5.3.2 Hosts Table

The ingest server has been delivered with a hosts table file, /etc/hosts, containing the IP address and a generic name for each host on the ESC system:

ins	ingest server
ps1	Primary processing server
ps2	Secondary or backup processing server
ows	Operator workstation
nas	Network Attached Storage Server. Note that the NAS also has the service tag as alias.
nts	Network Time Server (NTS/GPS unit)

These names are used in various scripts and launch programs to minimize the on-site configuration. You can add your own name, but we recommend you keep the names listed above as aliases. For example, replace the line

```
x.x.x.x <default-ingest-server-name> ins
```

with

```
y.y.y.y <your-ingest-server-name> ins
```

It is important to keep the alias representing the NAS server service tag. This alias allows mounting the NAS storage file systems. To edit /etc/hosts, log in as user root and execute the command ‘vi /etc/hosts’. Enter the correct IP addresses and add your choice of host names.

5.3.3 Clock Synchronization

The system has been delivered with a Network Time Server (NTS) unit equipped with a GPS antenna. Each server or workstation delivered with the system has been pre-configured to synchronize with this NTS unit. The unit IP address should be in the hosts table along with ‘nts’ as its host name or one of its aliases.

The Network Time Protocol (NTP) configuration file /etc/ntp.conf may contain a list of “pool” servers:

```
server 0.rhel.pool.ntp.org  
server 1.rhel.pool.ntp.org
```



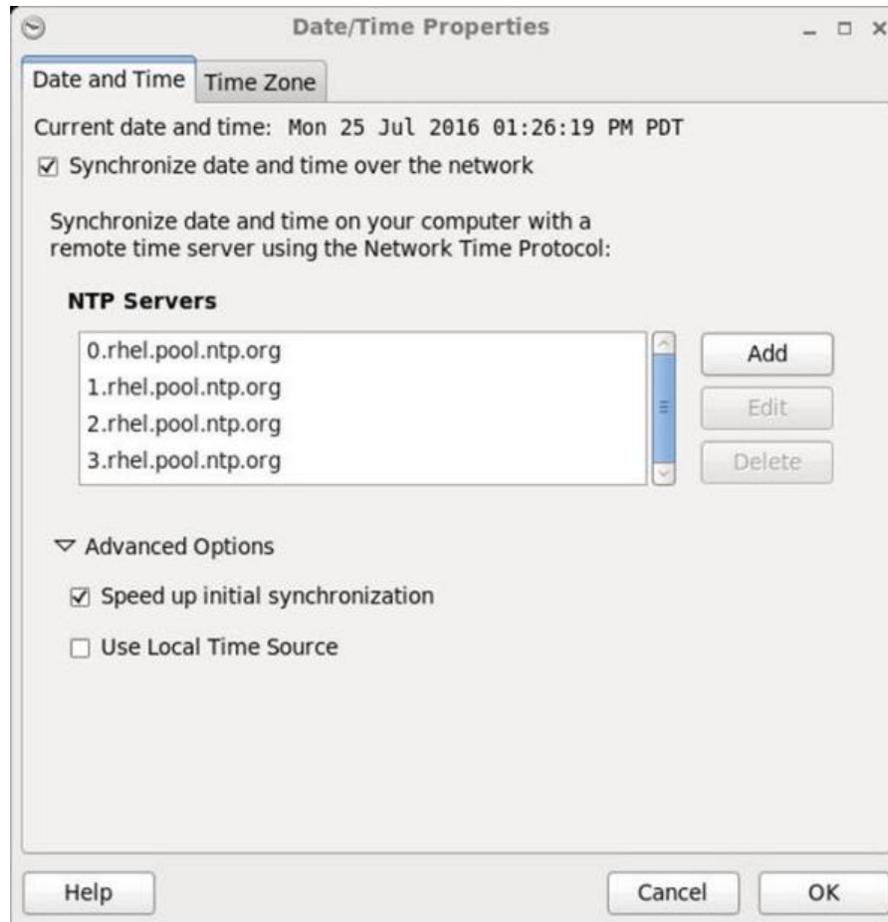
```
server 2.rhel.pool.ntp.org
```

It is recommended you edit this file and comment these lines unless you wish to join the NTP pool project at <http://www.pool.ntp.org/join.html>.

To verify that NTP is configured correctly, execute the command

```
/usr/bin/system-config-date
```

The following dialog appears:



Follow these steps:

- Display “Date and Time” panel
- Select “Synchronize date and time over the network”
- Remove the RHEL pool servers and add the server “nts” in the “NTP Servers” window.
- Extend “Advanced Options”
- Select “Speed up initial synchronization”
- Click OK to exit. The NTP service will start automatically.

The clock showing in the upper left corner of the screen should show the correct time.



5.3.4 Changing the Passwords

The ESC system has been delivered with pre-configured passwords. These passwords are listed in the pre-configuration sheet delivered with the system. To change the user passwords on a server or on the workstation, enter the command ‘passwd <user>’ where <user> is root, seadas, modis, or gae.

5.3.5 Password less SSH Access

The processing servers have been pre-configured to allow password less remote access to user seadas on each processor from various remote user and machines. This password less access is necessary for some operations of the system:

- Pop-up warning if failure to download the orbital elements.
- Execute commands from remote host without password request (in launch icons).
- System Alert such as computer failure, network failure, or NAS failure.

The table below lists the source users and machines that **need** password less access to the user seadas on each processing server

Source		Destination	
user1	host1	user2	host2
seadas	ows	seadas	ps1
seadas	ows	seadas	ps2
modis	ins	seadas	ps1
modis	ins	seadas	ps2

The file authorized_keys in \$HOME/.ssh of each destination user must have a DSA key from the source user/host. Note that this file may contain the keys for other source users/hosts. Some access is allowed only to facilitate remote command execution. Refer to Appendix B for details on setting password less SSH access.

5.3.6 Orbital Elements Download

To download the elements, execute the command

```
crontab -u gae -l
```

An entry containing the command get_oes is shown. Execute this command including its argument to download the orbital elements and test the Internet access. If downloading from NASA, execute the command

```
sudo -u gae /users/gae/oestools/get_oes nasa
```

The output should be as follows:

```
Working in /users/gae/oestools  
/usr/bin/wget ... ftp://169.154...  
drl.tle downloaded.  
/usr/bin/wget ... ftp://169.154...
```



```
norad.tle downloaded.  
cat drl.tle ... | /users/gae/oestools/nav2bbs > tle.txt.new  
mv tle.txt.new tle.txt  
/users/gae/oestools/tle2ole tle.txt
```

Once the elements can be downloaded, you may need to set a time at which the elements are downloaded every day. To verify the time at which the elements are downloaded, execute the command

```
crontab -u gae -l
```

An entry containing the command `get_oes` is shown. The first two columns indicate the minute and hour of day at which the command is executed. If you wish to modify it, execute the command

```
crontab -u gae -e
```

and set a new time.

Lastly, edit the script `/users/gae/oestools/get_oes` and replace the line ‘unset alert’ with ‘set alert’ to enable a pop-up window on the workstation in the event the orbital elements cannot be downloaded. The output of this cron job is mailed to user `gae` and resides in the file `/var/mail/gae`.

Note that user `gae` on the operator workstation must have password less access to user `seadas` on the operator workstation.

5.3.7 Mounting NAS Storage Drives

The processing servers and the operator workstation have been delivered with the NAS storage drives mounted as `/nas0` and `/nas1`. The file `/etc/fstab` contains two entries specifying the remote storage (`<remote-host>:<remote-drive>`), the mount directory (`/nas0` or `/nas1`) and the login parameters.

To verify the NAS drives are mounted, enter the command ‘`bdm`’ or ‘`df -h`’. If `/nas0` or `/nas1` do not appear, execute these tasks:

- Create the mount points:

```
mkdir /nas0 /nas1  
chmod 777 /nas0 /nas1
```
- Edit `/etc/fstab` and set the password for the `nas0` and `nas1` entries:

```
<remote-host>:nas0 /nas0 cifs username=Administrator,password=<password>  
<remote-host>:nas1 /nas1 cifs username=Administrator,password=<password>
```

where `<remote-host>` is the NAS hostname (usually `nas`) and `<password>` is the password of user `Administrator` on the NAS.
- Execute the command ‘`ping <remote-host>`’ to check the Internet connection. `<remote-host>` is the first component of each NAS entry in `/etc/fstab`.
- If there is no connection, check the network parameters of the machine you are logged into and the network parameters of the NAS server. Check the connections to the network switch. Repeat the step above.
- Execute the commands ‘`mount /nas0`’ and ‘`mount /nas1`’.
- If there is an error message, contact Global Imaging.
- Execute the command ‘`bdm`’ to verify that `/nas0` and `/nas1` are mounted.
- If they are not mounted, contact Global Imaging.



- Create a file in each filesystem

```
touch /nas0/SEADAS/dummy /nas1/SEADAS/dummy
rm /nas0/SEADAS/dummy /nas1/SEADAS/dummy
```
- If there is a problem creating the file, contact Global Imaging.

5.3.8 Automatic MODIS Processing

You can verify the start-up of the automatic SeaDAS MODIS processing with the command ‘ps -el | grep auto_proc’.

If you are running RHEL 5 and this command does not output anything, log in as user root (su -), verify that the execution mode of auto_proc in /etc/inittab is set to ‘respawn’. If it is not, set it, save your modifications, and execute ‘init Q’ for the modifications to take effect.

If you are running RHEL 6 and this command does not output anything, verify that asmp.conf is in the folder /etc/init. If it is not, execute the following command as root user

```
/users/gae/sbin/Upstart_load asmp
```

Check again with the command ‘ps -el | grep auto_proc’.

Refer to document RD-05 for details on the automatic MODIS processing.

5.3.9 Remote Management

To change the Remote Management network parameters and password on a server, reboot the server. During the reboot process, wait for the message

```
iDRAC6 Configuration Utility 1.45
```

```
...
```

```
Press <Ctrl><E> for remote access setup within 5 seconds...
```

Once you have typed [Ctrl-E], the iDRAC Configuration Utility appears. Use the up and down arrow keys to move/highlight the desired item. Follow these steps:

- Move to "LAN Parameters" and press [Enter]. In this dialog:
 - Move to "IPV4 Address". Move the first dotted octet of the IP address and set it. Repeat for the other octets.
 - Move the "Subnet mask" and set it.
 - Move to "Default Gateway" and set it.
 - Move to "DNS Server" and set it.
 - Press [Esc] to exit this dialog.
- Move to "LAN User Configuration" and press [Enter]. In this dialog:
 - Move to "Enter Password" and set it.
 - Move to "Confirm Password" and repeat it.
 - Press [Esc] to exit this dialog.
- Press [Esc] to exit. Move to "Save Changes and exit" and press [Enter]. The boot will continue automatically.

You can manage the server remotely from any Internet browser on any computer on the network with the URL <http://<iDRAC-IP-address>>. At the prompt, enter the iDRAC user name (Admin) and its password.



5.3.10 Product Sharing Deployment Instructions

This section describes the deployment of the Product Sharing software. The Product Sharing software distributes products stored on the NAS to a Zone Interface Point (ZIP) server on the CFWOS firewall. The software is described in RD-13.

The Product Sharing is deployed on the primary processing server and the backup processing server. However, the product distribution will be active only on the primary processing server.

The software is delivered in patch 160401A. Before installing this patch, patch 160324A containing the latest GPF_install must be installed. The deployment consists of various tasks described in the following sub-sections. **The steps below are performed on both processors as user seadas unless stated otherwise.**

5.3.10.1 Deployment Prerequisite

The following are requirements for the ZIP environment for a successful product sharing:

- ZIP Server is ready to receive data via Secure Socket Handler (SSH)
- Firewall are configured to allow SSH between the processing servers and ZIP
- A user has been created on the ZIP server to receive the data
- Proper cycling of the data on the ZIP server has been enabled
- ZIP server IP and user name are available prior to installing patch 160401A

The administrator must acquire the following information prior to installing the package:

- Get the user and IP address of the ZIP server receiving the data.
- Check SSH access to this user from the processing servers.

5.3.10.2 Authentication Setup Using Pair of Keys

The authentication is to be done on both processing servers as user seadas. Execute the following commands to set the authentication between the processing server and the ZIP server:

```
# On Processing server check to see if the .ssh directory already exists:
ls -d ~/.ssh

#If it doesn't exist, we need to create it before the next step
# and change the permissions on our .ssh directory:
mkdir ~/.ssh
chmod 700 ~/.ssh

# Check if the DSA keys are present
ls -l ~/.ssh/id_dsa.pub ~/.ssh/id_dsa

# If the two files exist, skip the next 5 commands.
# IF DSA KEY FILES EXIST DO NOT CREATE AGAIN!!!
# Press the [Enter] key when prompted to use the defaults.
cd ~/.ssh
ssh-keygen -t dsa -f id_dsa
chmod 600 id_dsa
chmod 644 id_dsa.pub
cd ~

# Now ssh to the zip user (myname) on the zip server (myip).
```



```
# (Replace myname and myip in the commands below with the appropriate value)
ssh myname@myip

# On the ZIP server:
# check to see if the .ssh directory exists there. On the server:
ls -d ~/.ssh

# If it doesn't exist, create it, and give it the appropriate permissions
mkdir ~/.ssh
chmod 700 ~/.ssh

# Same for the authorized_keys file. First check that it exists.
ls ~/.ssh/authorized_keys

# If it doesn't, create it , and give it the appropriate permissions
touch ~/.ssh/authorized_keys
chmod 644 ~/.ssh/authorized_keys

# log out of the zip server:
logout

# Now you need to place the contents of your local public key file
# (~/.ssh/id_dsa.pub, which you created earlier with ssh-keygen) into
# the file ~/.ssh/authorized_keys on your server.
cat ~/.ssh/id_dsa.pub | ssh myname@myip 'cat >> ~/.ssh/authorized_keys'

# Now your public key is installed on the server, and you should be able
# to execute a ssh command without a password
ssh myname@myip hostname
```

5.3.10.3 *Installation and Configuration*

The following patches are needed to install the Product Sharing software; patch 160324A (latest GPF_install) and 160401A (Product Sharing software). The patches are installed on both processing servers as user root with the following commands:

```
cd /users/gae/patch
./GPF_install 160324A
./GPF_install 160401A
```

The Product Sharing software is installed and configured on both processing servers as user seadas with the following command:

```
~/bin/pszip_config.sh install
```

Edit the connection parameters file `~/config/connectionparameter.ini` to define the user and the IP address of the ZIP server.

```
user="enter user name"           (the user on the ZIP destination)
ip="enter IP address"           (the IP address of ZIP destination)
```

Please, do the same with the file `~/config/connectionparametertest.ini`



5.3.10.4 *Pre-operation Test*

This test is performed on the backup processing server as user seadas. To test the connection to the ZIP and the product sharing of the PNG images, execute the following command:

```
~/bin/pszip_start.py ~/config/connectionparameteretest.ini
```

This should transfer all PNG images less than 1 day old. You need to check the ZIP directory and compare it with the NAS data in the source directory ~/Images. Also, check the log file ~/products-sharing/logFile.log for errors.

5.3.10.5 *First Product Sharing Run and Operation Test*

The first run of the product sharing would transfer all data that was generated within the last 24 hours, which might consist of a large amount of data to be transferred. Therefore, we recommend that the first run of the product sharing to be done manually and monitored as an operation test.

We also recommend that whenever there is a long interruption of the Product Sharing application for any reason, to use this same manual procedure before enabling the Product Sharing through the CRON process.

This test is done on the primary processing server as user seadas. To manually start the product sharing of all the products and PNG images, execute the following command:

```
~/bin/pszip_start.py ~/config/connectionparameter.ini
```

This should transfer all data L2, L3 as well as images less than 1 day old. You need to check the ZIP directory and compare it with the NAS data in the source directories ~/DATA/GRAN/, ~/DATA/L3, and ~/Images. Also, check the log file ~/products-sharing/logFile.log for errors.

5.3.10.6 *Scheduling Product Sharing Application*

The scheduling of the product sharing application has been configured but not enabled when the install command was executed:

```
~/bin/ pszip_config.sh install
```

The command above added the product sharing application to the cron of user seadas scheduled to execute every 2 hours at 5 minutes after the hour. The job is commented by default:

```
#5 0,2,4,6,8,10,12,14,16,18,20,22 * * * ~seadas/bin/pszip_start.py \  
~seadas/config/connectionparameter.ini > /dev/null 2>&1
```

To have the Product Sharing operational, the program should be installed on both servers, enabled on one server and disabled on the other. It is recommended to enable the product sharing on the primary processing server.

To Enable the product sharing task on the cron, execute the command below as user seadas. This command is to be executed on one server only.

```
~/bin/ pszip_config.sh enable (this will enable the scheduled task on the crontab)
```

The command above will enable the scheduled task on the cron of user seadas.



To Disable the product sharing task on the cron, execute the command below as user seadas. This command is to be executed only on the other server.

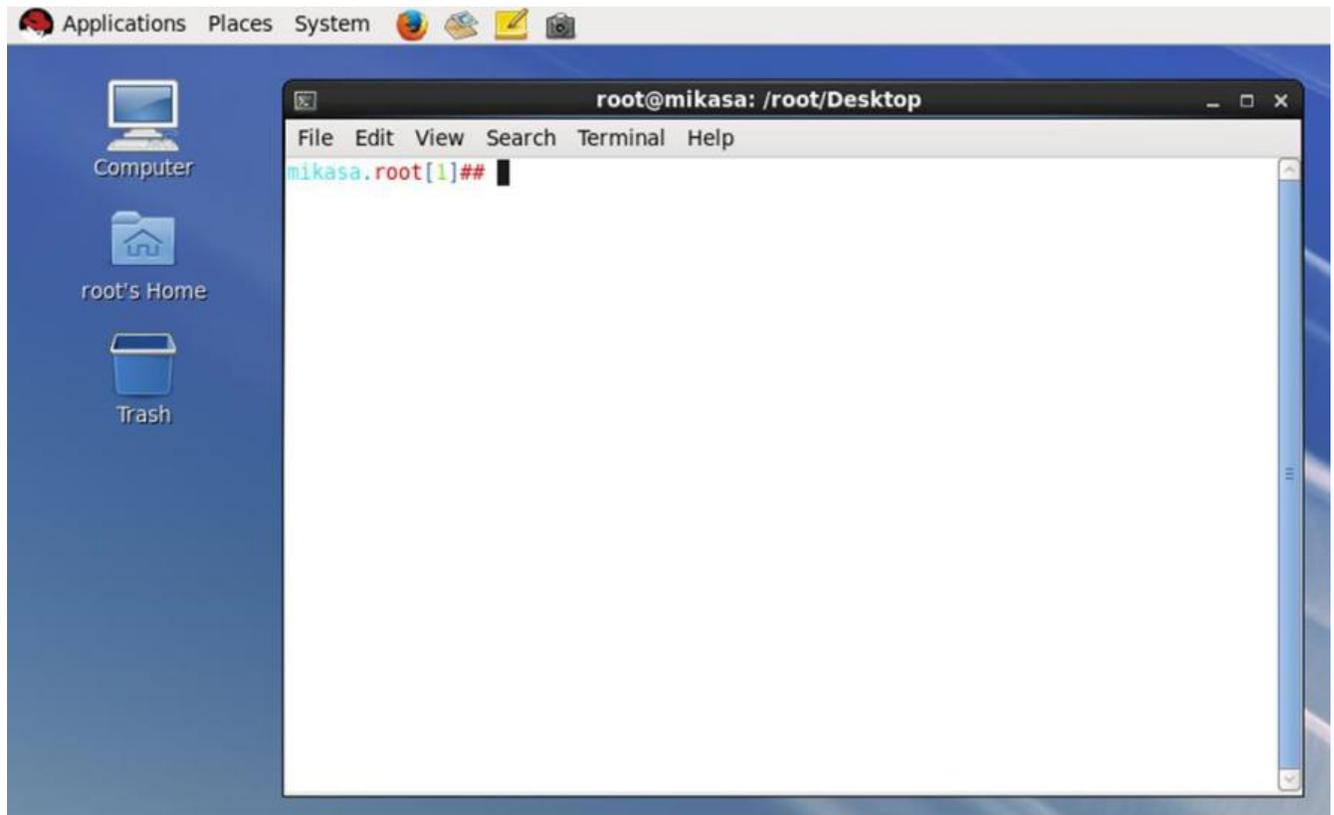
```
~/bin/pszip_config.sh disable      (this will disable the scheduled task on the crontab.)
```

The command above will disable the scheduled task on the cron of user seadas.



