Oracle® Communications

Diameter Signaling Router

C-Class Hardware and Software Installation Guide

Release 8.6.0.1.0

F70196-02
September 2022

ORACLE

Oracle Communications Diameter Signaling Router C-Class Hardware and Software Installation Guide, Release 8.6.0.1.0

Copyright © 2022 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

CAUTION: Use only the Upgrade procedure included in the Upgrade Kit.

Before upgrading any system, please access My Oracle Support (MOS) (https://support.oracle.com) and review any Technical Service Bulletins (TSBs) that relate to this upgrade.

My Oracle Support (MOS) (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html.

See more information on My Oracle Support (MOS).

Table of Contents

Table of Contents 3

1. Introduction 6
1.1 Purpose and Scope 6
1.2 References 6
1.3 Acronyms and Terms 6
1.4 Terminology 8
1.5 How to Use This Document 9

2. Acquiring Firmware 10

3. Installation Overview 11
3.1 Required Materials 11
3.2 Installation Strategy 11
3.3 SNMP Configuration 12
3.4 NTP Strategy 12
3.5 Overview of DSR Networks 14

4. Software Installation Procedures 14
4.1 Configure and IPM the Management Server 15
4.1.1 Install TVOE on the Management Server 15
4.1.2 Upgrade Management Server Firmware 15
4.1.3 Deploy Virtualized PMAC 21
4.1.3.2 Deployment Procedure 23
4.1.4 Configure TVOE Network 24
4.2 Install PMAC 36
4.2.1 Deploy PMAC 36
4.2.2 Set Up PMAC 39
4.2.3 Backup PMAC 46
4.3 Configure netConfig Repository 47
4.3.1 Configure Aggregation Switches 65
4.4 Configure PMAC for NetBackup (Optional) 75
4.4.1 Configure NetBackup Feature 75
4.4.2 Install and Configure NetBackup Client on PMAC 79
4.5 HP C-7000 Enclosure Configuration 82
4.5.1 Configure Initial OA IP 82
4.5.2 Configure Initial OA Settings Using the Configuration Wizard 84
4.5.3 Configure OA Security 91
4.5.4 Upgrade or Downgrade OA Firmware 92
4.5.5 Add SNMP Trap Destination on OA 94
4.5.6 Store Configuration on Management Server 96
4.6 Enclosure and Blades Setup 99
4.6.1 Add PMAC Host Rack Mount Server to PMAC System Inventory 106
4.7 Configure Enclosure Switches 110
4.8 Server Blades Installation Preparation 135
4.8.1 Upgrade Blade Server Firmware 135
4.8.2 Confirm/Upgrade Blade Server BIOS Settings 140
4.9 Install TVOE on Rack Mount Servers 143
4.9.1 Add Rack Mount Server to PMAC System Inventory 144
4.9.2 Add ISO Images to the PMAC Image Repository 149
4.9.3 IPM Servers Using PMAC Application 153
4.9.4 Add SNMP Trap Destination on TPD-Based Application 155
4.10 Install TVOE on Blade Servers 157

Appendix A. Initial Product Manufacture of RMS and Blade Server 157
Appendix A.1 Set Server's CMOS Clock 157

Appendix A.2 Configure BIOS Settings **157**
Appendix A.3 OS IPM Installation for HP Rack Mount Servers **160**
Appendix A.4 IPM Command Line Procedures **161**
Appendix A.5 Post Installation Processing **164**
Appendix A.6 Media Check **166**

Appendix B. Change SNMP Configuration Settings for iLO **169**

Appendix C. Access a Server Console Remotely Using iLO **170**

Appendix D. Install NetBackup Client on TVOE Server (Optional) **171**

Appendix E. Uninstall NetBackup Client on TVOE Server (Optional) **173**

Appendix F. Using WinSCP **180**

Appendix G. Upgrade Cisco 4948 PROM **182**

Appendix H. Backup Procedures **185**

Appendix H.2 Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig) **188**

Appendix I. Determine which Onboard Administrator is Active **191**

Appendix J. NetBackup Procedures (Optional) **192**
Appendix J.1 Application NetBackup Client Install/Upgrade Procedures **192**
Appendix J.2 NetBackup Client Install/Upgrade with nbAutoInstall **194**
Appendix J.3 NetBackup Client Install/Upgrade with platcfg **195**
Appendix J.4 Create NetBackup Client Configuration File **202**

Appendix K. Disable SNMP on the OA **200**

Appendix L. Downgrade Firmware on a 6125 Switch **201**

Appendix M. Configure Speed and Duplex for 6125XLG LAG Ports (netConfig) **210**

Appendix N. RPM Installation of Switch 6127XLG for PMAC **211**

Appendix O. Operational Dependencies on Platform Account Passwords **217**
Appendix O.1 PMAC Credentials for Communication with Other System Components **217**
Appendix O.2 GUI Account Credentials **220**
Appendix O.3 PMAC Linux User Account Credentials **220**

Appendix P. Edit Rack Mount Server in the PMAC System Inventory **221**

Appendix Q. Increase the PMAC NetBackup File System Size **223**

Appendix R. netConfig backup Configuration/restoreConfiguration/upgradeFirmware with TPD Cipher Change **229**

Appendix S. My Oracle Support (MOS) **231**

List of Tables

Table 1. Acronyms 8
Table 2. Terminology 10
Table 3. DSR Networks 16
Table 4. Procedure Reference Table 18
Table 5. Installed Packages and Services for NetBackup Client 7.0, 7.1, 7.5, and 7.7 169

1. Introduction

1.1 Purpose and Scope

This document provides the methods and procedures used to configure the DSR 8.6 Management Server TVOE and PMAC, initialize the system's aggregation switches and enclosure switches, and perform the initial configuration of the DSR system's RMS and HP c-Class enclosure.

The procedures in this document should be executed in order. Skipping steps or procedures is not allowed unless explicitly stated.

Note: Before executing any procedures in this document, power must be available to each component, and all networking cabling must be in place. Switch uplinks to the customer network should remain disconnected until instructed otherwise.

The audience for this document includes oracle customers and the following:

- Software System personnel
- Product verification staff
- Documentation staff
- Customer service including software operations and first office applications
- Oracle partners

1.2 References

For HP Blade and RMS firmware upgrades, Software Centric customers need the HP Solutions Firmware Upgrade Pack and Software Centric Release Notes on http://docs.oracle.com under Platform documentation. Beyond the minimum version specified for the Platform, the application dictates which Firmware Upgrade Packs to use.

[1] DSR Software Installation and Configuration Procedure, Part 2/2

[2] HP Solutions Firmware Upgrade Pack, version 2.x.x

The latest is recommended if an upgrade is to be performed; otherwise, version 2.2.12 is the minimum.

[3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes

The latest is recommended if an upgrade is to be performed; otherwise, version 2.2.12 is the minimum.

[4] TPD Initial Product Manufacturer Software Installation Procedure

[5] Platform Configuration Reference Guide

[6] Interconnect Technical Reference Procedure

1.3 Acronyms and Terms

An alphabetized list of acronyms and terms used in the document.

Table 1. Acronyms

Acronym	Definition
BIOS	Basic Input Output System
CA	Certificate Authority
CSR	Certificate Signing Request

Acronym	Definition
DB	Database
DNS	Domain Name System
DSCP	Differentiated Services Code Point, a form of QoS
DSR	Diameter Signaling Router
DVD	Digital Versatile Disc
EBIPA	Enclosure Bay IP Addressing
FMA	File Management Area
FQDN	Fully Qualified Domain Name
FRU	Field Replaceable Unit
GUI	Graphical User Interface
HP c-Class	HP blade server offering
HP FUP	HP Firmware Upgrade Pack
IE	Internet Explorer
iLO	Integrated Lights Out remote management port
iLOM, ILOM	Integrated Lights Out manager
IMI	Internal Management Interface
IP	Internet Protocol
IPM	Initial Product Manufacture — the process of installing TPD on a hardware platform
MP	Message Processing or Message Processor
NAPD	Network Architecture planning Diagram
NMS	Network Management Station
NOAM	Network OAM
NOAMP	Network OAM Program
OA	HP Onboard Administrator
OAM	Operations, Administration and Maintenance
OS	Operating System (e.g., TPD)
PMAC, PMAC	Platform Management & Configuration
RMS	Rack Mounted Server
QoS	Quality of Service
SAN	Storage Area Network
SFTP	Secure File Transfer Protocol
SNMP	Simple network Management Protocol
SOAM	System OAM
SSH	Secure Shell

Acronym	Definition
SSO	Single Sign On
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtual Operating Environment
UI	User Interface
VIP	Virtual IP
VSP	Virtual Serial Port
XMI	External Management Interface

1.4 Terminology

This section describes terminology as it is used within this document.