5.4 Operator Workstation Configuration

This section describes the on-site configuration of the operator workstation running Red Hat Linux. The instructions in this section assume you are logged in as user root on the console of the server. If you are not user root on the console, log off by clicking the “Log Out” function under the “System” menu. In the dialog, click “Log Out” to log out. Enter ‘root’ at the prompt. The GNOME Environment appears. Next, move the cursor on the background, press the right-mouse button, move to “Open Terminal” and release the button. A terminal window appears. The commands will be entered in this window.

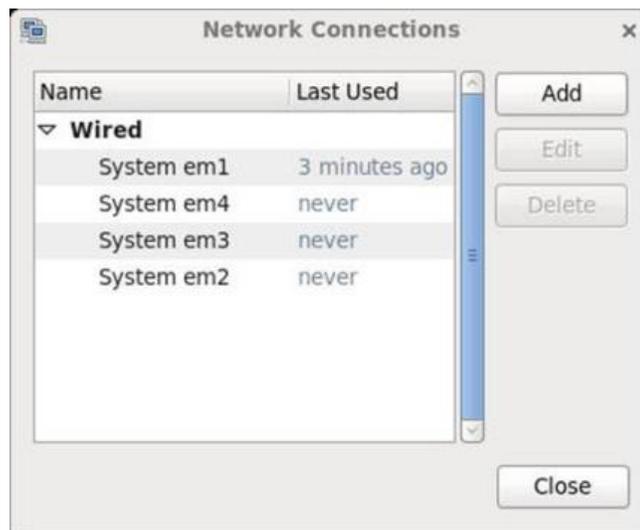


5.4.1 Network Parameters

Execute the command

```
/usr/bin/nm-connect-editor
```

to define the network parameters. The following dialog window appears:



Highlight “System em1” and click “Edit”. The following dialog appears:



Follow these steps:

- Select “Connect automatically”
- Select “Available to all users”
- Select “IPv4 Settings”



- Select “Manual” for “Method”
- Set Address, Netmask, and Gateway
- Set DNS servers
- Select “Require IPv4 addressing for this connection to complete”
- If required, configure the routes
- Click “Apply” to save your changes and exit this dialog
- Click “Close” to close the “Network Connections” dialog.

Execute the following command for your changes to take effect:

```
service network force-reload
```

An easy way to check Internet access is to launch a Web browser and try a Web page.

5.4.2 Hosts Table

The ingest server has been delivered with a hosts table file, /etc/hosts, containing the IP address and a generic name for each host on the ESC system:

ins	ingest server
ps1	Primary processing server
ps2	Secondary or backup processing server
ows	Operator workstation
nas	Network Attached Storage Server. Note that the NAS also has the service tag as alias.
nts	Network Time Server (NTS/GPS unit)

These names are used in various scripts and launch programs to minimize the on-site configuration. You can add your own name, but we recommend you keep the names listed above as aliases. For example, replace the line

```
x.x.x.x <default-ingest-server-name> ins
```

with

```
y.y.y.y <your-ingest-server-name> ins
```

It is important to keep the alias representing the NAS server service tag. This alias allows mounting the NAS storage file systems. To edit /etc/hosts, log in as user root and execute the command ‘vi /etc/hosts’. Enter the correct IP addresses and add your choice of host names.

5.4.3 Clock Synchronization

The system has been delivered with a Network Time Server (NTS) unit equipped with a GPS antenna. Each server or workstation delivered with the system has been pre-configured to synchronize with this NTS unit. The unit IP address should be in the hosts table along with ‘nts’ as its host name or one of its aliases.

The Network Time Protocol (NTP) configuration file /etc/ntp.conf may contain a list of “pool” servers:

```
server 0.rhel.pool.ntp.org  
server 1.rhel.pool.ntp.org
```



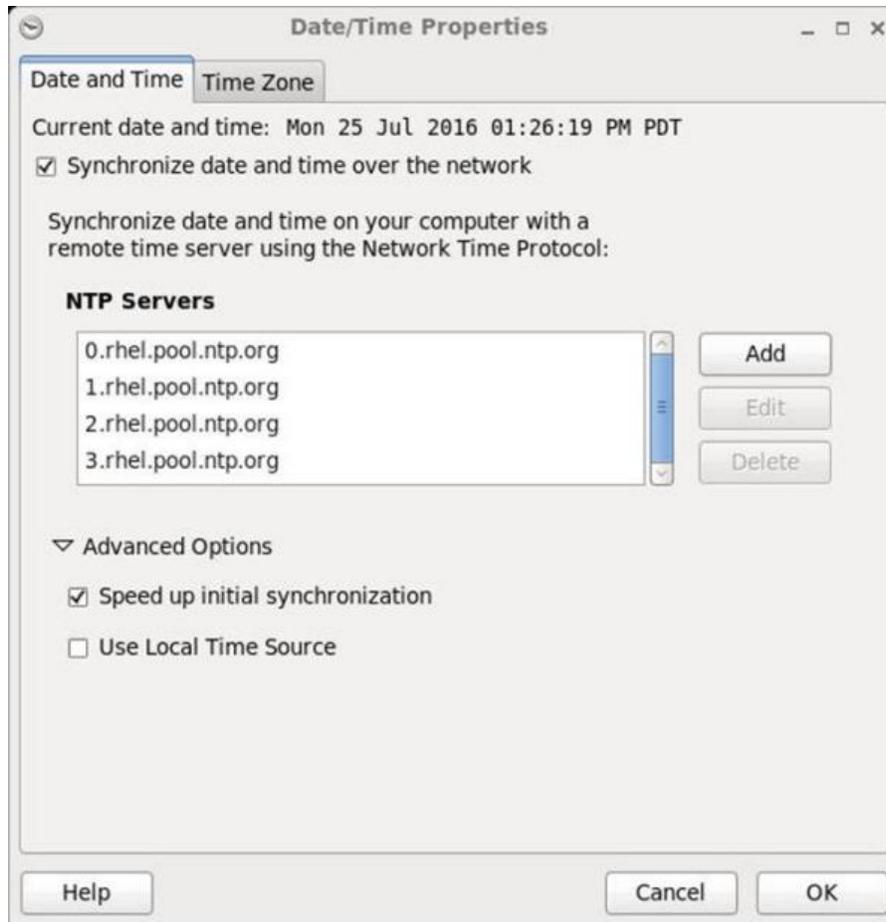
```
server 2.rhel.pool.ntp.org
```

It is recommended you edit this file and comment these lines unless you wish to join the NTP pool project at <http://www.pool.ntp.org/join.html>.

To verify that NTP is configured correctly, execute the command

```
/usr/bin/system-config-date
```

The following dialog appears:



Follow these steps:

- Display “Date and Time” panel
- Select “Synchronize date and time over the network”
- Remove the RHEL pool servers and add the server “nts” in the “NTP Servers” window.
- Extend “Advanced Option
- Select “Speed up initial synchronization
- Click OK to exit. He NTP service will start automatically.

The clock showing in the upper left corner of the screen should show the correct time.



5.4.4 Changing the Passwords

The ESC system has been delivered with pre-configured passwords. These passwords are listed in the pre-configuration sheet delivered with the system. To change the user passwords on a server or on the workstation, enter the command ‘passwd <user>’ where <user> is root, seadas, modis, or gae.

5.4.5 Password less SSH Access

The workstation has been pre-configured to allow password less remote access to user seadas from various remote users and machines. This password less access is necessary for some operations of the system:

- Pop-up warning if failure to download the orbital elements.
- Execute commands from remote host without password request (in launch icons).
- System Alert such as computer failure, network failure, or NAS failure.

The table below lists the source users and machines that **need** password less access to the user seadas on the operator workstation:

Source		Destination	
user1	host1	user2	host2
gae	ins	seadas	ows
gae	ows	seadas	ows
gae	ps1	seadas	ows
gae	ps2	seadas	ows

The file authorized_keys in \$HOME/.ssh of each destination user must have a DSA key from the source user/host. Note that this file may contain the keys for other source users/hosts. Some access is allowed only to facilitate remote command execution. Refer to Appendix B for details on setting password less SSH access.

5.4.6 Orbital Elements Download

To download the elements, execute the command

```
crontab -u gae -l
```

An entry containing the command get_oes is shown. Execute this command including its argument to download the orbital elements and test the Internet access. If downloading from NASA, execute the command

```
sudo -u gae /users/gae/oestools/get_oes nasa
```



The output should be as follows:

```
Working in /users/gae/oestools
/usr/bin/wget ... ftp://169.154...
drl.tle downloaded.
/usr/bin/wget ... ftp://169.154...
norad.tle downloaded.
cat drl.tle ... | /users/gae/oestools/nav2bbs > tle.txt.new
mv tle.txt.new tle.txt
/users/gae/oestools/tle2ole tle.txt
```

Once the elements can be downloaded, you may need to set a time at which the elements are downloaded every day. To verify the time at which the elements are downloaded, execute the command

```
crontab -u gae -l
```

An entry containing the command `get_oes` is shown. The first two columns indicate the minute and hour of day at which the command is executed. If you wish to modify it, execute the command

```
crontab -u gae -e
```

and set a new time.

Lastly, edit the script `/users/gae/oestools/get_oes` and replace the line ‘unset alert’ with ‘set alert’ to enable a pop-up window on the workstation in the event the orbital elements cannot be downloaded. The output of this cron job is mailed to user `gae` and resides in the file `/var/mail/gae`.

Note that user `gae` on the operator workstation must have password less access to user `seadas` on the operator workstation.

5.4.7 Mounting NAS Storage Drive

The processing servers and the operator workstation have been delivered with the NAS storage drives mounted as `/nas0` and `/nas1`. The file `/etc/fstab` contains two entries specifying the remote storage (`<remote-host>:<remote-drive>`), the mount directory (`/nas0` or `/nas1`) and the login parameters.

To verify the NAS drives are mounted, enter the command ‘`bdfm`’ or ‘`df -h`’. If `/nas0` or `/nas1` do not appear, execute these tasks:

- Create the mount points:

```
mkdir /nas0 /nas1
chmod 777 /nas0 /nas1
```
- Edit `/etc/fstab` and set the password for the `nas0` and `nas1` entries:

```
<remote-host>:nas0 /nas0 cifs username=Administrator,password=<password>
<remote-host>:nas1 /nas1 cifs username=Administrator,password=<password>
```

where `<remote-host>` is the NAS hostname (usually `nas`) and `<password>` is the password of user `Administrator` on the NAS.
- Execute the command ‘`ping <remote-host>`’ to check the Internet connection. `<remote-host>` is the first component of each NAS entry in `/etc/fstab`.
- If there is no connection, check the network parameters of the machine you are logged into and the network parameters of the NAS server. Check the connections to the network switch. Repeat the step above.



- Execute the commands ‘mount /nas0’ and ‘mount /nas1’.
- If there is an error message, contact Global Imaging.
- Execute the command ‘bdfm’ to verify that /nas0 and /nas1 are mounted.
- If they are not mounted, contact Global Imaging.
- Create a file in each filesystem

```
touch /nas0/SEADAS/dummy /nas1/SEADAS/dummy
rm /nas0/SEADAS/dummy /nas1/SEADAS/dummy
```
- If there is a problem creating the file, contact Global Imaging.

5.4.8 System Alert

The script `sds_ops_system_alert` allows the operator to automatically check the various computers on the system. This script runs every 5 minutes as a cron job of user `seadas`. The script tests if the machines are powered, networked, and storage is available. A pop-up window will appear on the operator workstation if one of the following tasks fails:

- Ping `ins`, `ows`, `ps1`, and `ps2`
- Copy a file to `/users/modis` of `ins`
- Copy a file to `/users/seadas` of `ows`, `ps1`, and `ps2`
- Copy a file to `/nas0/SEADAS` of `ows`, `ps1`, and `ps2`
- Copy a file to `/nas1/SEADAS` of `ows`, `ps1`, and `ps2`

You can list the cron jobs of user `seadas` with the command ‘`crontab -u seadas -l`’. The following line shows the system alert job:

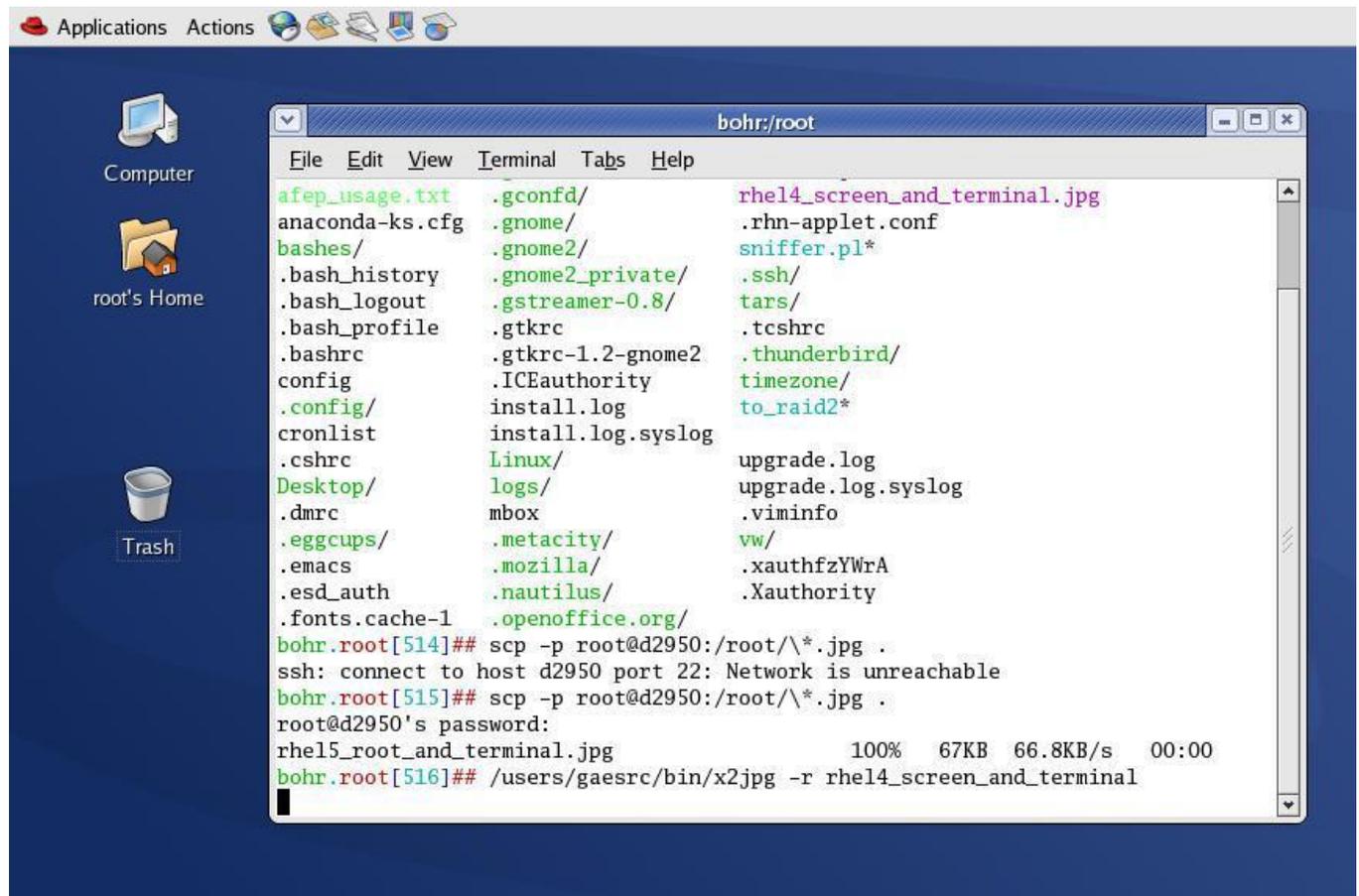
```
0,5,10,15,20,25,30,35,40,45,50,55 * * * * \
    /users/seadas/bin/sds_ops_system_alert \
    >> /users/seadas/alert.log 2>&1
```

If there is no such line, execute the command ‘`crontab -u seadas -e`’ and add it to the list.



5.5 Ingest Server Configuration

This section describes the on-site configuration of the ingest server running Red Hat Linux. The instructions in this section assume you are logged in as user root on the console of the workstation. If you are not user root on the console, log off by clicking the “Log Out” menu under the “Actions” menu. In this menu, click “OK” to log out. Enter ‘root’ at the prompt. The GNOME Environment appears. Next, move the cursor on the background, press the right-mouse button, move to “Open Terminal” and release the button. A terminal window appears. The commands will be entered in this window.

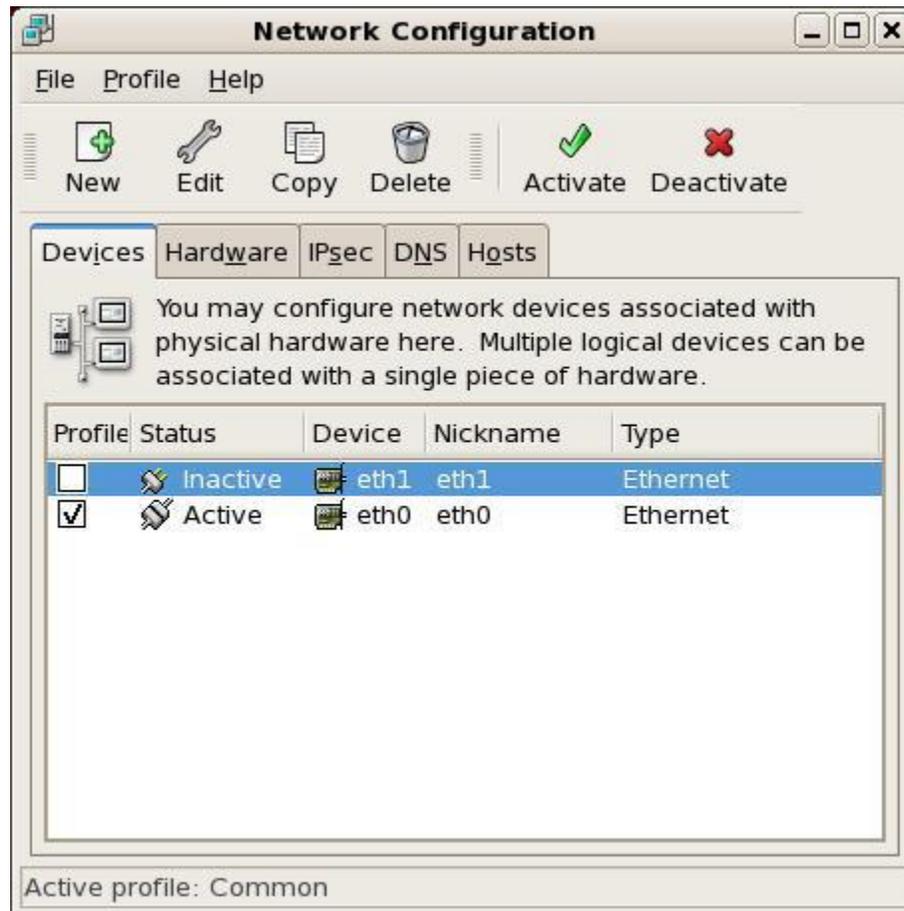


5.5.1 Network Parameters

Execute the command

```
/usr/bin/system-config-network
```

The following dialog appears:



Follow these steps:

- Click on the “Devices” panel tab.
- Select the ‘eth0’ device and click “Edit”.
 - Click “Statically set IP address”.
 - Enter the IP address of this host.
 - Enter the subnet mask.
 - Enter the default gateway.
 - Click “OK”.
- Click on the “DNS” panel tab.
 - Enter the host name
 - Enter the primary DNS address
 - Enter other DNS if they are used
- Click on the “Devices” panel tab.
- Click “Activate”. The status of the eth0 device will switch to Active.

An easy way to check Internet access is to launch a Web browser and try an external Web page.



5.5.2 Hosts Table

The ingest server has been delivered with a hosts table file, `/etc/hosts`, containing the IP address and a generic name for each host on the ESC system:

<code>ins</code>	ingest server
<code>ps1</code>	Primary processing server
<code>ps2</code>	Secondary or backup processing server
<code>ows</code>	Operator workstation
<code>nas</code>	Network Attached Storage Server. Note that the NAS also has the service tag as alias.
<code>nts</code>	Network Time Server (NTS/GPS unit)

These names are used in various scripts and launch programs to minimize the on-site configuration. You can add your own name, but we recommend you keep the names listed above as aliases. For example, replace the line

```
x.x.x.x      <default-ingest-server-name> ins
```

with

```
y.y.y.y      <your-ingest-server-name> ins
```

To edit `/etc/hosts`, log in as user `root` and execute the command `'vi /etc/hosts'`. Enter the correct IP addresses and add your choice of host names.

5.5.3 Clock Synchronization

The system has been delivered with a Network Time Server (NTS) unit equipped with a GPS antenna. Each server or workstation delivered with the system has been pre-configured to synchronize with this NTS unit. The unit IP address should be in the hosts table along with `'nts'` as its host name or one of its aliases.

The Network Time Protocol (NTP) configuration file `/etc/ntp.conf` may contain a list of “pool” servers:

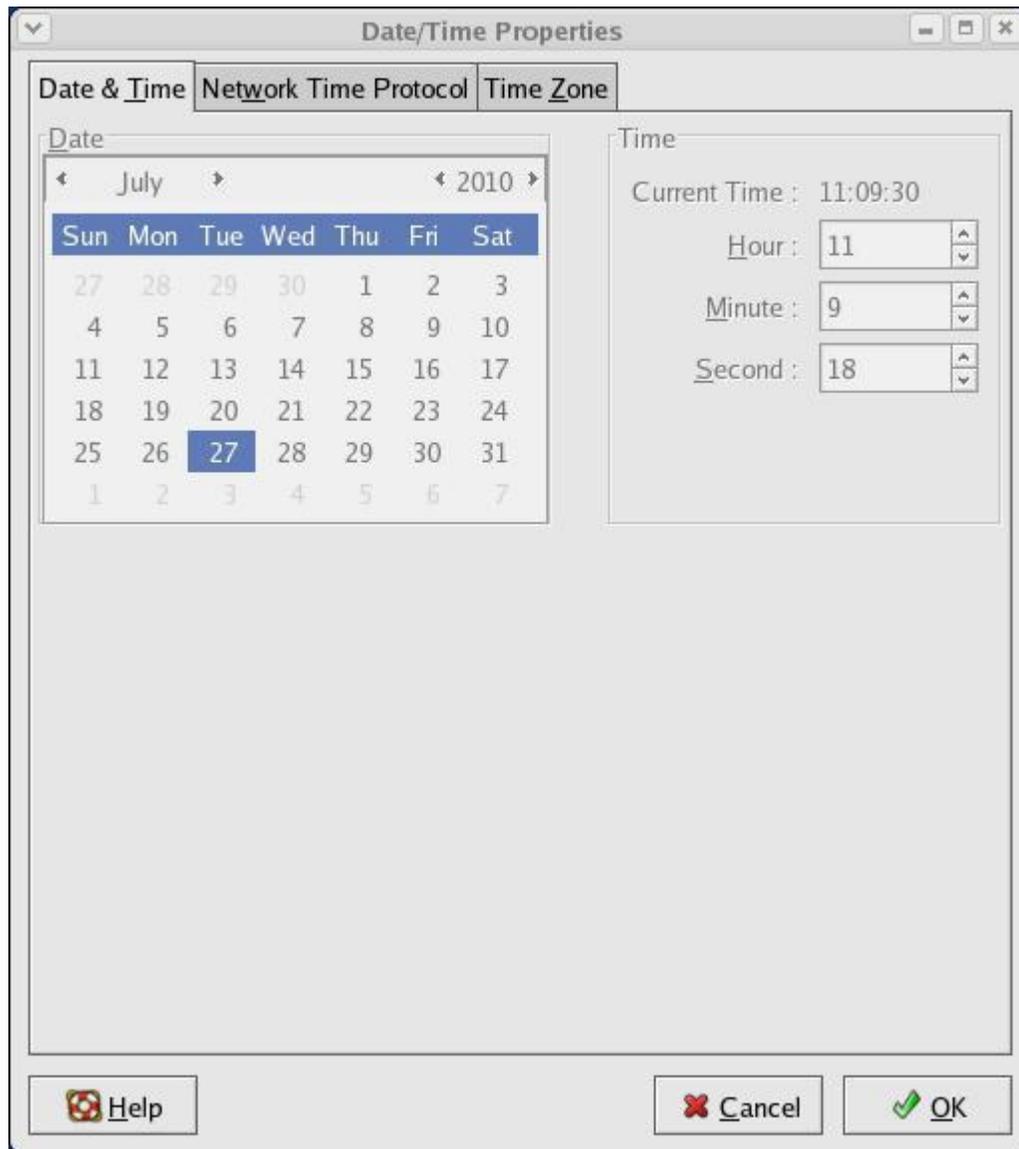
```
server 0.rhel.pool.ntp.org
server 1.rhel.pool.ntp.org
server 2.rhel.pool.ntp.org
```

It is recommended you edit this file and comment these lines unless you wish to join the NTP pool project at <http://www.pool.ntp.org/join.html>.

To verify that NTP is configured correctly, execute the command

```
/usr/bin/system-config-date
```

The following dialog appears:



Follow these steps:

- Click on the “Network Time Protocol” panel tab.
- Select the “Enable Network Time Protocol” if it is not already selected.
- If “nts” does not appear in the list, enter ‘nts’ and click “Add”.
- Click OK to exit.

The clock showing in the upper left corner of the screen should show the correct time.

5.5.4 Changing the Passwords

The ESC system has been delivered with pre-configured passwords. These passwords are listed in the pre-configuration sheet delivered with the system. To change the user passwords on a server or on the workstation, enter the command ‘passwd <user>’ where <user> is root, seadas, modis, or gae.



5.5.5 Password less Access

The ingest server has been pre-configured to allow password less remote access to user modis processor from various remote user and machines. This password less access is necessary for some operations of the system:

- Pop-up warning if failure to download the orbital elements.
- Execute commands from remote host without password request (in launch icons).
- System Alert such as computer failure, network failure, or NAS failure.

The table below lists the source users and machines that **need** password less access to the user modis on the ingest server:

Source		Destination	
user1	host1	user2	host2
seadas	ows	modis	ins

The file `authorized_keys` in `$HOME/.ssh` of each destination user must have a DSA key from the source user/host. Note that this file may contain the keys for other source users/hosts. Some access is allowed only to facilitate remote command execution. Refer to Appendix B for details on setting password less SSH access.

5.5.6 Orbital Elements Download

To download the elements, execute the command

```
crontab -u gae -l
```

An entry containing the command `get_oes` is shown. Execute this command including its argument to download the orbital elements and test the Internet access. If downloading from NASA, execute the command

```
sudo -u gae /users/gae/oestools/get_oes nasa
```

The output should be as follows:

```
Working in /users/gae/oestools
/usr/bin/wget ... ftp://169.154...
drl.tle downloaded.
/usr/bin/wget ... ftp://169.154...
norad.tle downloaded.
cat drl.tle ... | /users/gae/oestools/nav2bbs > tle.txt.new
mv tle.txt.new tle.txt
/users/gae/oestools/tle2ole tle.txt
```

Once the elements can be downloaded, you may need to set a time at which the elements are downloaded every day. To verify the time at which the elements are downloaded, execute the command

```
crontab -u gae -l
```

An entry containing the command `get_oes` is shown. The first two columns indicate the minute and hour of day at which the command is executed. If you wish to modify it, execute the command



```
crontab -u gae -e
```

and set a new time.

Lastly, edit the script `/users/gae/oestools/get_oes` and replace the line ‘unset alert’ with ‘set alert’ to enable a pop-up window on the workstation in the event the orbital elements cannot be downloaded. The output of this cron job is mailed to user gae and resides in the file `/var/mail/gae`.

Note that user gae on the operator workstation must have password less access to user seadas on the operator workstation.

If you have set a new download time, you will need to modify the time at which the scheduling and tracking program, STracker+, updates its own elements from the elements downloaded by `get_oes`. Refer to Section 5 in document RD-04 for details concerning STracker+.

5.5.7 Remote Management

To change the Remote Management network parameters and password on a server, reboot the server. During the reboot process, wait for the message

```
iDRAC6 Configuration Utility 1.45
```

```
...
```

```
Press <Ctrl><E> for remote access setup within 5 seconds...
```

Once you have typed [Ctrl-E], the iDRAC Configuration Utility appears. Use the up and down arrow keys to move/highlight the desired item. Follow these steps:

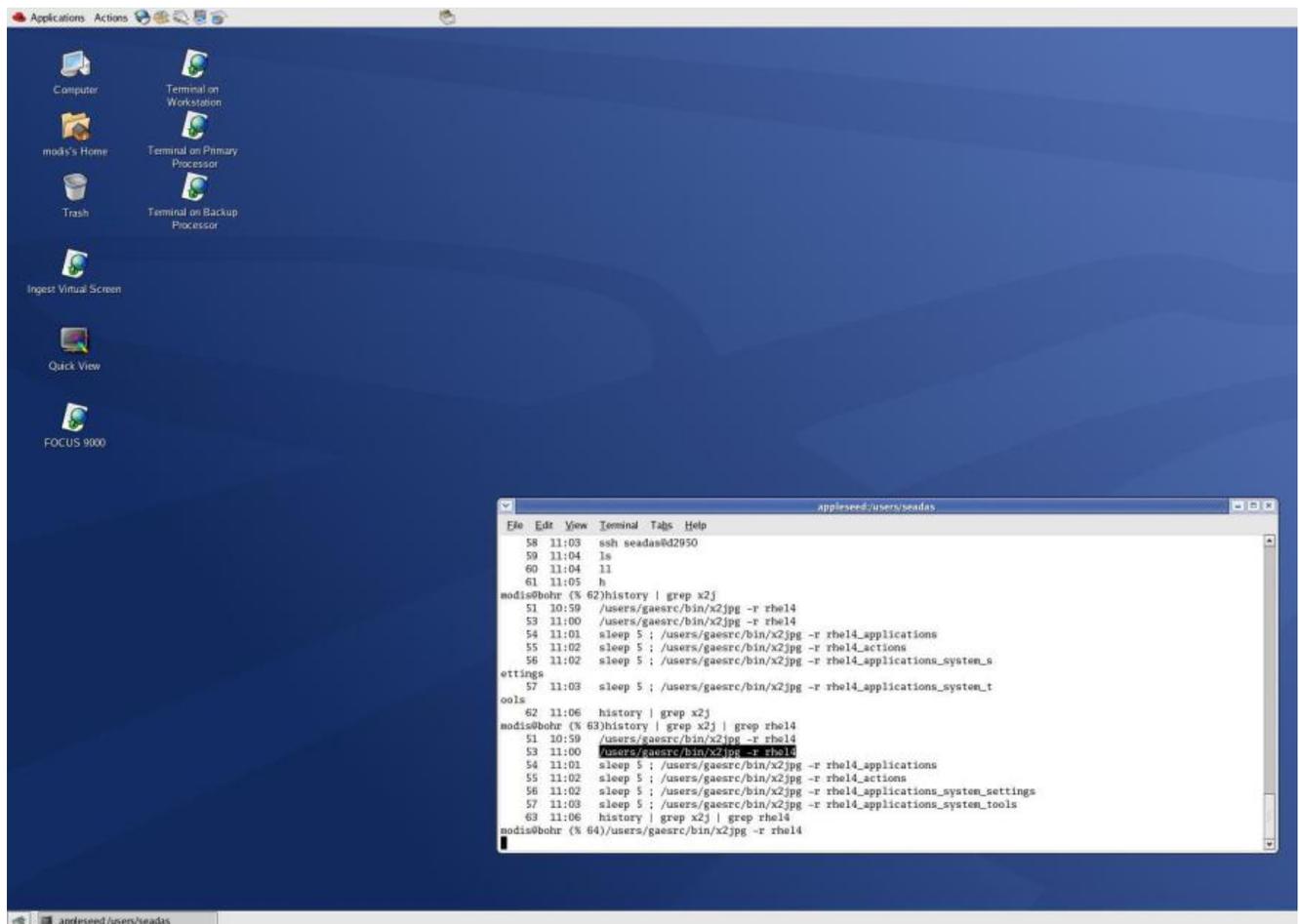
- Move to "LAN Parameters" and press [Enter]. In this dialog:
 - Move to "IPV4 Address". Move the first dotted octet of the IP address and set it. Repeat for the other octets.
 - Move the "Subnet mask" and set it.
 - Move to "Default Gateway" and set it.
 - Move to "DNS Server" and set it.
 - Press [Esc] to exit this dialog.
- Move to "LAN User Configuration" and press [Enter]. In this dialog:
 - Move to "Enter Password" and set it.
 - Move to "Confirm Password" and repeat it.
 - Press [Esc] to exit this dialog.
- Press [Esc] to exit. Move to "Save Changes and exit" and press [Enter]. The boot will continue automatically.

You can manage the server remotely from any Internet browser on any computer on the network with the URL `http://<iDRAC-IP-address>`. At the prompt, enter the iDRAC user name (Admin) and its password.



5.6 Ingest Server Verification

This sections describes the configuration and verification of the IVS and the distribution on the ingest server. The instructions in this section assume you are logged in as user modis on the console of the workstation. If you are not user modis on the console, log off by clicking the “Log Out” menu under the “Actions” menu. In this menu, click “OK” to log out. Enter ‘modis’ at the prompt. The GNOME Environment appears. Next, move the cursor on the background, press the right-mouse button, move to “Open Terminal” and release the button. A terminal window appears. The commands will be entered in this window.



Alternately, you can perform these tasks remotely with the following login command:

```
ssh -Y modis@ins
```

The scheduling, tracking, and ingestion are done in the background by the STracker+ program running in an Ingest Virtual Display (IVS). The IVS is launched at boot time and is viewable using vncviewer. Before configuring the ingestion and distribution on the ingest server, make sure that the IVS is not running in the background by executing the following command:

```
/users/gae/v4.0/x/vnc-ivs -kill
```



5.6.1 Changing VNC Password

The ESC system has been delivered with pre-configured VNC password. The password is listed in the pre-configuration sheet delivered with the system. This password gives the operator access to the IVS from its workstation. To change the VNC password used by user modis to control access to the IVS, execute the command 'vncpasswd' and enter the new password.

5.6.2 Configure Level 0 Data Distribution

The ingest server has been pre-configured to distribute L0 data to either MODIS processors (ps1 and ps2), always sending the oldest dataset first. Verify that ps1 and ps2 are in the hosts table, /etc/hosts, and have the correct IP address. If you need to modify the level 0 distribution parameters, execute the command /users/modis/bin/Config_l0_dist. Verify that the first and second destination are set to ps1 and ps2. Set the correct password for both destinations if you are using FTP transfer mode.