Table 2. Terminology

Term	Definition
Community String	An SNMP community string is a text string used to authenticate messages sent between a management station and a device (the SNMP agent). The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent.
Domain Name System	A system for converting hostnames and domain names into IP addresses on the Internet or on local networks that use the TCP/IP protocol.
Management Server	An HP ProLiant DL 360/DL 380 that has physical connectivity required to configure switches and may host the PMAC application or serve other configuration purposes.
NetBackup Feature	Feature that provides support of the Symantec NetBackup client utility on an application server.
Non-Segregated Network	Network interconnect where the control and management, or customer, networks use the same physical network.
PMAC	An application that supports platform-level capability to manage and provision platform components of the system, so they can host applications.
Segregated Network	Network interconnect where the control and management, or customer, networks utilize separate physical networks.
Server	A generic term to refer to a server, regardless of underlying hardware, be it physical hardware or a virtual TVOE guest server.
Software Centric	A term used to differentiate between customers buying both hardware and software from Oracle, and customers buying only software.
Virtual PMAC	Additional term for PMAC - used in networking procedures to distinguish activities done on a PMAC guest and not the TVOE host running on the Management server.

1.5 How to Use This Document

Although this document is primarily to be used as an initial installation guide, its secondary purpose is to be used as a reference for Disaster Recovery procedures.

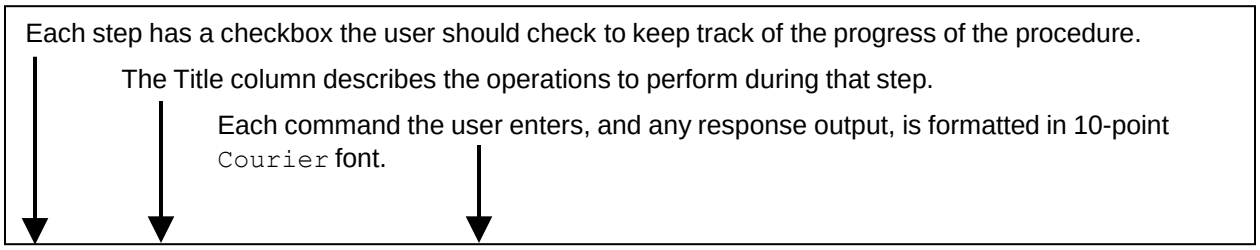
When executing this document for either purpose, there are a few points which help to ensure that the user understands the author's intent. These points are as follows;

1. Before beginning a procedure, completely read the instructional text (it will appear immediately after the Section heading for each procedure) and all associated procedural WARNINGS or NOTES.
2. Before execution of a STEP within a procedure, completely read the left and right columns including any STEP specific WARNINGS or NOTES.

If a procedural STEP fails to execute successfully, STOP and contact Oracle's Customer Service for assistance before attempting to continue. See Appendix R, for information on contacting Oracle Customer Support.

Figure 1 shows an example of a procedural step used in this document.

- Any sub-steps within a step are referred to as step X.Y. The example in Figure 1 shows steps 1 through 3, and step 3.1.
- GUI menu items, action links, and buttons to be clicked on are in bold Arial font.
- GUI fields and values to take note of during a step are in bold Arial font.
- Where it is necessary to explicitly identify the server on which a particular step is to be taken, the server name is given in the title box for the step (for example, "ServerX" in step 2 Figure 1).



	Title	Directive/Result Step
1. ☐	Change directory	Change to the backout directory. `$ cd /var/TKLC/backout`
2. ☐	**ServerX**: Connect to the console of the server	Establish a connection to the server using cu on the terminal server/console. `$ cu -l /dev/ttyS7`
3. ☐	Verify Network Element data	View the Network Elements configuration data; verify the data; save and print report. 3. Select **Configuration > Network Elements** to view Network Elements Configuration screen.

Figure 1. Example of a Procedure Steps Used in This Document

2. Acquiring Firmware

Several procedures in this document pertain to the upgrading of firmware on various servers and hardware devices that are part of the Platform 7.6 configuration.

Platform 7.6 servers and devices requiring possible firmware updates are:

- HP c7000 Blade System Enclosure Components
  - Onboard Administrator
  - 1GB Ethernet Pass-Thru Module
  - Cisco 3020 Enclosure Switches
  - HP6120XG Enclosure Switches
  - HP6125G Enclosure Switches
  - HP6125XLG Enclosure Switches
  - HP6127XLG Enclosure Switches
  - Blade Servers (BL460)
- HP Rack Mount Server (DL360/380)
- HP External Storage Systems
  - D2200sb (Storage Blade)
  - D2220sb (Storage Blade)
- Cisco 4948/4948E-F Rack Mount Network Switches

Software centric customers do not receive firmware upgrades through Oracle. Instead, refer to the [3] HP Solution Firmware Upgrade pack, Software Centric Release Notes on http://docs/oracle.com under Platform documentation. The latest release is recommended if an upgrade is performed; otherwise, release 2.2.12 is the minimum.

The required firmware and documentation for upgrading the firmware on HP hardware systems and related components are distributed as the HP Solutions Firmware Upgrade Pack 2.x.x. The minimum firmware release required for Platform 7.6 is HP Solutions Firmware Upgrade Pack 2.2.12. However, if a firmware upgrade is needed, the current GA release of the HP Solutions Firmware Upgrade Pack 2.x.x should be used.

Each version of the HP Solutions Firmware Upgrade Pack [3] contains multiple items including media and documentation. If an HP FUP 2.x.x version newer than the Platform 7.6 minimum of HP FUP 2.2.12 is used, then the HP Solutions Firmware Upgrade Guide should be used to upgrade the firmware. Otherwise, the Upgrade Guide of the HP Solutions Firmware Upgrade Pack [3] is not used for new installs. Instead, this document provides its own upgrade procedures for firmware.

The three pieces of required firmware media provided in the HP Solutions Firmware Upgrade Pack 2.x.x releases are:

- HP Service Pack for ProLiant (SPP) firmware ISO image
- HP MISC Firmware ISO image

Refer to the Release Notes of the HP Solutions Firmware Upgrade Pack [3] to determine specific firmware versions provided. Contact My Oracle Support (MOS) for more information on obtaining the HP Firmware Upgrade Pack.

Note: "Warning: Creating/using bootable USB SPP media to upgrade HP RMS firmware is currently unsupported. All other methods for upgrading HP RMS firmware detailed in the HP FUP Upgrade Procedures Document are still supported."

3. Installation Overview

This section contains the installation overview, and includes information about required materials, strategies, and SNMP configuration.

This section configures the DSR base hardware systems (RMS and HP c-Class enclosure) (RMS and Blade IPM, Networking, Enclosure and PMAC Configuration). Following the execution of this document, the DSR user follows a DSR application procedure document to complete the DSR application specific configurations.

Note that IPM refers to installing either TVOE or TPD on the target system. TVOE is used when virtualization is needed (for example, for the PMAC and NO/SO). TPD is used for systems that do not require virtualization and for the Virtual Machines.

3.1 Required Materials

1. One (1) ISO of TPD, release specified by Release Notes.
2. One (1) ISO of PMAC, release specified by Release Notes.
3. One (1) USB of TVOE, release specified by Release Notes.
4. One (1) USB or ISO of DSR 8.6 and all configuration files and templates acquired via the DSR ISO.
5. Passwords for users on the local system.
6. Access to the iLO Terminal or direct access to the server VGA port.
7. HP Solutions Firmware Upgrade Pack, version 2.x.x (the latest version must be used if an upgrade is to be performed, otherwise version 2.2.12 is the minimum). A 4GB or larger USB Flash Drive.
8. NAPD and all relevant configuration materials for ALL sites involved. This includes host IP addresses, site network element XML files, and netConfig configuration files.
9. Keyboard and monitor if configuring iLO addresses.

Note: Customers are required to download all software from the Oracle Software Delivery Cloud (OSDC).

3.2 Installation Strategy

To ensure a successful application installation, plan and assess all configuration materials and installation variables. After a customer site survey has been conducted, an installer can use this section to plan the exact procedures that should be executed at each site.

1. Establish an overall installation requirement. The data collected should include the following:
   - The total number of sites
   - The number of servers at each site and their role(s)
   - Determine if the application's networking interface terminates on a Layer 2 or Layer 3 boundary
   - Establish the number of enclosures at each site (if any)
   - Determine if the application uses rack-mount servers or server blades
   - What time zone should be used across the entire collection of application sites
   - Will SNMP traps be viewed at the application level, or an external NMS be used (or both)
2. Conduct a site survey to determine exact networking and site details. Additionally, IP networking options must be well understood, and IP address allocations collected from the customer, in order to complete switch configurations

3.3 SNMP Configuration

The network plan for SNMP configuration should be decided upon before DSR installation proceeds. This section provides some recommendations for these decisions.

SNMP traps can originate from the following entities in a DSR installation:

- DSR Application Servers (NOAMP, SOAM, MPs of all types)
- DSR Auxiliary Components (OA, Switches, TVOE hosts, PMAC)

DSR application servers can be configured to:

1. Send all their SNMP traps to the NOAMP via merging from their local SOAM. All traps terminate at the NOAMP and are viewable from the NOAMP GUI (entire network) and the SOAM GUI (site specific) if only NOAMP and SOAM are configured as Manager and the **Traps Enabled** checkbox is selected for these managers on **Administration > Remote Servers > SNMP Trapping** screen. This is the default configuration option.
2. Send all their SNMP traps to an external Network Management Station (NMS). The traps are NOT seen at the SOAM or at the NOAM. They are viewable at the configured NMS(s) only if the external NMS is configured as Manager and **Traps Enabled** checkbox is selected for this manager on **Administration > Remote Servers > SNMP Trapping** screen.
3. Send SNMP traps from individual servers like MPs of all types if the **Traps from Individual Servers** checkbox is selected on **Administration > Remote Servers > SNMP Trapping** screen.

Application server SNMP configuration is done from the NOAMP GUI, near the end of DSR installation. See the procedure list for details.

DSR Auxiliary components must have their SNMP trap destinations set explicitly. Trap destinations can be the NOAMP VIP, the SOAMP VIP, or an external (customer) NMS. The recommended configuration is as follows:

The following components:	Should have their SNMP trap destinations set to:
• TVOE for PMAC server • PMAC (App) • OAs • All Switch types (4948, 3020, 6120, 6125, 6127XLG) • TVOE for DSR Servers	1. The local SOAM VIP 2. The customer NMS, if available

Note: All the entities must use the same community string during configuration of the NMS server.

Note: SNMP community strings, (for example, read only or read/write SNMP community strings) should be the same for all components like OAM/MP servers, PMACs, TVOEs, and external NMS.

Note: Default SNMP trap port used to receive traps is 162. You can provide the port number from the SNMP configuration screen.

3.4 NTP Strategy

The following set of general principles capture the recommendations for NTP configuration of DSR:

Principle 1 — Virtual guests should not be used as NTP servers

Avoid specifying virtual guests as NTP references for other servers. Guest emulated clocks have been shown to result in poor NTP server behavior.

Principle 2 — Virtual guests should synchronize to their virtual hosts

When virtualization is used in the product deployment, virtual guests should use their TVOE hosts as their NTP references.

Principle 3 — Follow a topology based approach

MP servers should use their topology parents (SOAMs in a three tier topology), or if those parents are virtual guests, the enclosing virtual hosts should be used instead. The PMAC TVOE host should be used as a third NTP source. See Figure 2 for clarification.

Similarly, SOAM servers should use their topology parents (NOAMs), or if those parents are virtual guests, the enclosing virtual hosts should be used instead. See Figure 2 for clarification.

NOAMP and other A-Level servers should use a pool of reliable, customer provided references if the NOAMPs are implemented in hardware, otherwise they should synchronize to their virtual hosts.

Principle 4 — Provide a robust pool of sources

The pool of customer NTP server references should be of stratum 3 or above, accurate and highly reliable. If possible, both local site server and backup remote site servers should be provided. Three or more customer NTP sources are required.

Principle 5 — Prefer local references

When references from multiple sites or networks are used on one server, the "prefer" keyword should be applied to the local references.

Principle 6 — Ensure connectivity

Ensure all NTP references are reachable through the appropriate networking configuration. In particular, firewall rules must be correctly specified to allow NTP clients to connect to their specified references.

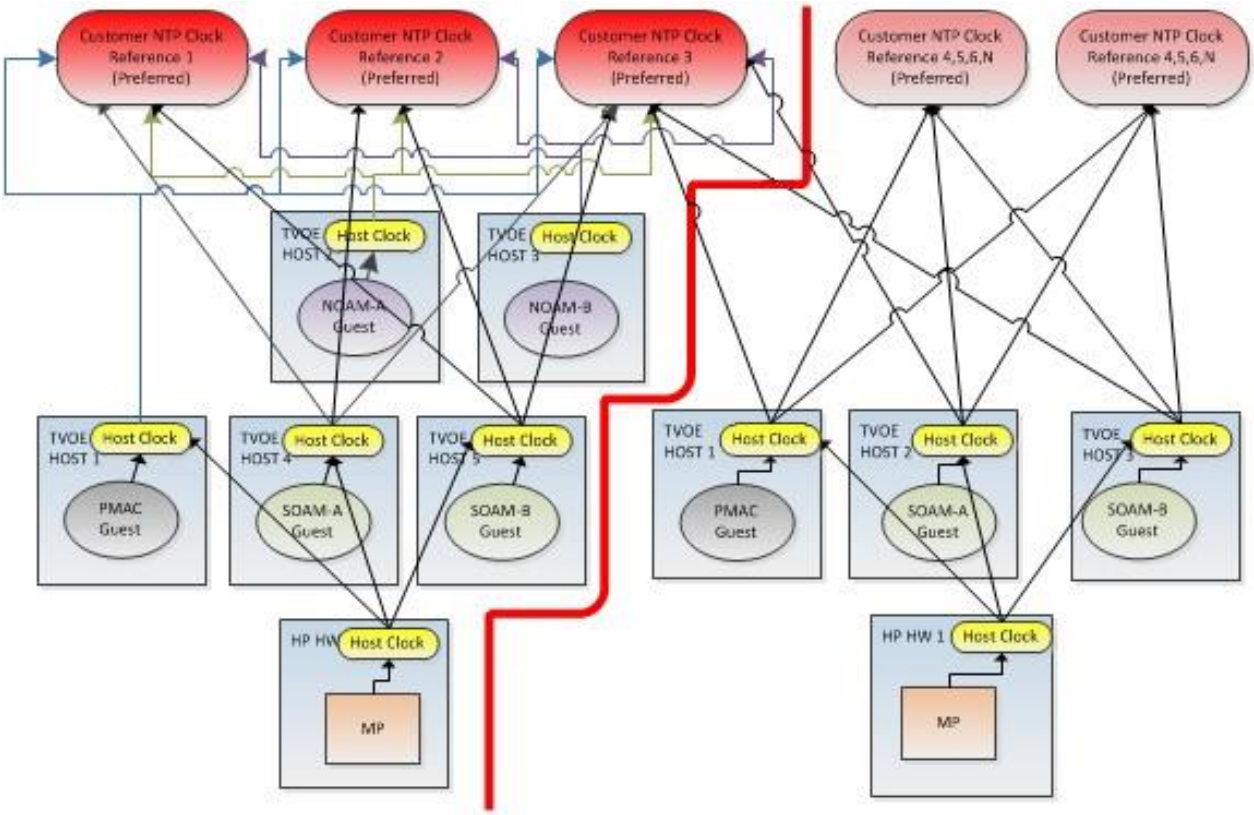


Figure 2. Per Site NTP Topology

3.5 Overview of DSR Networks

This table presents an overview of the networks configured and used by DSR at a site. Based on the deployment type/requirements, the networks could be physically or logically separated using VLANs.