5.6.3 GSI Ingest Device

To test the ingest device interface, execute the following command:

```
/users/gae/scsidvr/Linux/bin/getrev /dev/scsi_tfsb_1
```

The command outputs the firmware revision: GSI Firmware Revision : 10.1. Next, execute this command to output the unit status every second:

```
/users/gae/scsidvr/Linux/bin/getsts -t modis
```

The command outputs the status every second as follows:

```
TFSB/SCSI: Mode=FLIP_READ, BUFFER=16384KB, MAX-READ=1024KB  
TFSB/SCSI: TIMEOUT=1000000 (usec)  
TFSB/SCSI: Set FIFO to 8192 Kbytes.  
TFSB/SCSI: Setting GSI/TUMSD card for TERRA feed.  
TFSB/SCSI: No file /users/gae/TFSB_SCSI_Raw, skipping raw data storage.  
/dev/scsi_tfsb_1 (eam1) started.  
Status = 0xff18c7c7, -15153209 BANK=1 READY=1 BIT=0 FRAME=0  
Status = 0xff18c7c7, -15153209 BANK=1 READY=1 BIT=0 FRAME=0  
Status = 0xff18c7c7, -15153209 BANK=1 READY=1 BIT=0 FRAME=0  
Status = 0xff18c7c7, -15153209 BANK=1 READY=1 BIT=0 FRAME=0
```

5.6.4 Antenna Controller

To test the interface to the antenna controller, execute the following command:

```
/users/gae/v4.0/sattools/gitrack -t modis point 45.0 90.0
```

This command moves the antenna to 45 degree elevation and 90 degree azimuth. If the antenna is not aligned, the position is approximate.

If the antenna is not in a radome, you can track the sun for 3 minutes (180 seconds) with the following command and observe its shadow on the dish:

```
/users/gae/v4.0/sattools/gitrack -t modis sun 180
```



5.6.5 X-Band Receiver

To test the receiver interface, execute the following command:

```
/users/gae/scsidvr/Linux/bin/setrcvr /dev/scsi_tfsb_1 eam1 8212.5
```

to set the receiver to TERRA. The LED on the receiver will show TERRA. Next, execute the following command:

```
/users/gae/scsidvr/Linux/bin/setrcvr /dev/scsi_tfsb_1 epm1 8160.0
```

to set the receiver to AQUA. The LED on the receiver will show AQUA.

5.6.6 Antenna Alignment

The antenna alignment is done by tracking the sun, measuring its offset from the center of the scan window, and applying this offset to a new azimuth and elevation HOME position for the antenna. Once the new HOME position has been determined, subsequent scans should produce a centered sun. If not, set the HOME a second time and scan again.

To perform a sun scan, execute the following command:

```
/users/gae/v4.0/x/xscan -t modis
```

You can use the default given on the interface. Press ‘Scan’ when ready. The entire scan takes about 4-5 minutes depending on the width and height of the scan and its resolution. When the scan is done, verify that the computed offset is visually correct. If this is the case, click on “Home” to apply the offset to a new HOME position. You should save the scan using “File->Save”. Start another scan to verify the alignment. You scan stop the scan by clicking ‘Stop’. It will take about 10-15 seconds for the antenna to move to its stow position and for you to regain control of the program.

5.6.7 Automatic Start-up

Two processes need to start automatically at boot time: Ingest Virtual Screen and level 0 distribution. In order to verify the automatic start-up of these processes, log in as user root and reboot the ingest server with the command ‘shutdown -r 0’.

Once the ingest server is rebooted, log in as user modis at the console, open a terminal window and execute the command

```
vncviewer :2
```

to access the Ingest Virtual Screen. A password dialog appears. Enter the VNC password. The STracker+ window should be in the VNC screen. The status panels at the bottom of the STracker+ window are shown in green to indicate proper operation. Refer to Sections 4 and 5 in document RD-04 for details on using STracker+.

You can verify the start-up of the level 0 distribution script l0_dist with the command ‘ps -el | grep l0_dist’.

If you are running RHEL 5 and this command does not output anything, log in as user root (su -), verify that the execution mode of l0_dist in /etc/inittab is set to ‘respawn’. If it is not, set it, save your modifications, and execute ‘init Q’ for the modifications to take effect.



If you are running RHEL 6 and this command does not output anything, execute the following command as root user

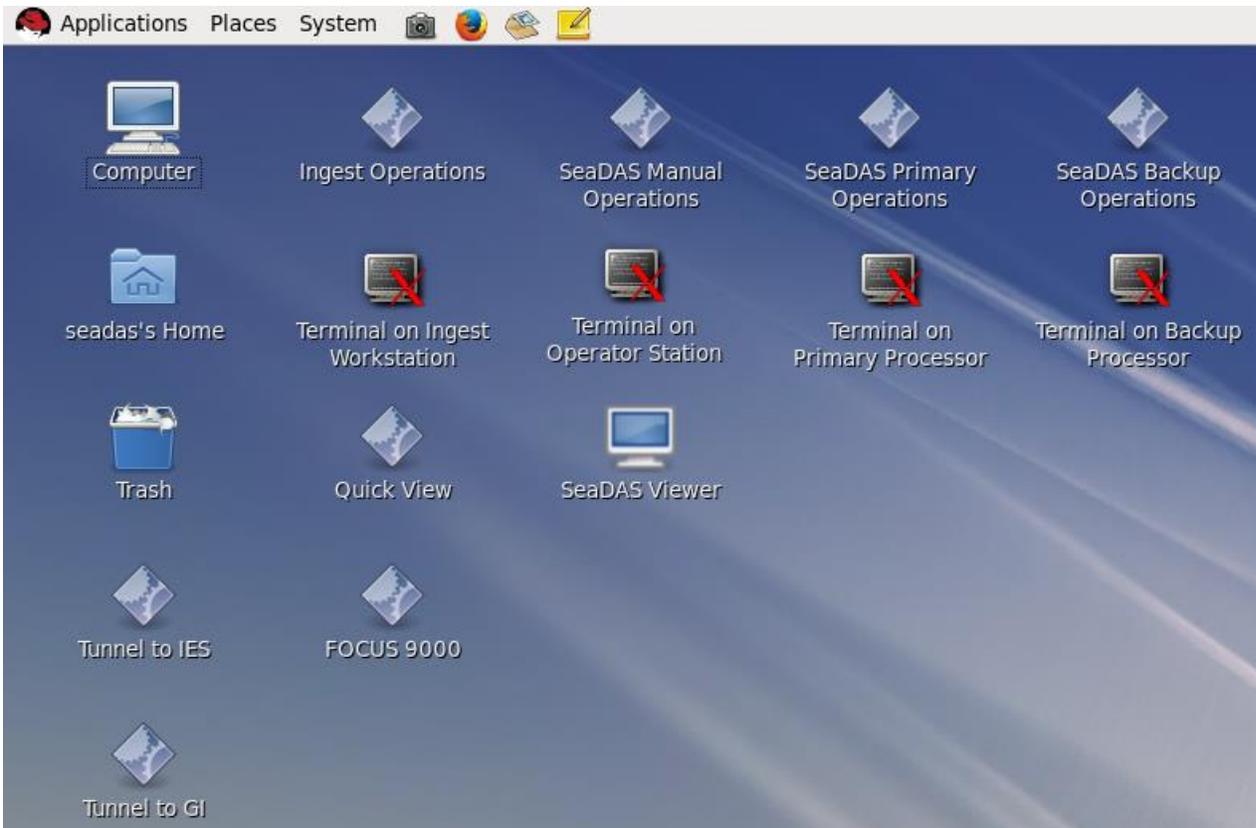
```
/users/gae/sbin/Upstart_load 10dd
```

Check again with the command 'ps -el | grep l0_dist'.

Refer to Section 6 in document RD-04 for details on level 0 distribution script l0_dist.

5.7 Operator Workstation Verification

The instructions in this section assume you are logged in as user seadas on the console of the operator workstation. If you are not user seadas on the console, log off by clicking the “Log Out” function under the “System” menu. In the dialog, click “Log Out” to log out. Enter ‘seadas’ at the prompt. The GNOME Environment appears. Next, move the cursor on the background, press the right-mouse button, move to “Open Terminal” and release the button. A terminal window appears. The commands will be entered in this window.



5.7.1 Ingest Virtual Screen Access

To access the Ingest Virtual Screen, execute the following command:

```
ssh -Y modis@ins "vncviewer :2"
```

5.7.2 Operator Console Access

To launch the operator console on the workstation, execute the following command:

```
sds_ops -noauto
```

Verify that the automatic processing functions have been de-sensitized. If /nas0 and /nas1 do not appear in the top window of the operator console, refer to Section 5.4.7 to verify the NAS storage mount.



To launch the operator console on the primary processing server, execute the following command:

```
ssh -Y seadas@ps1 "sds_ops -noman"
```

Verify that the manual processing functions have been de-sensitized. If /nas0 and /nas1 do not appear in the top window of the operator console, refer to Section 5.3.7 to verify the NAS storage mount.

To launch the operator console on the backup processing server, execute the following command:

```
ssh -Y seadas@ps2 "sds_ops -noman"
```

Verify that the manual processing functions have been de-sensitized. If /nas0 and /nas1 do not appear in the top window of the operator console, refer to Section 5.3.7 to verify the NAS storage mount.



6 Administrator Tasks

This section describes the administrator tasks such as start-up of each component of the system, the operating system support and various administrative tasks.

6.1 *Start-up - Remote Site*

The section describes the steps to start the components located at the remote site.

6.1.1 Antenna and Electronics

Verify that the antenna positioner controller is powered and that the outdoor fiber optic unit is also powered. All connectors should be secure in their appropriate sockets. Note that the positioner controller is un-powered while the radome hatch is opened.

6.1.2 UPS Unit

The UPS unit is located at the bottom of the ingest rack and has a small LED panel indicating its status. A blue panel indicates normal operations. Refer to Section 9 for details on the UPS unit.

6.1.3 NTS/GPS Unit

The NTS/GPS unit is located in the top back of the ingest rack. Make sure the NTS-150 unit is powered and connected to the GPS antenna and to the network switch. It may take up to 20 minutes for the unit to be operational.

The NTS-150 unit is equipped with two status lights: a connection active indicator (ACT) and a System Status Indicator (SSI). The ACT light should be green to indicate at 100 Mbps connection. The SSI light is solid red when there is no signal from the time source or a major failure is detected. Otherwise, the SSI light blinks green to indicate a lock to GPS.

6.1.4 Network Switch

The network switch is located in the top back of the ingest rack. Make sure the network switch is powered and is connected to the GP-NET router. If the power is off, verify the power cord is secure in the power supply socket and also on the PDU.

6.1.5 X-Band Receiver

The X-Band is located in the ingest rack. Verify the X-Band receiver is powered. The unit has an LED display. If the display is black, flip the power switch close to the power socket in the back of the unit. If the power is still off, verify the power cord is secure in the power supply socket and also on the PDU.

6.1.6 GSI Unit

The GSI MODIS ingest unit is located in the ingest rack. Verify the unit is powered. The unit has a power indicator on its front panel. If the power is off, flip the power switch. If the power is still off, verify the power cord is secure in the power supply socket and also on the PDU.



6.1.7 IF Fiber Optic Unit

The IF fiber optic unit is located in the ingest rack. Verify the IF fiber optic unit is powered. The unit has a power indicator on each of the two power supplies. If the power is off, verify the power cord is secure in the power supply socket and also on the PDU.

6.1.8 RS-485 Fiber Optic Unit

The RS-485 fiber optic is located in the ingest rack. Verify that the power cord of the RS-485 fiber optic unit is secure in its socket and also on the PDU.

6.1.9 KVM console

The KVM console has a power button at the bottom of its LCD. The button shows blue when the KVM is powered. If the power is still off, verify the power cord is secure in its socket and also on the PDU.

6.1.10 Ingest Server

Before booting the ingest server, verify that the following connections are secure:

- Power cords are secure in their sockets and also on the PDU.
- Analog Video and Keyboard/Mouse to the KVM console
- SCSI connection to the ingest unit
- USB connection to the MODIS Mk II Receiver
- USB Dongle
- Serial connection to the RS-485 Fiber Optic unit
- Built-in 1Gbit NIC 1 connected to the network switch

Additionally, confirm that the receiver I/Q channels and the G/T Test cables are connected to the GSI unit and that the receiver is connected to the IF fiber optic unit. Additionally, both fiber optic units must be connected to the outdoor fiber optic unit in the radome.

To boot the ingest server, remove the front panel, press the power button and replace the panel. The boot process is displayed on the KVM console. Once the boot process is done, a login window appears. Note that the ingest server starts its operations automatically at boot-up. The ingest server operations can be monitored locally or from the operator workstation. Refer to Section 3 of document RD-02 for details.

6.2 Start-up - Base Site

This section describes the steps to start the components located at the base site in the server room (6.2.1 through 6.2.7) and in the METOC room (6.2.8).

6.2.1 KVM Switch

The KVM switch has a power switch beside its power cord. Make sure the switch is in the ON position.



6.2.2 KVM Console

The KVM console has a power button at the bottom of its LCD. The button shows blue when the KVM is powered. Press [Ctrl] twice to show the KVM menu. In this menu, select the server you wish to view and press [Enter].

6.2.3 Network Switch

Make sure the network switch is powered and is connected to the GP-NET router or an alternate router.

6.2.4 LTO drive

Make sure the LTO drive is powered and connected to the backup processing server.

6.2.5 Network Attached Storage Server

Before booting the NAS server, make sure it is connected to the network switch and the KVM switch. To boot this server, remove the front panel, press the power button and replace the panel. The boot process is displayed on the KVM console by selecting this server (Section 6.2.2). Once the boot process is done, a login window appears. Note that the NAS server starts its operations automatically at boot-up.

Once the NAS has booted, verify that /nas0/SEADAS and /nas1/SEADAS can be accessed (read/write) by the processing servers and the workstations. If there is a problem with the access, simply reboot the machine with NAS access problem and check the NAS access again.

6.2.6 Primary Processing Server

Before booting the primary processing server, make sure it is connected to the network switch and the KVM switch. A USB license dongle must be present. To boot this server, remove the front panel, press the power button and replace the panel. The boot process is displayed on the KVM console by selecting this server (Section 6.2.2). Once the boot process is done, a login window appears. Note that the primary processing server starts its operations automatically at boot-up. These operations are monitored from the operator workstation.

If you have booted this server while the NAS is down, make sure to manually mount the NAS storage devices once the NAS server is up (Section 5.3.7). If there is still a problem, reboot the primary processing server once the NAS server is started.

6.2.7 Backup Processing Server

Before booting the backup processing server, make sure it is connected to the network switch, the KVM switch, and the LTO drive. A USB license dongle must be present. To boot this server, remove the front panel, press the power button and replace the panel. The boot process is displayed on the KVM console by selecting this server (Section 6.2.2). Once the boot process is done, a login window appears. Note that the backup processing server starts its operations automatically at boot-up. These operations are monitored from the operator workstation.

If you have booted this server while the NAS is down, make sure to manually mount the NAS storage devices once the NAS server is up (Section 5.3.7). If there is still a problem, reboot the



backup processing server once the NAS server is started.

6.2.8 Operator Workstation

Before booting the operator workstation, make sure it is connected to a network switch, to the two monitors, to the keyboard, and to the mouse. A USB license dongle must be present. To boot this workstation press the power button. The boot process is displayed on the monitors. Once the boot process is done, a login window appears. Refer to Section 3 of document RD-02 for details on the Operator's tasks.

If you have booted this workstation while the NAS is down, make sure to manually mount the NAS storage devices once the NAS server is up (Section 5.4.7). If there is still a problem, reboot the operator workstation once the NAS server is started.

6.3 Operating System Support

The Red Hat Enterprise Linux installed on the ingest server, the processing servers, and the workstation are delivered with a 1-year subscription to Red Hat. The subscription information can be found with the OS installation DVDs. Each server and the workstation must be registered with Red Hat in order to receive the OS patches.

The Windows Storage 2008 Standard is installed with automatic update download. However, they are not installed until the administrator authorizes it.

6.4 Administrative Tasks

The administrative tasks consist of various system configurations such as network, password, NTS, etc. as well as viewing the system logs and checking the clock. These tasks are done in the same fashion on the ingest server, processing server, or the workstation. However, the menus and function are slightly different on the ingest server (RHEL V4) than on the processing server and the workstation (RHEL V6). Most of these tasks require user root privileges.

6.4.1 Ingest Server

The picture below shows the menu displayed on the desktop of the ingest server:



From the Applications menu, you can perform these tasks and much more.

- Applications ->Internet ->Firefox Web Browser
- Applications -> File Browser
- Actions -> Shut Down

Before rebooting or shutting down the ingest server, look at the bottom of the STracker+ program for the countdown to the next pass. A negative count indicates the time left until the next pass. If a pass is running or will start very soon, wait until 5 minutes after the pass is completed to shut down.



- Applications -> System Tools -> Network Tools
- Applications -> System Tools -> System Logs

The following picture shows one of the most useful sub-menus:





From this menu, you can perform these tasks:

- Applications -> System Settings -> Date & Time (NTS, Time Zone)
- Applications -> System Settings -> Network
- Applications -> System Settings -> Users & Groups
- Applications -> System Settings -> Security Level & Firewall

Most of these tasks can be executed remotely with the appropriate script. For example, the NTS is configured with the command `/usr/bin/system-config-date`. Because most of these scripts have a GUI, their remote execution requires a log in as follows:

```
ssh -Y root@<remote-host>
```

Check `/usr/bin` for the system configuration scripts.

6.4.2 Processing Servers and Workstation

The picture below shows the menu displayed on the desktop of the processing servers and the operator workstation:



From these menus, you can perform these tasks and much more.

- Applications → Internet → Firefox Web Browser
- Applications → System Tools → CD/DVD Creator
- Applications → System Tools → Disk Usage Analyzer
- Applications → System Tools → File Browser
- System → Preferences → Network Connections
- System → Administration → Date & Time (NTS, Time Zone)
- System → Administration → Users & Groups
- System → Administration → Firewall
- System -> Shut Down

Before shutting down one of the processing servers, check its processing log. If a granule is being processed, wait until the processing is done before shutting down.

Most of these tasks can be executed remotely from the workstation with the appropriate command. For example, the NTS is configured with the command `/usr/bin/system-config-date`. Because most of these commands have a GUI, their remote execution requires a log in as follows:

```
ssh -Y root@<remote-host>
```

Check `/usr/bin` for the system configuration scripts.



6.4.3 NAS Server

The following tasks can be performed on the NAS server:

- Configure the Network (Section 5.2.1)
- Set the Internet Time (Section 5.2.2)
- Administrator Password (Section 5.2.3)
- OS Updates

An icon located on the right side of the bottom panel indicates when updates are ready to install. Simply pass the cursor over these icons to show a brief description and select the appropriate icon.

- Symantec Updates

An icon located on the right side the bottom panel indicates when updates are ready to install. Simply pass the cursor over these icons to show a brief description and select the appropriate icon.

- Shutdown

Before shutting down the NAS server, check the processing log on the primary and backup servers. If a granule is being processed, wait until the processing is done before shutting down. Note that the NAS server should be booted before the next pass is distributed and processed. To shut down the NAS, perform the following steps:

- Press the Start button located on the left side of the bottom panel. A menu appears.
- Move to the right arrow shown on the lower right corner of the menu.
- Various functions including Shutdown appear.
- Select Shutdown and follow the instructions.