Table 3. DSR Networks

Network Name	Default VLAN ID*	Routable	Description
Control	1	No	Network used by PMAC to IPM the servers/blades/VMs. Refer to the NAPD for site-specific IP information (IPs are assigned by the PMAC using DHCP)
Management	2	Yes	Network used for iLO interfaces, OAs, and enclosure switches. Also used to provide remote access to the TVOE and PMAC servers
XMI	3	Yes	Network used to provide access to the DSR entities (GUI, ssh), and for inter-site communication
IMI	4	No	Network used for intra-site communication
XSI-1	5	Yes	Network used for DSR signaling traffic
XSI2-XSI16**	6-20	Yes	Networks used for DSR signaling traffic
Replication	21	Yes	Network used for DSR PCA secondary replication (for example, PCA)

* The VLAN ID assignments are site and deployment specific.

** Optional.

4. Software Installation Procedures

This section contains the software installation procedures, including preparation and configuration information for a site.

The procedures in this section are expected to be executed in the order presented in this section.

If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support (MOS).

Sudo

Platform 6.7 introduced a new non-root user, admusr. As a non-root user, many commands (when run as admusr) now require the use of **sudo**. Using **sudo** requires a password with the first command, and intermittently over time. Therefore, if a prompt for **[sudo] password** displays, the user should re-enter the admusr login password.

Example:

```
[admusr@hostname ~]$ sudo <command>
[sudo] password for admusr: <ENTER PASSWORD HERE>
<command output omitted>
[admusr@hostname ~]$
```

4.1 Configure and IPM the Management Server

The management server is installed as a virtual host environment and hosts the PMAC application. It may also host other DSR applications as defined by the deployment configuration for the customer site.

Depending on the deployment plan, you can IPM a server with either TVOE (if virtualization is needed) or TPD (if no virtualization is needed).

4.1.1 Install TVOE on the Management Server

Install the TVOE hypervisor platform on the management server. The PMAC is not available to an IPM of the TVOE management server. It is necessary to provide the TVOE media physically using a bootable USB. Refer to section 3.1 Required Materials for more information.

Procedure 1. Configure DL380

Step #	Procedure	Description
This procedure describes the configuration of DL380. Prerequisites: set the HW clock accurately per Appendix A. TPD or TVOE installation media to be used for IPM. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Configure the iLO IP address	For more information, refer to Appendix F in the TPD Initial Product Manufacturer Software Installation Procedure [4].
2. ☐	Configure and IPM	Configure the DL380 Gen8/Gen9 server as described in Appendix A. For a DL380 Gen8/Gen9 server, the correct options to use for the IPM of the management server are: `TPDnoraid console=tty0 diskconfig=HWRAID,force` Note: Do not use the remote serial console for installation.

4.1.2 Upgrade Management Server Firmware

Software Centric Customers:

If Oracle Consulting Services or any other Oracle Partner is providing services to a customer that include installation and/or upgrade then, as long as the terms of the scope of those services include that Oracle Consulting Services is employed as an agent of the customer (including update of Firmware on customer provided services), then Oracle consulting services can install FW they obtain from the customer who is licensed for support from HP.

Note: This procedure uses a custom SPP version that cannot be obtained from the customer and, therefore, cannot be used for a Software Centric Customer. Software Centric Customers must ensure their firmware versions match those detailed in the HP Solutions Firmware Upgrade Pack, Software Centric Release Notes [3] document.

The service pack for ProLiant (SPP) installer automatically detects the firmware components available on the target server and only upgrades those components with firmware older than what is provided by the SPP in the HP FUP version being used.

Table 4. Procedure Reference Table

Variable	Description	Value
<iLO>	IP address of the iLO for the server being upgraded	
<ilo_admin_user>	Username of the iLO Administrator user	
<ilo_admin_password>	Password for the iLO Administrator user	
<local_HPSPP_image_path>	Filename for the HP support pack for ProLiant ISO	
<admusr_password>	Password for the admusr user for the server being upgraded	

Needed Material:

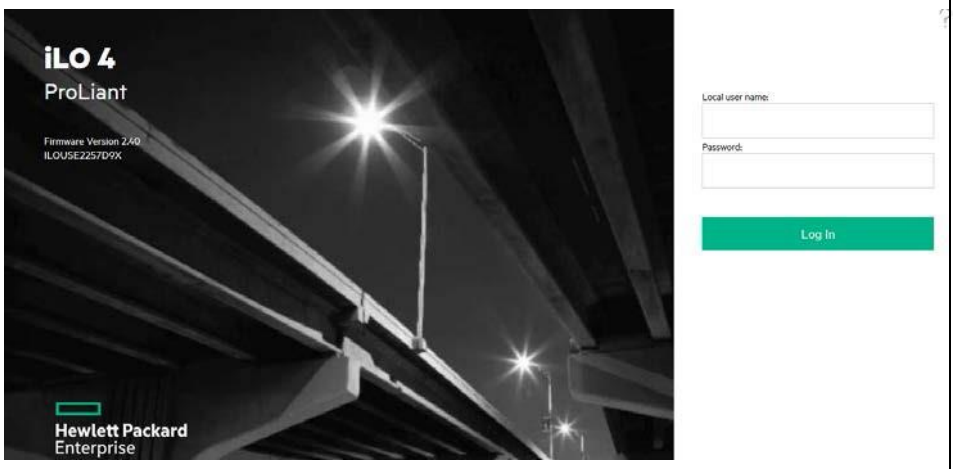
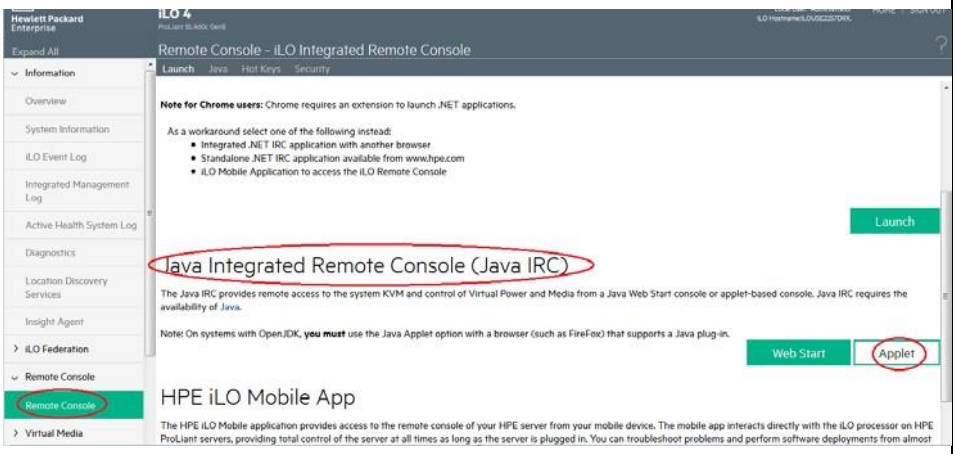
- HP Service Pack for ProLiant (SPP) firmware ISO image
- HP MISC firmware ISO image (for errata updates if applicable)
- Release Notes of the HP Solutions Firmware Upgrade Pack, version 2.x.x [2]
- Upgrade Guide of the HP Solutions Firmware Upgrade Pack, version 2.x.x [2]

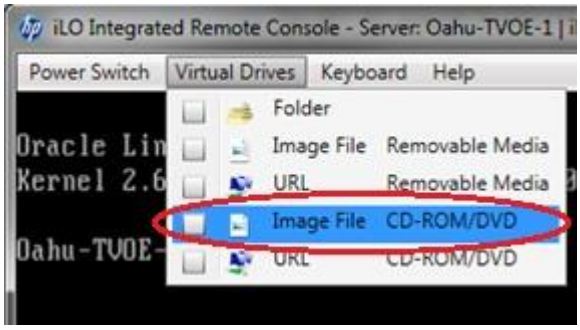
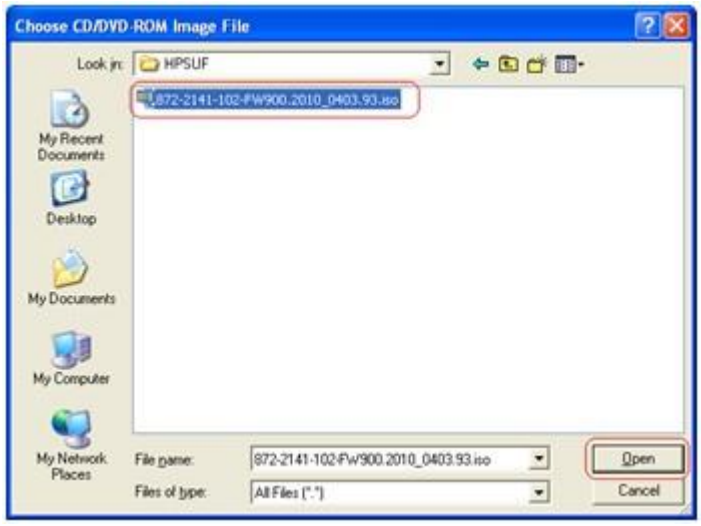
Important Notes:

- Ignore references to the Copy the ISO Images to the Workstation procedure
- Ignore the <local_HPSPP_image_path> variable
- For the Update Firmware Errata step, check the HP Solutions Firmware Upgrade Pack, version 2.x.x Upgrade Guide to see if there are any firmware errata items that apply to the server being upgraded. If there is, there is a directory matching the errata's ID in the /errata directory of the HP MISC firmware ISO image. The errata directories contain the errata firmware and a README file detailing the installation steps.

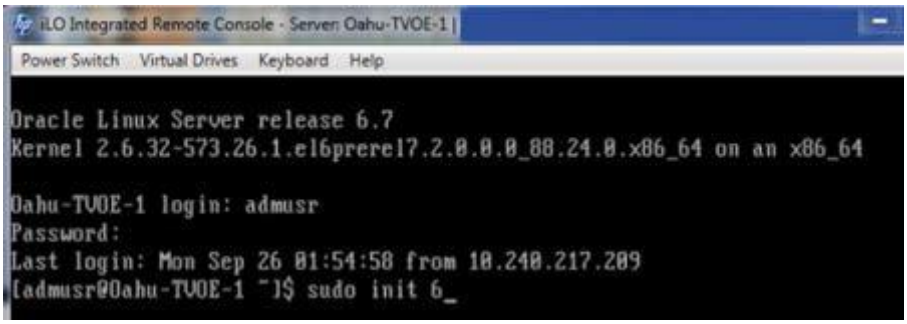
Procedure 2. Upgrade Management Server Firmware

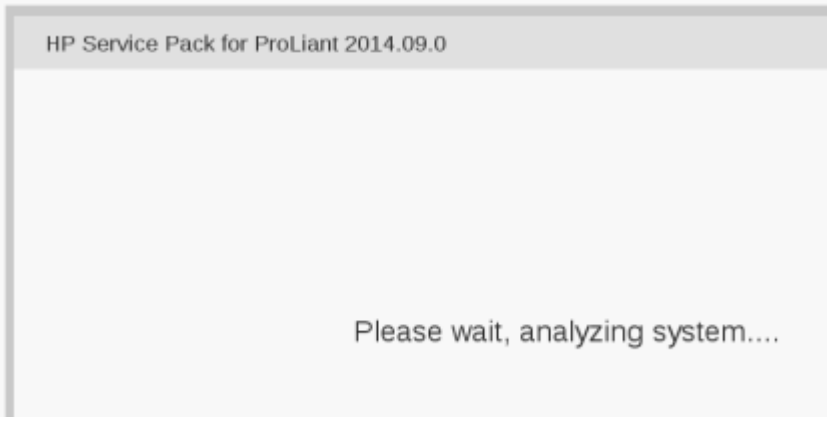
Step #	Procedure	Description
This procedure upgrades the DL380 server firmware. All servers should have SNMP disabled. Refer to Appendix B. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Local Workstation**: Access iLO Web GUI	Access the ProLiant Server iLO Web Login Page from an Internet Explorer session using the following URL: `https://<ilo_IP>/`

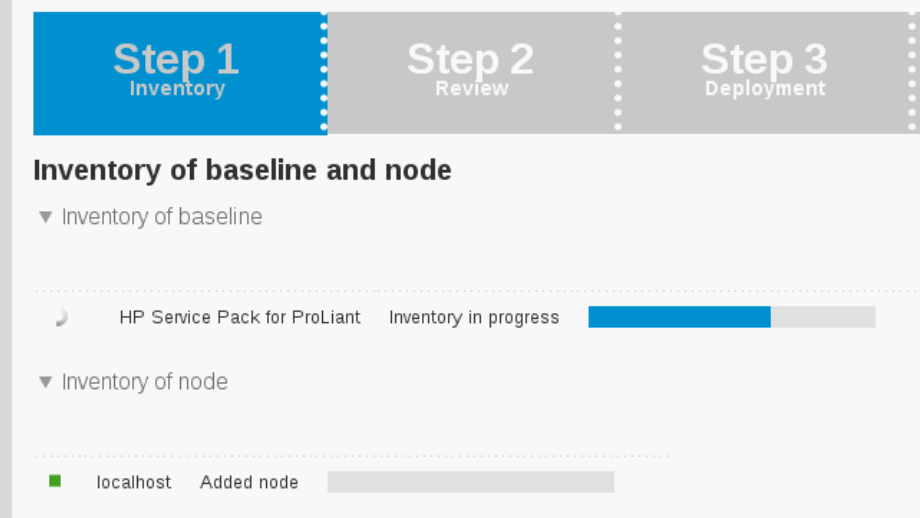
Step #	Procedure	Description
2.	**iLO Web GUI**: Log into iLO	Log into iLO as the administrator user. Username = <ilo_admin_user> Password = <ilo_admin_password> 
3.	**iLO Web GUI**: Open Java	Open the Java Integrated Remote Console applet. On the menu to the left, navigate to the **Remote Console** page. Click on the **Java Integrated Remote Console → Applet** to open it.  Click **Continue**.

Step #	Procedure	Description
		 If other warning screens display, acknowledge them to proceed to the Java integrated Remote Console applet.
4.	**iLO4 Remote Console**: Create virtual drive connection	Click on the Virtual Drives list and select the **Image File (CD-ROM/DVD)**.  Locate the HP Support Pack for ProLiant ISO file copied to the workstation and click **Open**. 

Step #	Procedure	Description

5.	**iLO4 Remote Console**: Reboot the server	Once the remote console application opens to the login prompt, log into the server as admusr.
		`Localhost login: admusr`
		`Password: <admusr_password>`
		Initiate a server reboot
		`$ sudo init 6`
		 

6.	**iLO4 Remote Console**: Perform an unattended firmware upgrade	After the server reboots into the HP Support Pack for ProLiant ISO, press Enter to select the Automatic Firmware Update procedure. If no key is pressed in 30 seconds, the system automatically performs an Automatic Firmware Update. ***Important***: Do not click inside the remote console during the rest of the firmware upgrade process. The firmware install stays at the EULA acceptance screen for a short period of time. The time it takes this process to complete varies by server and network connection speed and takes several minutes. During that time, the following screen displays on the console.  No progress indication displays during the system scan and analysis stage. In about 10 minutes, the installation automatically proceeds to the next step.