If the NAS will be down for an extended period, disable the L0 distribution on the ingest server. Refer to Section 6 of document RD-04 for details on l0_dist.

6.5 Clock Synchronization

An accurate clock is crucial for tracking Terra and Aqua satellites. Therefore, the ingest server clock should be synchronized to a Network Time Source (NTS) at all time. It is recommended that more than one NTS be used for this purpose. An accurate clock on the other servers and the workstation ensures that the file in the various storage devices have the correct creation time. To that end an NTS/GPS unit has been installed at the antenna site. The workstation and all the servers synchronize their clock with this NTS unit.

The quickest way to check the clock is to visually compare with an external clock you know to be accurate. The following Internet clock can be used:

<http://www.usno.navy.mil/USNO>

The procedure is outlined sections 6.5.1 through 6.5.5 for each machine on the system.



6.5.1 Checking the Ingest Server Clock

These instructions assume you are logged in at the Operator Workstation console.

- Start an Internet Browser (Mozilla or Firefox) via the Application menu of the Desktop:
Desktop: Applications→Internet→...

Enter this URL <http://www.usno.navy.mil/USNO>. The USNO Internet time is displayed.

- Open a Terminal Window and execute the following command

```
ssh modis@ins /users/gae/v4.0/tools/gmtclock
```

to display the system time of the ingest server.

- Visually compare the time shown in the browser with the time shown in terminal window.

If the system time is off by more than 2 seconds, execute these steps:

- Telnet to the NTS/GPS unit and check its status (Section 9). If the NTS/GPS unit is not working properly, submit a problem report. Otherwise, login as root user on the ingest server and proceed with the steps below.

- Verify the NTP daemon is running:

```
/etc/init.d/ntpd status
```

If it is not, start it with the command `/etc/init.d/ntpd start`. Otherwise, re-start it with the command `/etc/init.d/ntpd restart`. If there is a problem, submit a problem report. If the clock is still off, proceed with the next step.

- Check for the following message in `/var/log/messages`:

```
... ntpd[nnn]: synchronized to <NTS-IP>, stratum 1
```

If there is no message or the last message is old, this may suggest an Internet access problem to the NTS. Check for other messages tagged as `'ntpd[nnn]`'. They may point to the problem.

- If Internet access is permitted, consider adding extra NTS in `/etc/ntp.conf` for redundancy. After adding NTS, execute `/etc/init.d/ntpd restart` for your changes to take effect. If the clock is still off, submit a problem report.

6.5.2 Checking the Operator Workstation Clock

These instructions assume you are logged in at the Operator Workstation console.

- Start an Internet Browser (Mozilla or Firefox) via the Application menu of the Desktop:
Desktop: Applications→Internet→...

Enter this URL <http://www.usno.navy.mil/USNO>. The USNO Internet time is displayed.

- Open a Terminal Window and execute the following command

```
ssh modis@ows /users/gae/v4.0/tools/gmtclock
```

to display the system time of the operator workstation.



- Visually compare the time shown in the browser with the time shown in terminal window.

If the system time is off by more than 2 seconds, execute these steps:

- Telnet to the NTS/GPS unit and check its status (Section 9). If the NTS/GPS unit is not working properly, submit a problem report. Otherwise, login as root user on the operator workstation and proceed with the steps below.

- Verify the NTP daemon is running:

```
/etc/init.d/ntpd status
```

If it is not, start it with the command `/etc/init.d/ntpd start`. Otherwise, re-start it with the command `/etc/init.d/ntpd restart`. If there is a problem, submit a problem report. If the clock is still off, proceed with the next step.

- Check for the following message in `/var/log/messages`:

```
... ntpd[nnn]: synchronized to <NTS-IP>, stratum 1
```

If there is no message or the last message is old, this may suggest an Internet access problem to the NTS. Check for other messages tagged as `'ntpd[nnn]'`. They may point to the problem.

- If Internet access is permitted, consider adding extra NTS in `/etc/ntp.conf` for redundancy. After adding NTS, execute `/etc/init.d/ntpd restart` for your changes to take effect. If the clock is still off, submit a problem report.

6.5.3 Checking the Primary Processing Server Clock

These instructions assume you are logged in at the Operator Workstation console.

- Start an Internet Browser (Mozilla or Firefox) via the Application menu of the Desktop:

Desktop: Applications → Internet → ...

Enter this URL <http://www.usno.navy.mil/USNO>. The USNO Internet time is displayed.

- Open a Terminal Window and execute the following command

```
ssh modis@ps1 /users/gae/v4.0/tools/gmtclock
```

to display the system time of the primary processing server.

- Visually compare the time shown in the browser with the time shown in terminal window.

If the system time is off by more than 2 seconds, execute these steps:

- Telnet to the NTS/GPS unit and check its status (Section 9). If the NTS/GPS unit is not working properly, submit a problem report. Otherwise, login as root user on the primary processing server and proceed with the steps below.

- Verify the NTP daemon is running:

```
/etc/init.d/ntpd status
```

If it is not, start it with the command `/etc/init.d/ntpd start`. Otherwise, re-start it with the command `/etc/init.d/ntpd restart`. If there is a problem, submit a problem report. If the



clock is still off, proceed with the next step.

- Check for the following message in `/var/log/messages`:
... `ntpd[nnn]: synchronized to <NTS-IP>, stratum 1`

If there is no message or the last message is old, this may suggest an Internet access problem to the NTS. Check for other messages tagged as `'ntpd[nnn]'`. They may point to the problem.

- If Internet access is permitted, consider adding extra NTS in `/etc/ntp.conf` for redundancy. After adding NTS, execute `'/etc/init.d/ntpd restart'` for your changes to take effect. If the clock is still off, submit a problem report.

6.5.4 Checking the Backup Processing Server Clock

These instructions assume you are logged in at the Operator Workstation console.

- Start an Internet Browser (Mozilla or Firefox) via the Application menu of the Desktop:

Desktop: Applications → Internet → ...

Enter this URL <http://www.usno.navy.mil/USNO>. The USNO Internet time is displayed.

- Open a Terminal Window and execute the following command

```
ssh modis@ps2 /users/gae/v4.0/tools/gmtclock
```

to display the system time of the back processing server.

- Visually compare the time shown in the browser with the time shown in terminal window.

If the system time is off by more than 2 seconds, execute these steps:

- Telnet to the NTS/GPS unit and check its status (Section 9). If the NTS/GPS unit is not working properly, submit a problem report. Otherwise, login as root user on the back processing server and proceed with the steps below.

- Verify the NTP daemon is running:

```
/etc/init.d/ntpd status
```

If it is not, start it with the command `'/etc/init.d/ntpd start'`. Otherwise, re-start it with the command `'/etc/init.d/ntpd restart'`. If there is a problem, submit a problem report. If the clock is still off, proceed with the next step.

- Check for the following message in `/var/log/messages`:
... `ntpd[nnn]: synchronized to <NTS-IP>, stratum 1`

If there is no message or the last message is old, this may suggest an Internet access problem to the NTS. Check for other messages tagged as `'ntpd[nnn]'`. They may point to the problem.

- If Internet access is permitted, consider adding extra NTS in `/etc/ntp.conf` for redundancy. After adding NTS, execute `'/etc/init.d/ntpd restart'` for your changes to take effect. If the clock is still off, submit a problem report.



6.5.5 Checking the NAS Server Clock

Because access to the vault is restricted and remote log in to the NAS is not allowed, the NAS clock is checked indirectly. These instructions assume you are logged in at the Operator Workstation console and that its clock has been checked (Section 6.5.2).

- Open a Terminal Window and execute the following commands

```
date; touch /nas0/SEADAS/file  
/bin/ls --full-time /nas0/SEADAS/file  
rm /nas0/SEADAS/file
```

The touch command creates a file on the NAS via its CIFS/NAS file system. The creation date for this file is set by the NAS itself. Thus, comparing the creation time with the operator workstation time displayed by the date command provides an indirect way to check the NAS clock. If the system time is off by more than 2 seconds, the NAS system clock and the NTS settings need to be checked directly via the NAS console.

6.6 Security

All users on all the computers comprising the ES system are password protected and each user has its screen (console) saver locking mechanism enabled. The screen saver locking timeout is user-configurable. All VNC servers are password protected. Access to the iDRAC for remote management is password protected.

Mounting the NAS partitions on the workstation and processing servers requires the password of the NAS administrator to be specified in the NAS entries in the file `/etc/fstab`. As a security precaution, this file has been made readable only by the root user.

In order for the operators to perform their tasks, SSH password less remote access was granted between various users on the ingest server and the processing servers.

The firewall is enabled on the servers, the workstation, and the NAS server. SSH is a trusted service on the Linux machines. FTP is also a trusted service on the operator workstation and the processing servers. The FTP service is needed on the processing servers in order to receive data from the ingest server. The Security Enhanced Linux (SELinux) is also enforced. The security configuration is accessed with the command:

```
/usr/bin/system-config-securitylevel
```

6.7 Remote Management

The remote management is done via the integrated Dell Remote Access Controller (iDRAC) installed on each server. To access the iDRAC, start a Web browser:

Applications → Internet → Firefox Web Browser

Enter the iDRAC IP address of the server you wish to access and log in as user Admin. The figure on the following page shows the Remote Access Controller Web page. In this page you can cycle the power, access the system event logs, check the server health, etc. A comprehensive help is available with the Help button shown on this page. The system has been delivered with a CD containing the Dell Remote Management software that can be installed on a Windows PC.



6.8 Antivirus

6.8.1 Manual Scan

The AutoProtect function of the Symantec antivirus software installed on Linux OS has been disabled. This function scans all I/O paths (SCSI, SAS, Ethernet, USB, etc.) for viruses. Running this function would have a detrimental impact on the MODIS ingestion and processing because of the high data rate during the ingestion. However, scanning of specific folders on the drives can be performed, either manually or automatically via cron jobs. The manual scan is done as follows:

```
# Manual Scanning
# /opt/Symantec/symantec_antivirus/sav manualscan -s <directory>
# --> Reports no info to terminal, check /var/symantec/Logs/<date>.log
# It is up to each site to come up with a schedule to
# perform the manual scans on a routine basis.
```



The following table lists the directories where new data is downloaded from the Internet.

Frequency	Computers	Directory	Description
Daily	ins, ows, ps1, ps2	/users/gae/oestools	Orbital Elements
As required by processing	ows, ps1, ps2	/usr/local/seadas/7.3/var/modis	Ancillary data for navigation
As required by processing	ows, ps1, ps2	/nas0/SEADAS/ancillary	Ancillary data for processing
Daily	ows, ps1, ps2	/usr/local/seadas/7.3/run/var/modisa /usr/local/seadas/7.3/run/var/modist	Ancillary data for processing
As required	ins, ows, ps1, ps2	/users/gae/patch	Global Imaging Patches

These files are strictly data files. However, GI patch files may contain executables in a compressed tar file.

For details on the Symantec antivirus for Linux software, refer to the files SAV_Linux_Client.pdf and SAV_Linux_Impl.pdf located in the Manual/Symantec/ folder on the GI-MODIS installation DVD.

6.8.2 Virus Definitions Download

By default the anti-virus definitions are downloaded weekly at 20:00 UTC. If you wish to download daily at 11:32 UTC instead, execute the following commands as user root:

```
cd /opt/Symantec/symantec-antivirus
./sav liveupdate -s -f daily -i 11:32 -m 1
./sav liveupdate -v
```

The virus definitions download is shown in the log files /var/symantec/Logs/**MDhm**.log:

```
..., "Symantec AntiVirus services shutdown was successful.",...
..., "New virus definition file loaded. Version: 120730b.",...
..., "Symantec AntiVirus services startup was successful.",...
```



7 Software Maintenance

This section describes the tasks necessary to maintain the ESC system.

7.1 System 9000 Software Backup

The Red Hat Enterprise Linux Version 4 has been installed on the ingest server along with the GI System 9000 software. The Red Hat Enterprise Linux Version 6 has been installed on the processing servers and the operator workstation along with the GI System 9000 software.

System 9000 consists of programs, scripts, and databases distributed among the users `gae`, `modis`, and `seadas`. User `gae` contains the orbital elements and various generic programs and scripts. User `modis` performs the scheduling, tracking, data ingestion and the sectorization. User `seadas` performs the NASA MODIS SeaDAS processing, whose software is located in the directory `/usr/local/seadas`. In addition to these three users, various files in `/etc` have been customized and the TFSB/SCSI driver was installed in `/usr/src/tfsb-1.0`. This driver interfaces with the GSI unit.

Prior to shipping, a backup of the users, `/etc` files, and the TFSB/SCSI driver, will be performed and stored on the NAS server. It is recommended you perform such a backup once the on-site configuration is done and the system is operational. To perform such a backup, log in as user `root` and execute the command

```
/users/gae/pub/save_users
```

The backup tar files are located in `/home/Saved_<hostname>`, copy this directory to `/nas0` of the NAS server for safe-keeping. The sections below describe the user's backup operations on the machines comprising the system.

Note that `/usr/local/seadas` containing the NASA MODIS SeaDAS software is not backed up with the script `save_users`. However, it is exactly the same on the operator workstation and the processing servers.

7.1.1 Backup System 9000 on Ingest Server

Log in as user `root` on the ingest server and execute the script `/root/save_users_to_nas0`. This script contains the following commands:

```
export name=Saved_`hostname`  
/bin/rm -rf /users/$name  
/users/gae/pub/save_users  
ssh root@ows /bin/rm -rf /users/$name /nas0/users/$name  
scp -r /users/$name root@ows:/users  
ssh root@ows /bin/cp -r /users/$name /nas0/users  
ssh root@ows /bin/rm -rf /users/$name  
/bin/rm -rf /users/$name
```

The directory `Saved_`hostname`` is sent to `/users` of workstation first because of potential problems with SCPing to a mounted NAS partition. From there, the directory is copied to the NAS partition (`/nas0`).



7.1.2 Backup System 9000 on Workstation or Processing Servers

Log in as user *root* on the workstation or one of the processing servers and execute the script `/root/save_users_to_nas0`. This script contains the following commands:

```
export name=Saved_`hostname`  
/bin/rm -rf /users/$name /nas0/users/$name  
/users/gae/pub/save_users  
/bin/cp -r /users/$name /nas0/users  
/bin/rm -rf /users/$name
```

7.2 Installing a System 9000 Patch

A System 9000 upgrade/patch is delivered in a file of the form `yyMD[X].gpf` where `yy` is the last two digits of the year, `mm` is the month and `dd` is the day of the month. `X` is an uppercase letter to differentiate the updates posted on the same day. The patch files are in:

<ftp://ftp.globalimaging.com/global/S9000/>
<ftp://ftp.globalimaging.com/global/S9000/Linux>

The GPF file is a tar file containing:

- `yyMD[X].doc`: description and installation instructions (ASCII file)
- `yyMD[X].lis` : list of files or folders tarred to the .tgz file
- `yyMD[X].tgz` : compress tar ball of the patch files
- `yyMD[X].tfl` : list of files in .tgz file
- `yyMD[X].pin` : patch information file

The patch is downloaded and installed with the command `GPF_install`. If this command is not in the folder `/users/gae/patch`, skip to section 7.2.2.

7.2.1 Install a patch with `GPF_install`

To install a patch with `GPF_install`, log on as user *root* on the appropriate machine and execute the following commands:

```
cd /users/gae/patch  
# If you do not have access to ftp.globalimaging.com from  
# this machine, download the patch from another computer  
# and copy it to this folder.  
./GPF_install -query yyMD[X]
```

The patch file is downloaded from one of the sources mentioned above if it is not already in the folder. When the `-query` is given on the command line, the patch is downloaded, its components are extracted but it is not installed. This modifier is used to check if the patch requires a manual installation and/or customization. If the line `Installation: Automatic` is displayed, execute the following command to install the patch:

```
./GPF_install yyMD[X]
```

If the line `Installation: Manual` and/ or `Customization: Required` is displayed, follow the instructions in `yyMD[X].doc`.



When installing a patch with `GPF_install`, a backup of the local files listed in `yyMD[X].lis` is done prior to installing the patch and is stored as `yyMD[X].bgz`.

Re-start any program that has been updated by this patch. If the patch contains `dcim.x` or `nodcim`, re-start the GAE terminal windows such as `GWARDI`, `GWARDP`, `GAE-FOCUS`, etc. If the patch contains `STracker`, stop it.

7.2.2 Install a patch without `GPF_install`

To install a patch without `GPF_install`, log on as user `root` on the appropriate machine and follow these instructions:

- Stop any program that is being updated by this patch. If the patch contains `dcim.x` or `nodcim`, stop the GAE terminal windows such as `GWARDI`, `GWARDP`, `GAE-FOCUS`, etc. If the patch contains `STracker`, stop it.
- Download and copy the patch file to the folder `/users/gae/patch`
- Login as `root` user and execute the following commands:

```
cd /users/gae/patch
tar xvzf yyMD[X].gpf
```

- Check `yyMD[X].pin` for the line '*Installation: Automatic*'. If this line is in the file, execute the following commands:

```
cd /users/gae/patch
tar xvf yyMD[X].tgz -C /users
```

- Check `yyMD[X].pin` for the lines '*Installation: Manual*' or '*Customization: Required*'. If either of these lines is in the file, follow the instructions in `yyMD[X].doc`.

Restart the program(s), GAE terminal window(s), and `STracker` if affected by the patch.

7.3 Problem Reporting

Problem reporting will be done mainly by DND operators and is also described in the Operator's Manual (RD-02). To report a problem, connect to IES's implementation of the Open Technologies Real Services (OTRS) by starting a Web browser and entering the following location:

<https://www.iescweb.com/customer>

You will need a user name and password. Problems are reported through an intuitive Web interface. Attach the relevant log files, or extract thereof, to expedite the problem resolution. Immediately after it is completed, the operator will receive an e-mail confirmation of the reported problems. Thereafter, each change to the problem report is easily tracked internally at IES and by DND personnel each receiving e-mail updates. The OTRS manual can be accessed with the file `OTRS Quick Guide for Customer Interface.pdf` located in the latest PE-ESC Maintenance DVD.

If the problem requires the repair of Dell equipment you will be asked to contact Dell for support. The number in Canada is 1-800-387-5757.



7.4 Remote Monitoring

The implementation of the remote monitoring functionality described below requires authorization from DIM Secur and the configuration of the GPNet routers in order to permit the associated network traffic. Please contact your ISSO or ES LCMM to determine if this functionality is available for use.

Remote monitoring will be initiated mainly by DND operators and is described in the Operator's Manual (RD-02). The remote monitoring is done by establishing a tunnel to GI/IES from DND. This tunnel gives GI/IES access to the operator workstation. From there, GI/IES personnel can monitor the ES system in order to analyze the problem.

The operator and GI/IES personnel must exchange passwords before establishing a tunnel. It is recommended that a mechanism be implemented by DND to use a temporary password for user seadas on the operator workstation for the duration of the remote session. Once the session is terminated, the password can be reset to its original value.

7.5 Red Hat Enterprise Linux Updates

Red Hat Enterprise Linux updates are available for user with a subscription to Red Hat support. Once the computers running RHEL are registered, you can update RHEL on your system. Red Hat maintains RHEL5 and RHEL6 but no longer maintains RHEL4.

The updates can be installed manually at regular intervals to keep RHEL up to date or only the updates pertaining to security can be installed. These two methods are discussed below.

Regular Updates

To update RHEL on your system by logging in as *root* user on each machine running RHEL 5 or 6 and executing the following command

```
yum update
```

It is recommended you run this command once a month or a security update is published. Note that updates to the kernel necessitate a system reboot to take effect. Execute the following commands to ascertain if a reboot is necessary

```
rpm -qa | grep kernel  
uname -r
```

If the output of the first command indicates a newer kernel revision number than the number shown with the second command, a reboot is necessary.

Security Updates

As an alternative, GI/IES has developed a procedure to handle only security update issues through OTRS which allows GI/IES to take the required corrective action with third party support groups and implement a proper resolution to the update issue.

- 1) GI/IES receives the Red Hat update notices. Upon receipt of a security issue, GI/IES opens a ticket in OTRS in the Minor category and assesses the impact of the security updates on the ES system operation. The assessment might include a required basic factory test on Red Hat computer at GI premises.



-
- 2) If the assessment results in No-Impact identified, the update will be authorized and DND will be informed through OTRS to proceed with the update and report on the operation of the system.
 - a. If the operation of the system is normal, close the ticket and exit the process
 - b. If there is a problem in the operation, DND team should undo the update and go through the next step.
 - 3) If the assessment results in a possible impact, or an operation problem appeared in step 2, the ticket category will be escalated to Major and will be handled as such.



8 Troubleshooting

The primary troubleshooting is done by the operator upon observation of a problem. The first type of problems concern the tracking, the ingestion, the distribution, or the automatic or manual processing chain. These problems will be observed by an absence of products or with specific messages in the ingestion, distribution, and processing logs. Refer to Section 5 in document RD-02 for details.

The second type of problems concerns access to a remote computer on the system and the download of the orbital elements. These problems are detected by the system alerts software running on the operator workstation. These problems are discussed in Sections 8.1 and 8.2 below.

The third type of problems relates to the Operating System, the daemon, or drivers running in the background. These problems may cause a disruption with the tracking, ingestion, distribution, or processing chain. Once diagnosed by IES personnel, Dell support will be contacted if needed.

The fourth type of problems relates to hardware malfunction or failure. Once diagnosed by IES personnel, Dell support will be contacted if Dell hardware is involved. Otherwise, the spare carried by DND will be used to allow the repair of the defective hardware.

Sections 8.3 through 8.8 describe the following checks that can be done on the system:

- Checking the antenna control chain
- By-passing the Fiber Optic Serial Link
- Checking the IF chain
- Checking the IF signal
- Checking the demodulated signal
- Miscellaneous Problems

Once a software component has been isolated as the cause of the problem, the administrator can perform the corrective maintenance. Once a hardware component has been isolated as the cause of the problem, the administrator or technician can perform the corrective maintenance (Section 9).

Throughout this section, consult Section 7.3 when asked to submit a problem report.

8.1 System Alert

The system alert messages are output by the script `sds_ops_system_alert` running as a cron job of user `seadas` on the operator workstation. These messages are logged in the file `/users/seadas/alert.log` on the operator workstation and are shown in a pop-up window.



Consult the log to determine if there is any error with the script or with the commands used in the script. If there is an error, submit a problem report. Otherwise, consult the troubleshooting tips below for each system alert message.



- **Problem PINGing nts**
 - Check if you can ping the ingest server. If not, consult the network administrator. Otherwise request the administrator or technician at the remote site to perform the remaining steps.
 - Switch Internet cable and try again.
 - Refer to “NTS/GPS Unit” in Section 9 for maintenance.
- **Problem PINGing ins**
 - Check if you can ping the NTS. If not, consult the network administrator. Otherwise request the administrator or technician at the remote site to perform the remaining steps.
 - Check if the ingest server is powered and booted. If not powered or booted, do so.
 - Switch Internet cable, check the status of ‘eth0’, and try again.
 - If there is still a problem, submit a problem report.
- **Problem PINGing ps1**
 - Check if you can ping the backup server. If not, consult the network administrator. Otherwise request the administrator to perform the remaining steps.
 - Check if the primary processor is powered and booted. If not, powered or booted, do so.
 - Switch Internet cable, check the status of ‘eth0’, and try again.
 - If there is still a problem, submit a problem report.
- **Problem PINGing ps2**
 - Check if you can ping the primary server. If not, consult the network administrator. Otherwise request the administrator to perform the remaining steps.
 - Check if the backup processor is powered and booted. If not, powered or booted, do so.
 - Switch Internet cable, check the status of ‘eth0’, and try again.
 - If there is still a problem, submit a problem report.
- **Problem PINGing nas**
 - Check if you can ping the primary or backup server. If not, consult the network administrator. Otherwise request the administrator to perform the remaining steps.
 - Check if the NAS is powered and booted. If not, powered or booted, do so.
 - Switch Internet cable, check the status network connection, and try again.
 - If there is still a problem, submit a problem report.
- **Problem accessing /users/modis on ins**
 - Check if there is enough space of the file system containing /users/modis. If not, contact IES for clean-up instructions. Otherwise, submit a problem report.



- **Problem accessing /users/seadas on ps1|ps2|ows**

On ps1, ps2 or ows:

- Check if there is enough space of the file system containing /users/modis. If not, contact IES for clean-up instructions. Otherwise, submit a problem report.

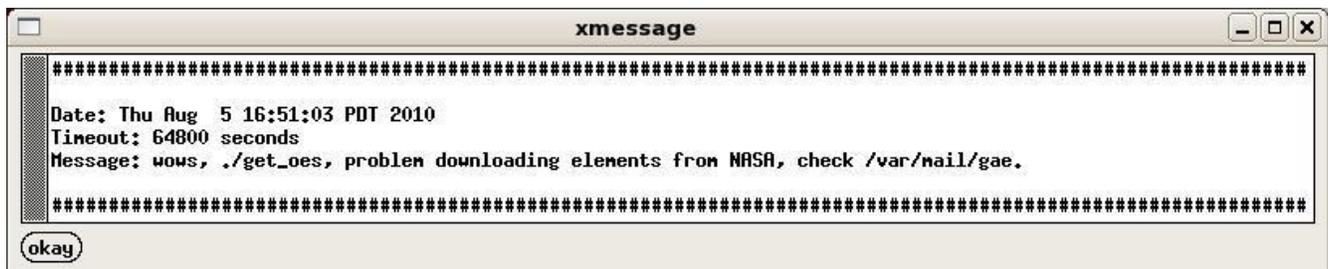
- **Problem accessing /nas0|nas1/SEADAS on ps1|ps2|ows:**

On ps1, ps2, or ows:

- Check if /nas0 is mounted. If not, do so.
- Check if /nas1 is mounted. If not, do so.
- Check if /nas0/SEADAS directory exists. If not, create it.
- Check if /nas1/SEADAS directory exists. If not, create it.
- Check if there is enough space on /nas0 and /nas1. If not, contact IES for clean-up instructions. Otherwise, submit a problem report.

8.2 Orbital Elements Download Alert

The orbital elements are downloaded daily from a NASA FTP site with the script `get_oes` running as a cron job of user `gae`. The output of the cron job is reported in the mail file `/var/mail/gae` on the computer running `get_oes`. If there is a download failure, an error message is shown in a pop-up window.



In the message above, `wows` indicate the west site operator workstation as the computer generating the message. It is followed by the script name and the message itself.

The following checks will help you find why the orbital elements in `/users/gae/oestools/tle.txt` are not current. The commands in this section are executed as root user on the machine experiencing the problem.

- Verify that `get_oes` is executed daily with the following command:

```
crontab -u gae -l
```

If there is no entry for `get_oes`, refer to Section 5.3.6, 5.4.6, or 5.5.6 to add one.

- Check the mail file `/var/mail/gae` for error messages. If there is no error, it is possible that the elements on the NASA Orbital Elements FTP site were not updated. In this case, submit a problem report.



- If there are errors, execute `get_oes` manually with the following command:

```
sudo -u gae /users/gae/oestools/get_oes nasa
```

If there is a problem, submit a problem report.

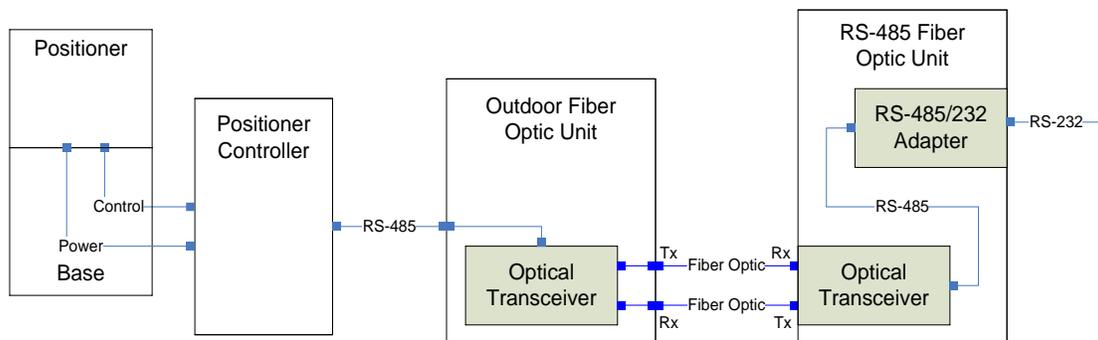
- If there was no error downloading the elements manually, check the age of the elements. If they are current, this indicates the problem with downloading the elements may be occasional. Monitor `/var/mail/gae` for the next 4-5 days. If the problem persists, submit a problem report.

8.3 Checking the Antenna Control Chain

This section describes how to check the antenna control (serial) chain in the event there is a communication problem between the ingest server and the antenna positioner.

The antenna control chain, shown below, consists of the following elements:

- Serial cable from ingest server to RS-485 Fiber Optic (FO) unit
- RS-485 FO unit
- FO cables and their connectors
- Outdoor FO unit
- Serial cable to positioner controller
- Positioner controller unit
- Positioner control cable and positioner power cable
- Positioner



Perform the following checks on the RS-485 FO unit (Section 9.1.3.1) in the ingest rack:

- Verify that the serial cable from the ingest server to the RS-485 FO unit is secure.
- Verify that the power cable to the RS-485 FO unit is secure.
- Verify that the RS-485 transceiver is powered.
- Verify that the dual mode FO optical cables are secure and in their appropriate sockets.

Ask the operator to stop STracker+ and perform the following tasks in the radome:

- Open the radome hatch. This step powers off the antenna.
- Insert the by-pass key in the red socket on left side of the radome hatch to power the antenna.
- Disconnect the power cable to the positioner controller and measure its voltage. If the voltage is less than 140V, submit a problem report. Otherwise, reconnect the power cable to the positioner controller.



- Disconnect the power cable to the outdoor FO unit and measure its voltage. If the voltage is less than 110V, submit a problem report. Otherwise, reconnect the power cable to the outdoor FO unit.
- Verify that the dual mode fiber optic cables are secure and in their appropriate sockets.
- Verify that the serial cable between the FO unit and the positioner controller is secure.

Ask the operator to start STracker+ and track the SUN or point the antenna. If there is still a communication problem, submit a problem report.

- Remove the by-pass key in the red socket on the left side of the radome hatch to power off the antenna.
- Close the radome hatch. This step powers the antenna.

Ask the operator to re-start STracker+ and track the SUN or point the antenna. If there is still a communication problem, submit a problem report. If necessary, you will receive custom instructions to check specific components of the chain. Here is the usual check order:

- By-pass Fiber Optic Serial Link (Section 8.4).
- Check the positioner controller.
- Check the RS-485 transceiver in the output FO unit (Section 9.1.2.4).
- Check the RS-485 transceiver in the indoor FO unit (Section 9.1.3.2).
- Switch to a spare dual mode fiber optic cable pair.

8.4 *By-passing the Fiber Optic Serial Link*

In the event there is a communication problem between the ingest server and the antenna positioner, the technician can test the antenna positioner directly with the Laptop PC and the serial cable listed in the “System Test Equipment” sheet of the System Configuration Items document (RD-07).

Follow these steps to by-pass the fiber optic serial link:

- Ask the operator to stop STracker+.
- Open the radome hatch. This step powers off the antenna.
- Disconnect the serial cable from the antenna controller unit.
- **Position yourself outside the radome hatch and the PC inside the radome.**
- Connect the PC to the antenna controller with the serial cable supplied with the PC.
- Insert the by-pass key in the red socket on the left side of the radome hatch to power the antenna.
- Insert the licence dongle in a USB slot and power the PC.
- Log in as user *modis* and click on the STracker+ icon. The antenna will go through its initialization sequence.
- If successful, interface with the positioner controller using the STracker+ Antenna menu to point to a particular position or to track the sun.

If the antenna does not behave correctly, there is a problem with the positioner controller or the positioner itself. In this case, submit a problem report describing the error messages shown in STracker+ log on the PC. If the antenna behaves correctly, there may be a problem with the following components:

- Outdoor Fiber Optic Interface Assembly



- Dual mode fiber optic cables or connectors
- Indoor RS-485 Fiber Optic unit or its connection to the ingest server

Submit a problem report describing the error messages shown in STracker+ log on the ingest server. You will receive custom instructions to further troubleshoot the problem.

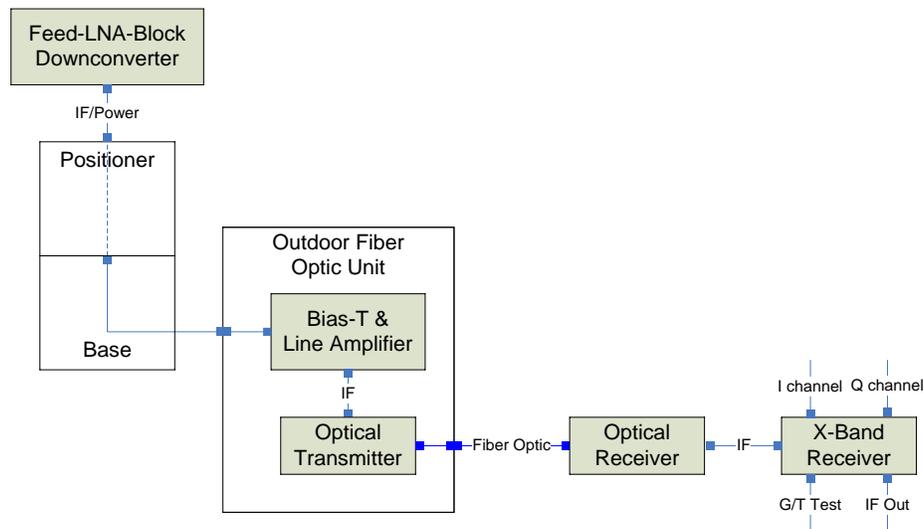
Follow the instructions below to re-establish the fiber optic link:

- Stop STracker+.
- Remove the by-pass key in the red socket on the left side of the radome hatch to power off the antenna.
- Shutdown the PC.
- Remove the serial cable between the PC and the positioner controller.
- Connect the serial cable from the positioner outdoor fiber optic interface assembly to the antenna controller.
- Close the radome hatch. This powers the antenna.

8.5 Checking the IF Chain

This section describes how to check the IF chain in the event the “Feed OK” light of the X-Band receiver is not on. The IF chain, shown below, consists of the following elements:

- X-Band receiver
- IF Fiber Optic (FO) unit
- IF FO cable and its connectors
- Outdoor FO unit
- IF cable from outdoor FO unit to positioner
- IF cable from positioner to Feed/LNB assembly
- Feed/LNB Assembly



Perform the following checks on the IF FO unit (Section 9.1.3.2) in the ingest rack:

- Verify the IF FO unit is powered and the “Power on” and “Optical Power” lights of the FO receiver are on.



- Verify that the IF (single mode) fiber optic cable is secure.
- Verify the IF cable from the IF fiber optic receiver to the X-Band receiver is secure.

Ask the operator to stop STracker+ and perform the following checks in the radome:

- Open the radome hatch. This step powers off the antenna.
- Insert the by-pass key in the red socket on the left side of the radome hatch to power the antenna.
- Disconnect the power cable to the outdoor FO unit and measure its voltage. If the voltage is less than 110V, submit a problem report. Otherwise, reconnect the power cable to the outdoor FO unit.
- Verify that the single mode fiber optic cable is secure.
- Verify that the IF cable from the positioner to the outdoor fiber optic unit is secure.
- Verify that the IF cable from the side of the positioner to the Feed/LNB is secure.

If the “Feed OK” of the receiver is still off, submit a problem report. If necessary, you will receive custom instructions to check specific components of the chain. Here is the usual check order:

- Check X-Band Receiver.
- Check optical receiver in indoor IF FO unit.
- Check voltage to the Feed/LNB.
- Check optical transmitter in outdoor FO unit.
- Switch to a spare single mode fiber optic cable.

8.6 Checking the IF Signal

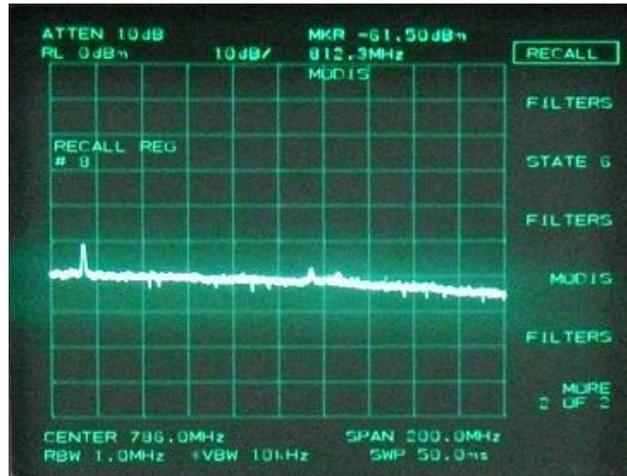
The IF from the Feed/LNB assembly can be tested with a spectrum analyzer at three points:

- IF out connector on the back of the X-Band receiver.
- IF out connector on the back of the indoor IF FO unit.
- IF out of the Bias-T & Line Amplifier unit located inside the outdoor fiber optic assembly in the radome. **Do not attempt to check the IF in the radome unless directed by IES/GI personnel.**

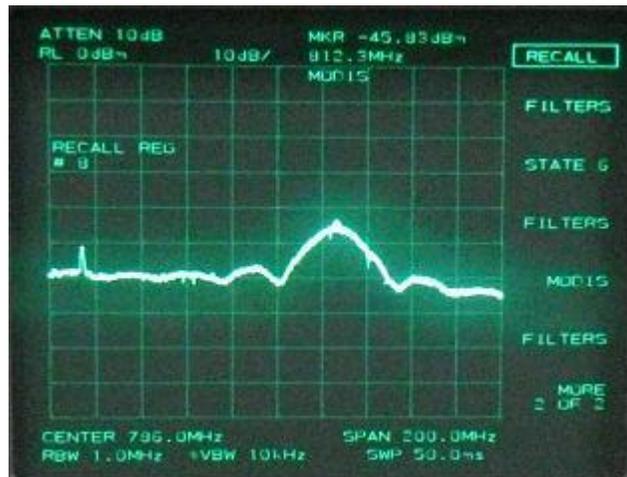
The spectrum analyzer settings are:

- Center frequency is 786MHz.
- Span 250 MHz
- Resolution Bandwidth is 1.0 MHz
- Video Bandwidth is 10.0 KHz
- Attenuation is 10dB
- Sweep is 50msec
- Amplitude Resolution 10db per division

The figure below shows the signal with the antenna stowed.