Step #	Procedure	Description
7.	**iLO4 Remote** Console: Monitor installation	Once analysis is complete, the installer begins to inventory and deploy the eligible firmware components. A progress indicator displays. If iLO firmware is applied, the Remote Console disconnects, but continues upgrading. If the Remote Console closes due to the iLO upgrading, wait 3-5 minutes and log back into the iLO Web GUI and reconnect to the Remote Console. The server might already be done upgrading and might have rebooted.  ***Note***: If the iLO firmware is to be upgraded, the iLO session is terminated and you lose the remote console, virtual media, and Web GUI connections to the server. This is expected and does not impact the firmware upgrade process.
8.	Local **Workstation**: Clean up	Once the firmware updates have been completed, the server automatically reboots. • If you are upgrading a Gen8 (iLO4) server; closing the remote console window disconnects the virtual image and you can close the iLO4 Web GUI browser session. • If you are using SPP USB media plugged into the server, you can now remove it.
9.	Local **Workstation**: Verify server availability	Wait 3 to 5 minutes and verify the server has rebooted and is available by gaining access to the login prompt.
10.	Update firmware errata	Refer to the ProLiant Server Firmware Errata section to determine if this HP Solutions Firmware Update Pack contains additional firmware errata updates that should be applied to the server at this time.
11.	Repeat	Repeat this procedure for all remaining RMSs, if any.

4.1.3 Deploy Virtualized PMAC

4.1.3.1 What You Need

Use the completed NAPD information to fill in the appropriate data in this Procedure's Reference tables. The following are provided to aid with the data collection for the TVOE management server and the PMAC Application hosted on the Management Server TVOE.

- Determine if the network configuration of this management server is non-segregated or segregated.

  Note: The term segregated networks refers to the separation of the management server's control and plat-management networks onto separate physical NICs. If either of the following scenarios exists, the networks are considered segregated.

  - Devices eth01 and eth02 of the management server are physically connected to the first pair of the c7000 enclosure switches.
  - Devices eth01 and eth02 of two RMS servers are directly connected to each other (e.g., eth01 > eth01 and eth02 > eth02.

- Determine the TVOE management server's required network interface, bond, Ethernet device, and route data.
- Determine if the control network on the TVOE management server is to be tagged. If appropriate, fill in the <control VLAN ID> value in the table; otherwise, the control network is not tagged.
- Determine if the management network on the TVOE management server is to be tagged. If appropriate, fill in the <TVO_Management_VLAN_ID> value in the table; otherwise, the management network is not tagged.
- Determine the bridge name to be used on the TVOE management server for the management network. Fill in the <TVOE_Management_Bridge> value in the table.
- Determine if the NetBackup feature is enabled.
  - Determine if the NetBackup network on the TVOE management server is to be tagged. If appropriate, fill in the <NetBackup_VLAN_ID> value in the table; otherwise, the NetBackup network is not tagged.
  - Determine the bridge name to be used on the TVOE management server for the NetBackup network. Fill in the <TVOE_NetBackup_Bridge> value in the table
  - Determine if the NetBackup network is to be configured with jumbo frames. If appropriate, fill in the <NetBackup_MTU_size> value in the table; otherwise, the NetBackup network uses the default MTU size.
  - If the PMAC NetBackup feature is enabled, and the backup service is routed with a source interface different then the management interface where the default route is applied, then define the route during PMAC initialization as a host route to the NetBackup server.
- The PMAC initialization profiles have been designed to configure the PMAC's networks and features. Profiles must identify interfaces. Existing profiles provided by PMAC use standard named interfaces (control, management). No VLAN tagging is expected on the PMAC's interfaces, all tagging should be handled on the TVOE management server configuration.

Network Interface	DL380 (with HP 4pt 1GB in PCI Slot 1) (Gen8 and Gen9)	DL380 (with HP 4pt 1GB 331FLR Adapter)
<ethernet_interface_1>	eth01	eth01
<ethernet_interface_2>	eth02	eth02
<ethernet_interface_3>	Eth11	eth03

Network Interface	DL380 (with HP 4pt 1GB in PCI Slot 1) (Gen8 and Gen9)	DL380 (with HP 4pt 1GB 331FLR Adapter)
<ethernet_interface_4>	Eth12	eth04
<ethernet_interface_5>	eth04	eth05

PMAC Interface Alias	TVO Bridge Name	TVOE Bridge Interface
Control	control	<TVOE_Control_Bridge_Interface> value for this site (default is bond0):
Management	<TVOE_Management_Bridge> value for this site:	<TVOE_Management_Bridge_Interface> value for this site:
NetBackup	<TVOE_NetBackup_Bridge> value for this site:	<TVOE_NetBackup_Bridge_Interface> value for this site:

Variable	Description	Value
<control_VLAN_ID>	For non-segregated networks, the control network may have a VLAN ID assigned. In most cases, there is none.	
<base_device_hosting_control_network>	If <control_VLAN_ID> has a value, then the device used for the control network <TVOE_Control_Bridge_Interface> has a tagged interface name. The base device for the control network is the untagged interface name. For example, if the device interface is bond1.2, then the base device is bond1.	
<management_VLAN_ID>	For non-segregated networks, the management network is on a tagged VLAN coming in on bond0.	
<mgmtVLAN_gateway_address>	Gateway address used for routing on the management network.	
<NetBackup_server_IP>	The IP address of the remote NetBackup server.	

Variable	Description	Value
<NetBackup_VLAN_ID>	For non-segregated networks, the NetBackup network is on a tagged VLAN coming in on bond0.	
<NetBackup_gateway_address>	Gateway address used for routing on the NetBackup network.	
<NetBackup_network_IP>	The Network IP for the NetBackup network.	
<PMAC_<NetBackup_netmask_or_prefix>	The IPv4 netmask or IPv6 prefix assigned to the PMAC for participation in the NetBackup network.	
<PMAC_NetBackup_IP_address>	The IP address assigned to the PMAC for participation in the NetBackup network.	
<NetBackup_MTU_size>	If desired, the MTU size can be set to tune the NetBackup network traffic.	
<management_server_mgmt_IP_address>	The TVOE management server's IP address on the management network.	
<PMAC_mgmt_IP____address>	The PMAC application's IP address on the management network.	
<mgmt_netmask_or_prefix>	The IPv4 netmask or IPv6 prefix for the management network.	
<PMAC_control_IP_address>	The PMAC application's IP address on the control network.	
<control_netmask>	The IP netmask for the control network.	

Network Bond Interface	Enslaved Interface 1 Value	Enslaved Interface 2 Value
bond0		
For segregated networks only		
bond1		
bond2		

4.1.3.2 Deployment Procedure

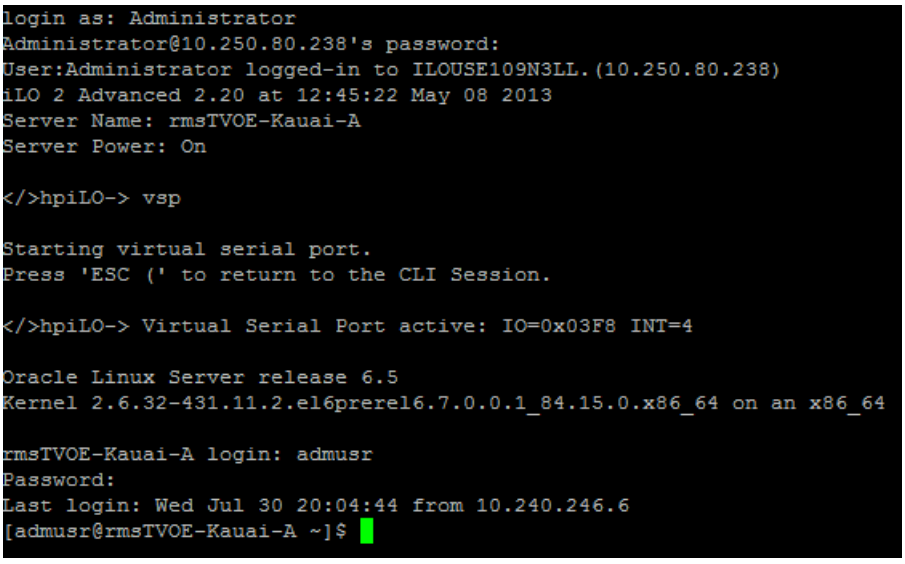
Deploying a VM guest in the absence of a PMAC is complicated. To facilitate this, the PMAC media includes a guest archive and a script that deploys the running PMAC into a state where the Initialization process can begin.