The next two figures depict the signal when tracking Terra and Aqua respectively.



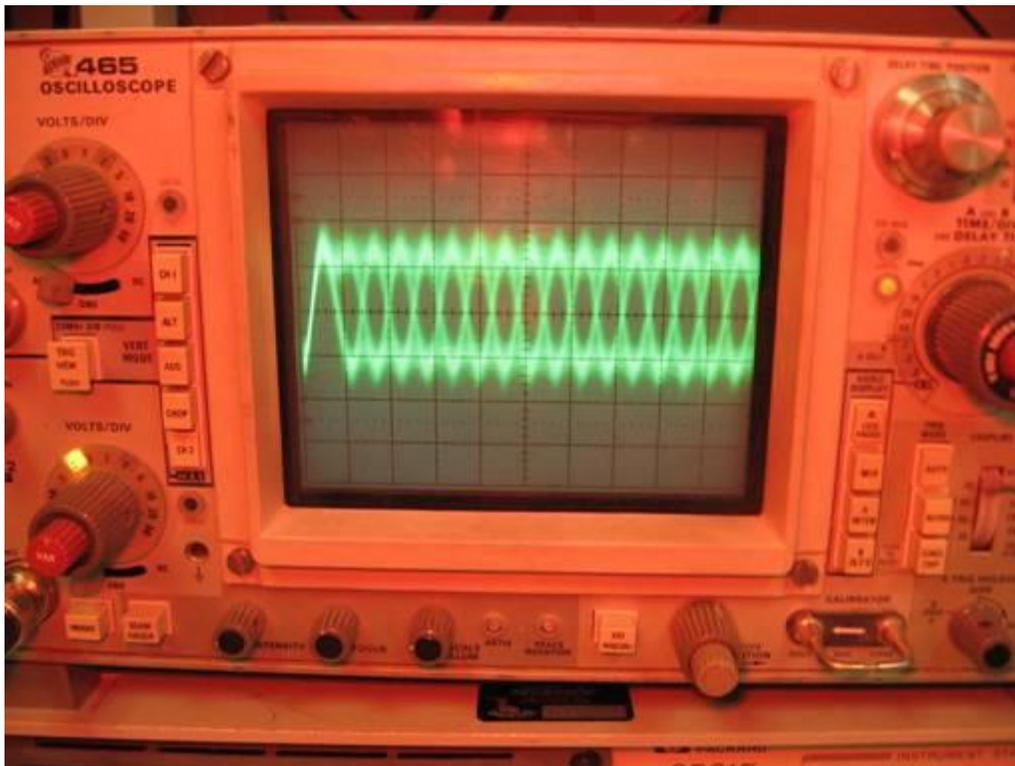
8.7 Checking the Demodulated Signal

The X-Band receiver outputs an I and Q signal to the GSI unit for Terra DB and only the I signal for Aqua DB. The demodulated signal can be observed with an oscilloscope

Follow these steps:

- Split I signal from receiver and connect to the GSI unit and to channel A of the oscilloscope.
- Split Q signal from receiver and connect to the GSI unit and to channel B of the oscilloscope.

The oscilloscope settings are .2 volt/division and .1 microsecond/division. The figure below shows an example of the I signal for Aqua. The Q signal is similar.



8.8 Miscellaneous

8.8.1 Loss of power to the server rack

Once the cause of a loss of power to the server rack has been determined and fixed, follow the start-up procedure in the order listed in Section 6.2 to re-start the components in the rack. Additionally, verify that the NAS server has booted correctly and its file system is not damaged before proceeding with the boot of the processing servers. Once the processing servers have booted verify that access to the NAS drives is allowed and the processing resumed normally. The operator workstation may also need to be re-booted for the workstation to access to the NAS drives.



9 Hardware Maintenance

The hardware maintenance is minimal. The indoor equipment needs to be dust free. Because the operator workstation is located in an area where DND personnel are frequently present, the inside of the workstation may require yearly cleaning. The remainder of the indoor equipment should not require yearly cleaning. The outdoor equipment has been sealed and is designed to operate without regular maintenance.

The corrective maintenance at the remote site requires the equipment listed in the “System Test Equipment” sheet of the System Configuration Items document (RD-07). Consult document RD-03 for a description of the hardware components. Note that some corrective maintenance may require custom instructions from the manufacturer.

Throughout this section, consult Section 7.3 when asked to submit a problem report. The IES technician will help DND’s personnel diagnose the problem and contact the manufacturer of the equipment if needed.

9.1 Remote Site

9.1.1 Radome

In some instances, weather conditions cause snow and/or ice to accumulate on the radome. It is recommended to visually inspect the outside of the radome after a storm and to use the rope hanging from the top of the radome to remove the accumulated snow or ice.

Periodic inspection of the radome should be performed annually after the radome has been installed. Of particular importance is the sealing of the panel caps and joints. Consult the maintenance section of the L-3 ESSCO Installation, Operations & Maintenance Manual for details.

9.1.2 Working in the Radome

The radome is equipped with a safety switch that causes the antenna controller to power off when the radome hatch is opened. The power is restored to the antenna controller once the hatch is closed.

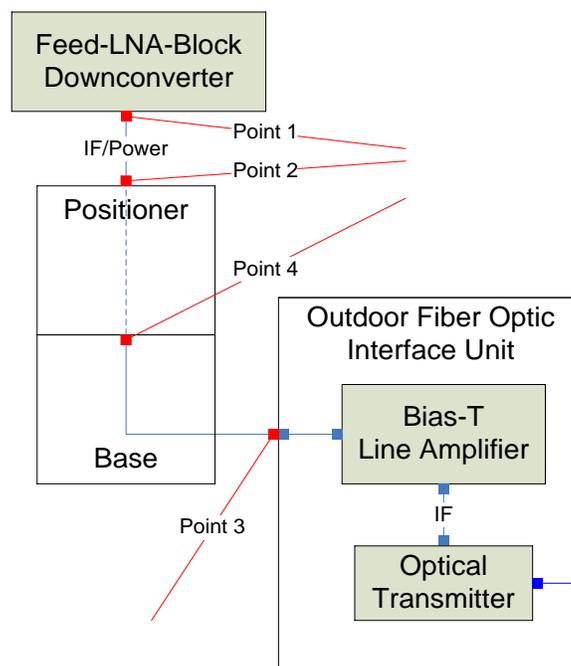
Once the power is restored, the antenna controller will not accept commands until it has been re-initialized. This initialization is done when STracker+ starts or at the beginning of a pass. In both cases, once the initialization is done, a ‘homing’ sequence is performed to align the antenna.

9.1.2.1 Feed/LNB

The Feed/LNB, shown below, is maintenance free.



The Feed/LNB is powered from the outdoor IF FO unit and sends an IF signal to the FO unit. The Bias-T and Line Amplifier inside the FO unit provides the power to the feed. The figure on the next page shows the voltage test points:



Follow the steps below to check the voltage to the Feed/LNB from the output IF FO unit:

- Ask the operator to stop STracker+.
- Enter radome and close the hatch to power the positioner controller.
- Ask the operator to start STracker+ and points to horizon.
- Open radome hatch.
- Disconnect IF cable to Feed/LNB (point 1) and check voltage. Reconnect.
- If voltage is **incorrect**, disconnect IF cable to feed arm (point 2) and check voltage. Reconnect.
- If voltage is **incorrect**, disconnect IF cable to outdoor fiber optic interface unit (point 3) and check voltage. Reconnect.
- If voltage is **correct**, disconnect IF cable inside base (point 4) and check voltage. Reconnect.
- Report your observations.

Follow the steps below in the event the Feed/LNB needs to be replaced:

- Ask the operator to position the antenna to the horizon (0 degree elevation).
- Enter radome and close the hatch to power the positioner controller.



- Ask the operator to start STracker+ and points to horizon.
- Open radome hatch.
- Disconnect power to the fiber optic unit.
- Disconnect the cable on top of the Feed/LNB.
- **Measure the distance between the edge of the collar and the top of the feed.**
- Remove the bolts from the four (4) feed arms.
- Remove the feed.
- Loosen the collar and attach it to the new feed at the same distance as measured above.
- Connect the feed to the four feed arms.
- Connect the cable at the top of the feed.
- Power the fiber optic unit.

Once the feed has been replaced, check that the “Feed OK” light of the receiver is green and the receiver strength is greater than 4. If not, adjust the gain of the “Bias-T & line Amplifier” unit (Section 9.1.2.4). Otherwise, wait for passes from Terra and Aqua to ascertain that the reception is correct.

9.1.2.2 *Antenna Positioner*

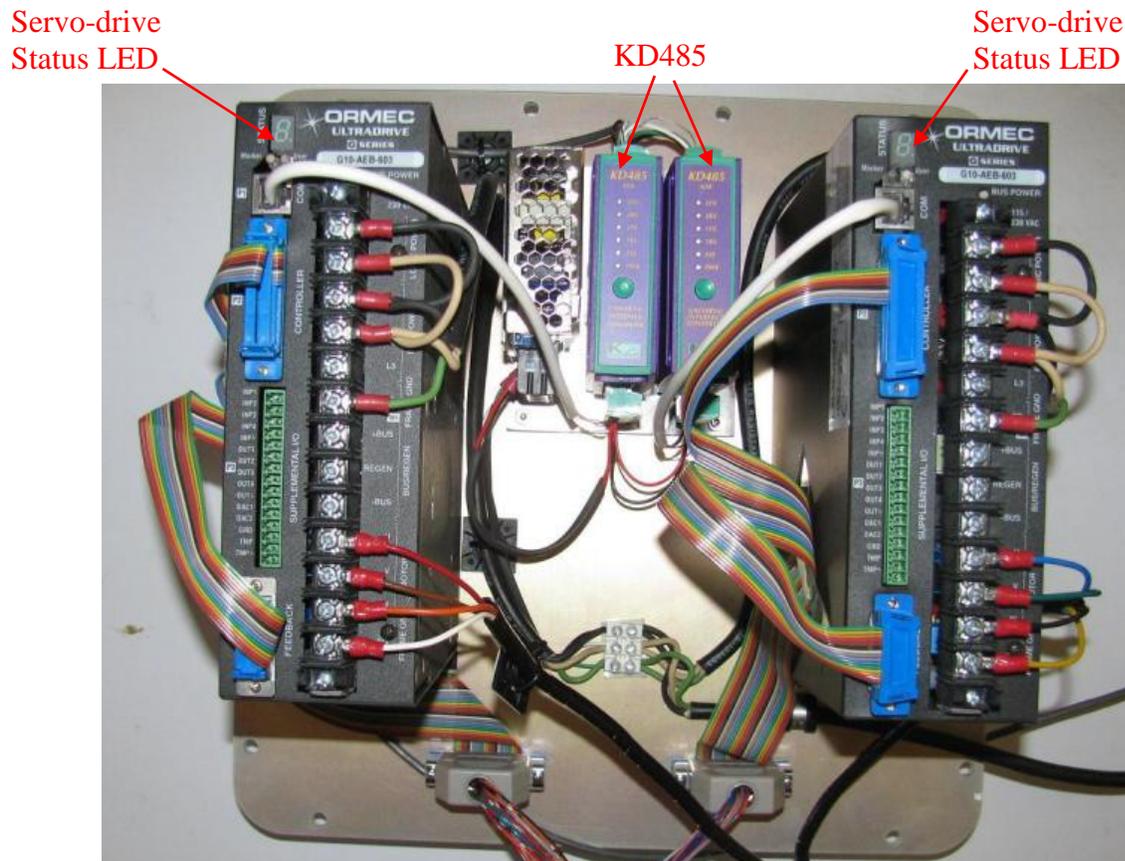
The antenna positioner is maintenance free. In the unlikely event the antenna positioner needs repair; specific instructions will be furnished by the manufacturer.

9.1.2.3 *Positioner Controller*

The positioner controller, shown below, is maintenance free.



The figure on the next page shows the inside of the positioner controller. Each motor is controlled with a servo-drive which receives commands from the ingest server via its KD485 unit. The power light of the KD485 should be on and the EXE light should be off. When a command is sent to the azimuth or elevation servo-drive the 1TX, 1RX, 2TX, and 2RX lights of the azimuth or elevation KD485 blinks. The status LED on the servo-drive displays a hexadecimal code. In the event of a servo-drive or motor failure, this hexadecimal code is used for troubleshooting.



If diagnostics need to be performed on the positioner controller, specific instructions will be furnished by the manufacturer. The diagnostics are performed while the antenna is running and should be done while in direct contact with a technician from the equipment manufacturer. A quick reference guide to the servo-drive is available at.

<http://www.ormec.com/LinkClick.aspx?fileticket=MDe30AOVEMQ%3d&tabid=127&mid=523>

or with in the file Ormec_Servodrive_Ref.pdf in the Manuals/Ormec/ folder on the GI-MODIS installation DVD. If the fault cannot be corrected, submit a problem report.

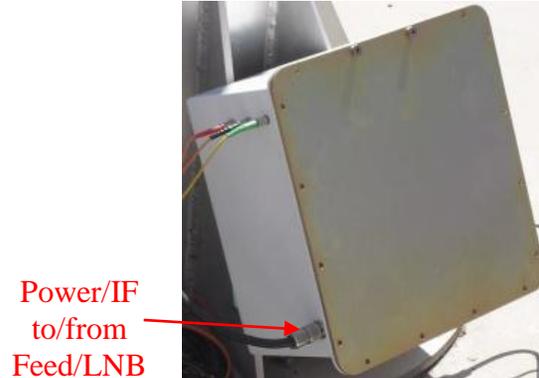
Follow the steps below in the event the Positioner Controller needs to be replaced:

- Ask the operator to stop STracker+.
- Enter the radome.
- Disconnect all cables to the positioner controller
- Replace the positioner controller with the new unit.
- Connect all cables.
- Power the positioner controller.
- Exit the radome.
- Ask the operator to start STracker+

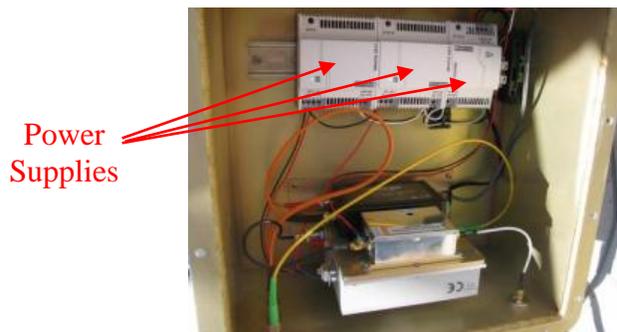
The positioner controller operates normally if the ANT status window on STracker+ shows green.

9.1.2.4 Fiber Optic Interface Assembly

The Fiber Optic Interface Assembly also known as the outdoor FO unit, shown below, is maintenance free.



The voltage output by the FO unit via the IF cable to the Feed/LNB should range between 12 and 15 volts. The figure below shows the interior of the outdoor FO assembly without the Electronic Thermal Control Unit. The DC/OK lights on the three power supplies should be on.



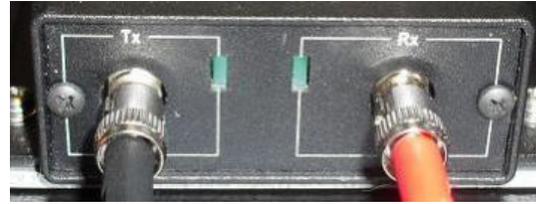
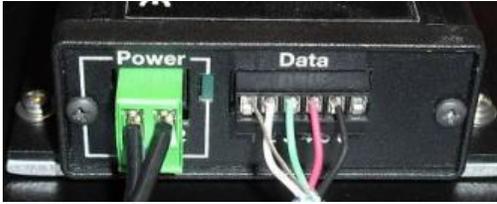
Within the Fiber Optic Outdoor Assembly is an Electric Temperature Controller. This unit monitors and displays the temperature within the antenna positioner using a wired sensor. The controller will turn on heater elements when the temperature falls below -10C and shut them off once the temperature reaches -4C. The heater elements are attached to both motor assemblies. There is also a heater element in the Fiber Optic Outdoor enclosure. The temperature should never be lower than -10C. The unit is shipped pre-programmed and does not require preventative nor corrective maintenance.

The “POWER ON” and “STATUS” lights of the FO transmitter, shown below, must be on. The “RF AT LASER” light of the FO transmitter must be amber.





The power light of the RS-485 transceiver, shown below, must be on. The Tx and Rx lights of the transceiver blink when data is received or transmitted.



The line amplifier that drives the laser diode of the fiber-optic link needs to be adjusted so that the RF system has its maximum dynamic range. The figure below shows the gain adjustment on the “Bias-T & Line Amplifier” unit. On the left side is the Power/IF line to the Feed/LNB. On the other side is the IF out to the FO transmitter. The IF output can be checked at this point with a spectrum analyzer.



Follow the steps below in the event the outdoor FO unit needs to be replaced:

- Make sure the antenna points to zenith.
- Ask the operator to stop STracker+.
- Enter the radome.
- Disconnect power to the fiber optic unit.
- Disconnect the fiber optic cables. **Make sure the ends are covered or stay clean.**
- Disconnect the remaining cables.
- Replace the fiber optic unit with the new unit.
- Connect all cables.
- Power the fiber optic unit.
- Wait 15 minutes for the electronics to warm up.

Once the unit has been replaced, disconnect the IF cable between the fiber optic assembly and the positioner, and check that the voltage output by the FO is 12 to 15 volts. Connect the IF cable.