1. Install the appropriate TVOE version on the management server via the ILO.
2. Create and configure the management bridge.

3. Determine if NetBackup Feature is enabled for this system. If enabled, install appropriate NetBackup client to the PMAC TVOE host.
4. Attach PMAC media to the TVOE (USB).
5. Mount the media.
6. Use the <mount-point>/upgrade/pmac-deploy script to create the VM and configure the guest on the first boot.
7. Navigate browser to the management IP address of the deployed PMAC.
8. Perform Initial Configuration.

4.1.4 Configure TVOE Network

Procedure 3. Configure TVOE Network

Step #	Procedure	Description
This procedure configures the TVOE network. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**TVOE Management Server**: Login	1. Log into the management server iLO on the remote console using application provided passwords via Appendix C. 2. Log into the iLO in Internet Explorer using password provided by application: `http://<management_server_iLO_IP>` 3. Click the Remote Console tab and open the Integrate Remote Console on the server.  4. Click **Yes** if the security alert displays.

Step #	Procedure	Description
2. ☐	**TVOE Management Server**: Configure the control network bond for back-to-back configurations	If the control network for the RMS servers consists of direct connections between the servers with no intervening switches (known as a "back-to-back" configuration), execute this step to set the primary interface of bond0 to <ethernet_interface_1>; otherwise, skip to the next step. ***Note***: The output shown is for illustrative purposes only. The site information for this system determines the network interfaces (network devices, bonds, and bond enslaved devices) to configure. `$ sudo /usr/TKLC/plat/bin/netAdm set --device=bond0 --onboot=yes --type=Bonding --mode=active-backup --miimon=100 --primary=<ethernet_interface_1>Interface bond0 updated`

3. ☐	**TVOE Management Server**: Verify control network bond	***Note***: The output shown is for illustrative purposes only to show the control bond configured.
		`$ sudo /usr/TKLC/plat/bin/netAdm query --device=<TVOE_Control_Bridge_Interface>`
		`Protocol: none`
		`On Boot: yes`
		`IP Address:`
		`Netmask:`
		`Bonded Mode: active-backup`
		`Enslaving: <ethernet_interface_1> <ethernet_interface_2>`
		If the bond has been configured, skip to the next step.
		If the RMS servers do not fit this configuration, move onto the next step.
		Note: The output shown is for illustrative purposes only. The site information for this system determines the network interfaces (network devices, bonds, and bond enslaved devices) to configure.
		`$ sudo /usr/TKLC/plat/bin/netAdm set --device=bond0 --onboot=yes --type=Bonding --mode=active-backup --miimon=100 --primary=<ethernet_interface_1>Interface bond0 updated`
		Remove existing bond:
		`$ sudo /usr/TKLC/plat/bin/netAdm set --type=Bridge --name=control --delBridgeInt=<TVOE_Control_Bridge_Interface>`
		`Interface <TVOE_Control_Bridge_Interface> updated`
		`Bridge control updated`
		`$ sudo /usr/TKLC/plat/bin/netAdm delete --device=<TVOE_Control_Bridge_Interface>`
		`Interface bond0 removed`
		Re-create control bond (<TVOE_Control_Bridge_Interface>) with primary interface set to <ethernet_interface_1>:
		`$ sudo /usr/TKLC/plat/bin/netAdm add --device=bond0 --onboot=yes --type=Bonding --mode=active-backup --miimon=100 --primary=<ethernet_interface_1>`
		`Interface <TVOE_Control_Bridge_Interface> added`
		`$ sudo /usr/TKLC/plat/bin/netAdm set --device=<ethernet_interface_1> --type=Ethernet --`

Step #	Procedure	Description

		master=<TVOE_Control_Bridge_Interface> --slave=yes --onboot=yes
		Interface <ethernet_interface_1> updated
		$ sudo /usr/TKLC/plat/bin/netAdm set --device=<ethernet_interface_2> --type=Ethernet --master=<TVOE_Control_Bridge_Interface> --slave=yes --onboot=yes
		Interface <ethernet_interface_2> updated
		Add <TVOE_Control_Bridge_Interface> back to existing control bridge:
		$ sudo /usr/TKLC/plat/bin/netAdm set --type=Bridge --name=control --bridgeInterfaces=<TVOE_Control_Interface>

4. □	**TVOE Management Server**: Verify control network bridge	***Note***: The output shown is for illustrative purposes only to show the control bond configured.
		$ sudo /usr/TKLC/plat/bin/netAdm query --type=Bridge --name=control
		Bridge Name: control
		On Boot: yes
		Protocol: dhcp
		Persistent: yes
		Promiscuous: no
		Hwaddr: 00:24:81:fb:29:52
		MTU:
		Bridge Interface: bond0
		If the bridge has been configured, skip to the next step.
		Note: The output shown is for illustrative purposes only. The site information for this system determines the network interfaces (network devices, bonds, and bond enslaved devices) to configure.
		Create control bridge <TVOE_Control_Bridge>
		$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=<TVOE_Control_Bridge> --bootproto=dhcp --onboot=yes --bridgeInterfaces=<TVOE_Bridge_Interface>

Step #	Procedure	Description

5. ☐	**TVOE iLO**: Create tagged control interface and bridge
	(optional)
		If you are using a tagged control network interface on this PMAC, then complete this step using values for the control interface on bond0 from the preceding tables; otherwise, proceed to the next step.
		`$ sudo /usr/TKLC/plat/bin/netAdm set --type=Bridge --name=control --delBridgeInt=bond0`
		`Interface bond0 updated`
		`Bridge control updated`
		`$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_Control_Bridge_Interface> --onboot=yes`
		`Interface <TVOE_Control_Bridge_Interface> created`
		`$ sudo /usr/TKLC/plat/bin/netAdm set --device=<Enslaved Interface 1> --onboot=yes`
		`$ sudo /usr/TKLC/plat/bin/netAdm set --device=<Enslaved Interface 2> --onboot=yes`
		`$ sudo /usr/TKLC/plat/bin/netAdm set --type=Bridge --name=control --bridgeInterfaces=<TVOE_Control_Bridge_Interface>`

6. ☐	**TVOE Management Server**: Verify the tagged/non-segregated management network	A Segregated Management Network can be either tagged or untagged. In most cases, the network is tagged when the TVOE Host is used to host DSR guests in addition to the PMAC guest. In this scenario, both the Management and XMI networks are required and are tagged on the same bond. In scenarios where only the PMAC is hosted by the TVOE and only the Management network is required, untagged can be used. The switch configuration of the connected switches must match the server configuration tagged or untagged.
		Note: This step only applies if the management network is tagged (non-segregated).
		Note: The output shown is for illustrative purposes only to show the configured management bridge on a non-segregated network setup.
		`$ sudo /usr/TKLC/plat/bin/netAdm query --device=bond0.2`
		`  Protocol: none`
		`   On Boot: yes`
		`IP Address:`
		`   Netmask:`
		`    Bridge: Member of bridge management`
		If the device has been configured, skip to the next step.
		This example illustrates a tagged device for a tagged management network.
		`$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_Management_Bridge_Interface> --onboot=yes`
		`Interface <TVOE_Management_Bridge_Interface> added`