Next, check that the “Feed OK” light of the X-Band receiver is green. If it is not, follow the steps below to adjust the gain of the “Bias-T & line Amplifier” unit:

- Remove the cover of the outdoor FO unit.
- Verify the DC/OK light on the three power supplies are on.
- Verify the “POWER ON” light of the FO transmitter is on.
- Verify the “STATUS” light of the FO transmitter is on.
- Turn the GAIN adjustment screw counter-clockwise until the “RF AT LASER” light is off.



- Next, turn the adjustment screw clockwise until the following occurs:
 - The “RF AT LASER” light of the FO transmitter turns amber. A red light indicates the signal is saturated (more than 15 dB gain). A green light indicates there is too much gain (additional 5 dB).
 - The “Power On” and “Optical Power” lights of the indoor FO receiver are on.
 - The FEED OK” light of the X-Band receiver is on.
 - The receiver strength shown on the LED of the X-Band receiver is more than 4.

If the “RF AT LASER” light of the FO transmitter turns red or green and the conditions above have not been achieved, submit a problem report.

- Replace the cover of the outdoor FO unit.
- Exit the radome.
- Ask the operator to start STracker+.

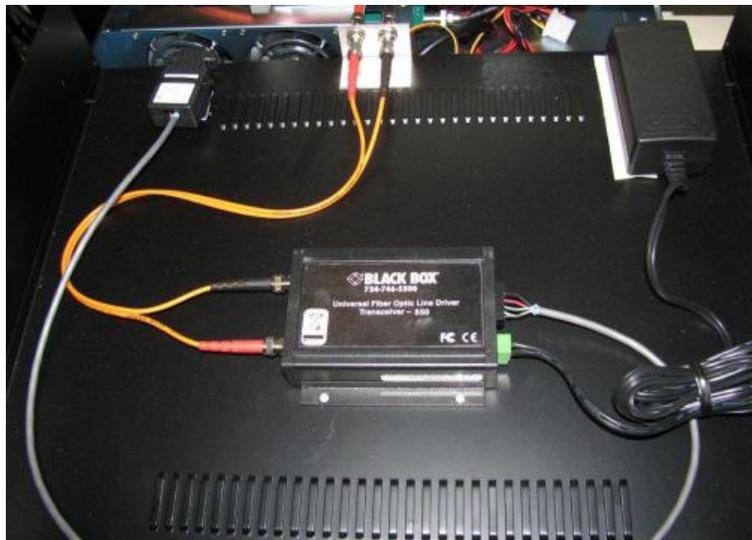
Next, wait for Terra and Aqua passes to ascertain that the reception is correct. If there is a reception problem, submit a problem report.

9.1.3 Indoor Downlink Electronics

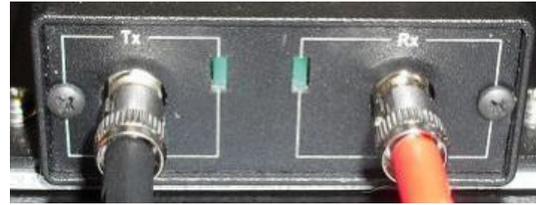
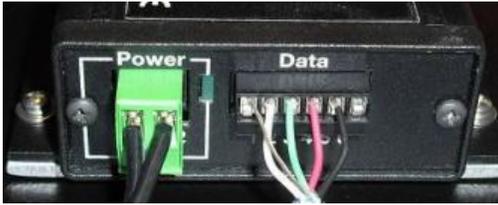
The following sections describe the corrective maintenance for the indoor electronics components.

9.1.3.1 RS-485 Fiber Optic Unit

The RS-485 FO unit, shown below, is maintenance free.



The figure below shows the inside of the unit with its RS-232/485 adapter, the FO transceiver (Black Box), and an AC/DC adapter. The power light of the RS-485 transceiver, shown below, must be on. The Tx and Rx lights of the transceiver blink when data is received or transmitted.



If you need to replace the RS-485 transceiver, specific instructions will be sent by the manufacturer of the RS-485 FO unit. Follow the steps below in the event the RS-485 FO unit needs to be replaced:

- Ask the operator to stop STracker+.
- Remove side panels of the rack in which the unit is mounted.
- Disconnect power to the unit.
- Disconnect the fiber optic cables. **Make sure the ends are covered or stay clean.**
- Disconnect the serial cable.
- Unscrew the unit and remove.
- Screw the new unit in place.
- Connect the serial cable.
- Connect the fiber optic cables.
- Connect and power the unit.
- Ask the operator to start STracker+

The RS-485 fiber optic unit operates normally if the ANT status window on STracker+ shows green. If the unit has a problem, submit a problem report.

9.1.3.2 IF Fiber Optic Unit

The IF Fiber Optic (FO) unit, shown below, is maintenance free.



The power lights on both power supplies must be on. The “Power On” and “Optical Power” lights of the FO receiver must be on. The figure below shows the back of the unit with the sockets for the FO cable and the IF cable to the X-Band receiver.





If you need to replace the FO receiver, specific instructions will be sent by the manufacturer of the IF FO unit. Follow the steps below in the event the IF FO unit needs to be replaced:

- Ask the operator to stop STracker+.
- Remove side panels of the rack in which the unit is mounted.
- Disconnect power to the unit.
- Disconnect the FO cable. **Make sure the ends are covered or stay clean.**
- Disconnect the IF cable.
- Unscrew the unit and remove.
- Screw the new unit in place.
- Connect the IF cable.
- Connect the FO cable.
- Connect and power the unit.
- Ask the operator to start STracker+

The IF FO unit is ready when the three power lights on its two power supplies are on and the “Power On” and “Optical Power” lights of the FO receiver are on. If these lights are off, adjust the gain of the “Bias-T & line Amplifier” unit (Section 9.1.2.4). Additionally, the “Feed OK” light of the X-Band receiver must be on and its strength greater than 4. If the “Feed OK” light of the receiver is off or the strength is 4 or less, adjust the gain of the “Bias-T & line Amplifier” unit (Section 9.1.2.4). Otherwise, wait for passes from Terra and Aqua to ascertain that the reception is correct.

9.1.3.3 X-Band Receiver

The X-band receiver is maintenance free. Some units have been supplied with a fan. However, they are unnecessary to the operation of the receiver. The figure below shows the front of the unit. To the left of the LED, a green “Feed OK” light indicates we have a signal from the Feed/LNB and a green “Rx LOCK” light indicates a receiver lock. The upper bar on the display indicates the relative receiver strength; the lower bar shows the frequency sweep. The sweep stops when locked to a signal and follows the Doppler shift. The satellite shown in yellow is the satellite currently programmed in the receiver.



The figure below shows the back of the receiver.



From left to right we have the following connections:

- IF from the IF FO unit.
- Q and I channels to the GSI unit.
- G/T Test to the GSI unit.
- IF OUT to check the signal with a spectrum analyzer.
- USB connection to the ingest server.

Follow the steps below in the event the X-Band receiver needs to be replaced:

- Ask the operator to stop STracker+.
- Remove side panels of the rack in which the unit is mounted.
- Power off the unit (switch above the power socket) and disconnect the power cable.
- Disconnect all cables.
- Unscrew the unit and remove.
- Screw the new unit in place.
- Connect all cables.
- Connect and power the unit.
- Ask the operator to start STracker+

The X-Band receiver interface operates normally if ACQ status window on STracker+ shows the receiver information. Check that the “Feed OK” light of the receiver is green, the strength is more than 4, and the frequency sweeps between -50 and 50. If the “Feed OK” light of the receiver is off or the strength is 4 or less, adjust the gain of the “Bias-T & line Amplifier” unit (Section 9.1.2.4). Otherwise, wait for passes from Terra and Aqua to ascertain that the reception is correct.

9.1.3.4 GSI Unit

Overheating is one of the main sources of the GSI unit power supply breakdown. With this in mind, a way to keep the unit up and running for as long as possible is to make sure the power supply fan keeping the unit cool is well maintained. In order to do so, the following operations are suggested:

- Once a year, vacuum the outside of the fan.
- If the fan is not running, replace the power supply immediately.
- If the fan becomes noisy, replace the power supply immediately. Leaving the unit as is without replacing the noisy fan runs the risk of the power supply overheating and breaking down.

The picture below shows the front of the unit with the power switch and three indicators: Power, SCSI activity, and frame sync. The SCSI light blinks when the unit is accessed. The frame sync light is on when the signal from the receiver has been bit and frame synchronized.



The picture below shows the back of the unit.



The upper BNC connects to the G/T Test socket of the X-Band receiver. The two adjacent BNCs connect to the Q and I output of the X-Band receiver. To the right, the SCSI process cards connect to the ingest server.

Follow the steps below in the event the GSI unit needs to be replaced:

- Ask the operator to stop STracker+.
- Remove the bezel in the front of the ingest server and press the power button. The server will shut down.
- Remove side panels of the rack in which the unit is mounted.
- Power off the unit (switch on the front of the unit) and disconnect the power cable.
- Disconnect all other cables.
- Unscrew the unit and remove.
- Screw the new unit in place.
- Connect the cables.
- Connect and power the unit.
- Power the ingest server.

The GSI unit operates normally when the power light is on and the SCSI light blinks when STracker+ is running. Next, wait for a pass. The bit/frame sync light will be on during the reception.

9.1.4 NTS/GPS Unit

There is no preventive maintenance activity that needs to be performed on this component. The NTS/GPS unit is located inside the ingest rack at the remote site. Make sure the NTS-150 unit is powered and connected to the GPS antenna and to the network switch. It may take up to 20 minutes for the unit to be operational. The picture below shows the front of the unit.



The NTS-150 unit is equipped with two status lights: a connection active indicator (ACT) and a System Status Indicator (SSI). The ACT light, located to the right of the RJ-45 socket, should be green to indicate a 100 Mbps connection. The SSI light, located at the bottom left of the unit, is solid red when there is no signal from the time source or a major failure is detected. Otherwise, the SSI light blinks green to indicate a lock to GPS.

To access the unit, execute the command ‘telnet nts’ from any computer on the ES system. Log in as user guest. The password is truetype. If you cannot access the unit via telnet, you can try accessing the unit from the serial port to verify the network parameters. Enter ‘quit’ to exit this session. Once logged in, execute the command ‘F72’ to request a fault status. If there is no fault and the NTS is working properly, the following line is output:

Antenna: OK GPS: Locked

If there is a fault, consult the NTS-150 manual at

<http://www.symmetric.com/media/files/support/ttm/product-manual/man-nts-150.pdf>

or consult the file nts-150man.pdf located in the Manuals/NTS-150/ folder on the PE-ESC MODIS DVD. If the fault cannot be corrected, submit a problem report.

If the GPS is not locked, execute the command ‘F60’ to list the GPS satellites and their strength. If there are no satellites or the strength is zero, verify the GPS cable is connected. If the fault cannot be corrected, submit a problem report.

If the unit needs to be replaced, specific instructions will be sent by IES or GI.

9.1.5 Ingest Server

There is no special maintenance activity that needs to be performed on this component. The server is equipped with a small LED. This LED is blue when the hardware is operating properly. It will turn orange for a moderate fault that does not prevent its normal operations and red when a fatal error occurs. The ingest server can be accessed remotely via its iDRAC (Section 6.7). The LED messages can be viewed from this interface. The iDRAC provides information of the status of the hardware components including the fans.



The ingest server is a PowerEdge R710 Dell Server. The Hardware Owner Manual can be accessed at <http://support.dell.com/support/edocs/systems/per710/en/HOM/HTML/index.htm>

or

<http://support.dell.com/support/edocs/systems/per710/en/HOM/PDF/HOM.pdf>

or with the file PER710_HOM.pdf located in the Manuals/Dell/PR710/ folder on the PE-ESC MODIS DVD.

9.1.6 Network Switch

There is no special maintenance activity that needs to be performed on this component. The network switch is a Linksys SRW2016. The user guide can be accessed at

http://www.cisco.com/en/US/docs/switches/lan/csbms/srw2048/administration/guide/SRW-US_v10_UG_A-Web.pdf

or with the file SRW-US_v1-UG_A-Web.pdf in the Manuals/Linksys/ folder on the GI-MODIS installation DVD.

9.1.7 KVM Console

There is no special maintenance activity that needs to be performed on this component. If you experience a problem with this hardware component submit a report to IES (Section 7.3).

9.1.8 UPS Unit

This unit is a Dell Online Rack UPS 2700W. Once a year, vacuum the outside of the UPS to keep it dust free and perform a battery test. Replace the batteries at least every 5 years to keep the unit running at peak efficiency. Refer to the maintenance section of the UPS user guide (RD-25). The user guide can be accessed at

<http://support.dell.com/support/edocs/acc/upsd/en/ug/ol2700w.pdf>

or with the file 2700_UPS.pdf in the Manuals/Dell/UPS/UserGuide/ folder on the PE-ESC MODIS DVD.

9.2 Base Site

9.2.1 Processing Servers

There is no special maintenance activity that needs to be performed on this component. The server is equipped with a small LED. This LED is blue when the hardware is operating properly. It will turn orange for a moderate fault that does not prevent its normal operations and red when a fatal error occurs. The ingest server can be accessed remotely via its iDRAC (Section 6.7). The LED messages can be viewed from this interface. The iDRAC provides information of the status of the hardware components including the fans.



The ingest server is a PowerEdge R710 Dell Server. The Hardware Owner Manual can be accessed at <http://support.dell.com/support/edocs/systems/per710/en/HOM/HTML/index.htm>

or

<http://support.dell.com/support/edocs/systems/per710/en/HOM/PDF/HOM.pdf>

or with the file PER710_HOM.pdf located in the Manuals/Dell/PR710/ folder on the PE-ESC MODIS DVD.

9.2.2 LTO Drive

There is no special maintenance activity that needs to be performed on this component. This unit is a Dell PowerVault LTO4-120HH tape drive. The user guide can be accessed at

http://support.dell.com/support/edocs/stor-sys/LTO4120H/IBM/en/ug_en/index.htm

The tape drive will display a C on the single-character display and the fault LED will flash amber when the drive needs cleaning. Only insert a cleaning cartridge into the tape drive when the C is displayed.

9.2.3 Network Attached Storage Server

There is no special maintenance activity that needs to be performed on this component. The server is equipped with a small LED. This LED is blue when the hardware is operating properly. It will turn orange for a moderate fault that does not prevent its normal operations and red when a fatal error occurs. The ingest server can be accessed remotely via its iDRAC (Section 6.7). The LED messages can be viewed from this interface.

The NAS is a Dell PowerVault NX3000. The Hardware Owner Manual and the Troubleshooting Guide manuals can be accessed at

<http://support.dell.com/support/edocs/stor-sys/NX3000/en/index.htm>

or with the files HOMA00MR.pdf and TG_en.pdf respectively. Both files are located in the Manuals/Dell/PVNX3000/ folder on the PE-ESC MODIS DVD.

9.2.4 KVM Console and Switch

There is no special maintenance activity that needs to be performed on this component. If you experience a problem with this hardware component submit a report to IES (Section 7.3).

9.2.5 Operator Workstation

Overheating is one of the main sources of workstation breakdown. With this in mind, a way to keep the operator workstation up and running for as long as possible is to make sure the fans keeping the components cool are well maintained. In order to do so, the following operations are suggested:

- Once a year, shut down the workstation and vacuum its inside and the fans.
- If a fan becomes noisy, replace it immediately. Leaving the computer as is without replacing noisy fans runs the risk of the computer overheating and breaking down.

Shutting down the workstation does not have an impact on the automatic ingestion and MODIS processing.



The operator workstation is a Dell Precision T7500. The Service Manual can be accessed at

<http://support.dell.com/support/edocs/systems/wst7500/en/sm/index.htm>

and the Setup and Features Information Technical Sheet manual can be accessed at

http://support.dell.com/support/edocs/systems/wst7500/en/sfits/sfits_en.pdf

or with the file sfits_en.pdf located in the Manuals/Dell/WST7500/ folder on the PE-ESC MODIS DVD.

9.3 Preventative Maintenance Schedule

The preventative maintenance is performed by DND personnel on a daily, weekly, and monthly basis and by GI/IES personnel on a yearly basis. The maintenance tasks are listed Maintenance Plan (RD-09) in four categories:

- **First Line Preventive Maintenance Schedule (DND)**
Clock synchronization check, ingestion check, and processing check.
- **Second Line Hardware preventive maintenance schedule (GI/IES)**
Hardware inspection and vacuuming. Elevation over Azimuth measurement.
- **First Line Software Preventive Maintenance Schedule (DND)**
Log cycling and System 9000 software backup.
- **Second Line Software Preventive Maintenance Schedule (GI/IES)**
System logs review. Patch installation review.
Review and check ingestion and processing chain.



A. Acronyms and Abbreviations

AD	Applicable Document
AOI	Area of Interest
ASCII	American Standard Code for Information Interchange
CADU	Channel Access Data Unit
CF	Canadian Forces
CFB	Canadian Forces Base
CFWOS	Canadian Forces Weather and Oceanographic Services
CCSDS	Consultative Committee for Space Data Systems
DB	Direct Broadcast
DND	Department of the National Defence
EOS	Earth Observing Satellite
ES	Environmental Sensing
ESC	Environmental Sensing Capability
GI	Global Imaging
GMT	Greenwich Mean Time
GUI	Graphical User Interface
ICD	Interfaces Control Document
IES	Info-Electronics Systems Inc.
IVS	Ingest Virtual Screen
MetOC	Meteorological and Oceanographic Centre
MODIS	Moderate Resolution Imaging Spectroradiometer
NAS	Network Attached Storage
NASA	National Aeronautic and Space Agency
NOAA	National Oceanic and Atmospheric Administration
NPOES	National Polar-orbiting Operational Environmental Satellite System
NPP	NPOES Preparatory Project
NSOF	NOAA Satellite Operation Facility
OC	Ocean Color
OCP	Ocean Color Products
OTRS	Open Technologies Real Services



PDU	Power Distribution Unit
RD	Reference Document
RHEL	Red Hat Enterprise Linux
SCID	Spacecraft ID
SeaDAS	SeaWiFS Data Analysis System
SeaWiFS	Sea-viewing Wide Field-of-view Sensor
SSH	Secure Shell Handler
SST	Sea Surface Temperature
TBC	To Be Confirmed
TBD	To Be Determined
TDP	Technical Data Package
UMS	Universal Multi-Satellite
UPS	Uninterruptible Power Supply
UTC	Universal Time Coordinated
VNC	Virtual Network Computing
VSS	Vendor Supplied System
VCDU	Virtual Channel Data Unit
VCID	Virtual Channel ID
ZIP	Zone Interface Point



B. Password Less SSH Access

Appendix to be provided on Contract award



C. West Site System Parameters

Appendix to be provided on Contract award



D. East Site System Parameters

Appendix to be provided on Contract award