Step #	Procedure	Description

7. ☐	**TVOE Management Server**: Verify the tagged/segregated management network	***Note***: This step only applies if the management network is tagged (segregated).
		Note: The output shown is for illustrative purposes only to show the configured management bond on a segregated network setup.
		`$ sudo /usr/TKLC/plat/bin/netAdm query --device=<TVOE_Management_Bridge_Interface>`
		`$ sudo /usr/TKLC/plat/bin/netAdm query --device=bond1`
		`Protocol: none`
		`On Boot: yes`
		`IP Address:`
		`Netmask:`
		`Bonded Mode: active-backup`
		`Enslaving: <ethernet_interface_3> <ethernet_interface_4>`
		If the bond has been configured, skip to the next step.
		`$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_Management_Bridge_Interface> --onboot=yes --type=Bonding --mode=active-backup --miimon=100 --bondInterfaces="<ethernet_interface_3>,<ethernet_interface_4>"`
		`Interface <TVOE_Management_Bridge_Interface> added`
		
		`# Create bond1.2 which will be used in next step`
		sudo /usr/TKLC/plat/bin/netAdm add --device=bond1.2 --onboot=yes

8. ☐	**TVOE Management Server**: Verify the management bridge	***Note***: The output shown is for illustrative purposes only to show the configured management bridge on a non-segregated network setup.
		`$ sudo /usr/TKLC/plat/bin/netAdm query --type=Bridge --name=management`
		`Bridge Name: management`
		`On Boot: yes`
		`Protocol: none`
		`IP Address: 10.240.4.86`
		`Netmask: 255.255.255.0`
		`Promiscuous: no`
		`Hwaddr: 00:24:81:fb:29:52`
		`MTU:`
		`Bridge Interface: bond1.2`
		If the bridge has been configured, skip to the next step.
		This example illustrates a tagged device for a tagged management bridge.
		`$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=<TVOE_Management_Bridge> --address=<management_server_mgmtVLAN_IP> --netmask=<mgmtVLAN_netmask_or_prefix> --onboot=yes --bridgeInterfaces=<TVOE_Management_Bridge_Interface>`

Step #	Procedure	Description

9. ☐	**TVOE Management Server**: Verify the NetBackup network, if needed	If the NetBackup feature is not needed, skip to the next step.
		Note: The output shown is for illustrative purposes only to show the NetBackup bridge is configured.
		`$ sudo /usr/TKLC/plat/bin/netAdm query --type=Bridge --name=netbackup`
		`Bridge Name: netbackup`
		`On Boot: yes`
		`Protocol: none`
		`IP Address: 10.240.6.2`
		`Netmask: 255.255.255.0`
		`Promiscuous: no`
		`Hwaddr: 00:24:81:fb:29:52`
		`MTU:`
		`Bridge Interface: bond2`
		`Bond2 can be created using NIC cards/Ethernet dedicated for NetBackup. Please refer [6] for Interconnect procedure to check dedicated card for NetBackup.`
		If the bridge has been configured, skip to the next step.
		Notes:
		The example below illustrates a TVOE management server configuration with the NetBackup feature enabled. The NetBackup network is configured with a non-default MTU size.
		The MTU size must be consistent between a network bridge, device, or bond, and associated VLANs.
		Select only one of the following configurations:
		• Option 1: Create NetBackup bridge using an untagged native interface.
		`$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=<TVOE_NetBackup_Bridge> --bootproto=none --onboot=yes --MTU=<NetBackup_MTU_size> --bridgeInterfaces=<Ethernet_interface_5> --address=<TVOE_NetBackup_IP> --netmask=<TVOE_NetBackup_Netmask_or_prefix>`
		• Option 2: Create NetBackup bridge using a tagged device.
		`$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_NetBackup_Bridge_Interface> --onboot=yes`
		`Interface <TVOE_NetBackup_Bridge_Interface> added`
		`$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=<TVOE_NetBackup_Bridge> --onboot=yes --MTU=<NetBackup_MTU_size> --bridgeInterfaces=<TVOE_NetBackup_Bridge_Interface> --address=<TVOE_NetBackup_IP> --netmask=<TVOE_NetBackup_Netmask_or_prefix>`

Step #	Procedure	Description

10. ☐	**TVOE Management Server**: Syscheck	syscheck must be configured to monitor bond interfaces. Replace "bondedInterfaces" with "bond0" or "bond0,bond1" if segregated networks are used:
		`$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --set --var=DEVICES --val=<bondedInterfaces>`
		`$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond –enable`
		`$ sudo /usr/TKLC/plat/bin/syscheck -v net ipbond`
		Note: The following is an example of the setup of syscheck with a single bond, bond0:
		`$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --set --var=DEVICES --val=bond0`
		`$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond -enable`
		`$ sudo /usr/TKLC/plat/bin/syscheck -v net ipbond`
		Note: The following is an example of the setup of syscheck with multiple bonds, bond0, and bond1:
		`$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --set --var=DEVICES --val=bond0,bond1`
		`$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond -enable`
		`$ sudo /usr/TKLC/plat/bin/syscheck -v net ipbond`

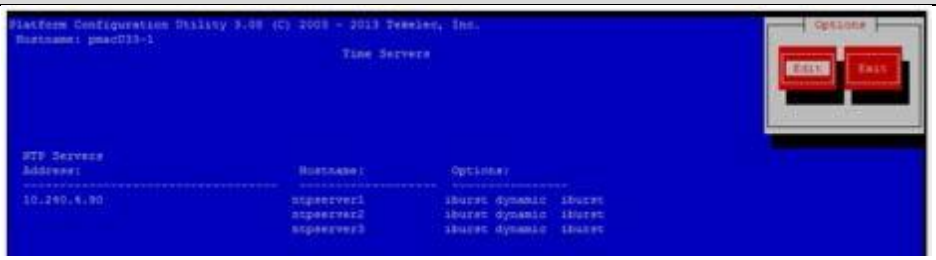
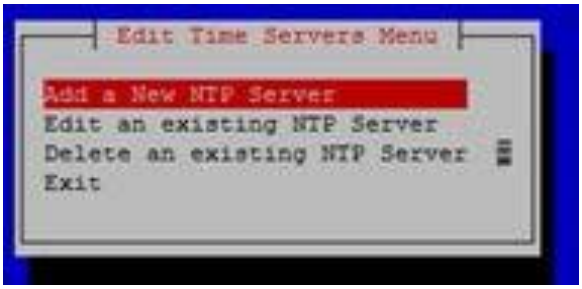
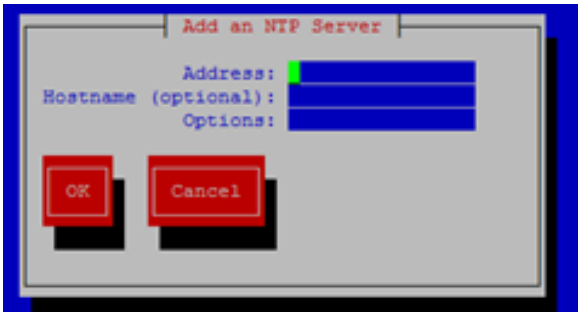
11. ☐	**TVOE Management Server**: Verify the default route	***Note***: The output shown is for illustrative purposes only to show the default route on the management bridge is configured.
		`$ sudo /usr/TKLC/plat/bin/netAdm query --route=default --device=management`
		`Routes for TABLE: main and DEVICE: management`
		`* NETWORK: default`
		`GATEWAY: 10.240.4.1`
		If the route has been configured, skip to the next step.
		For this example, add the default route on the management network.
		`$ sudo /usr/TKLC/plat/bin/netAdm add --route=default --device=<TVOE_Management_Bridge> --gateway=<mgmt_gateway_address>`
		`Route to <TVOE Management Bridge> added`

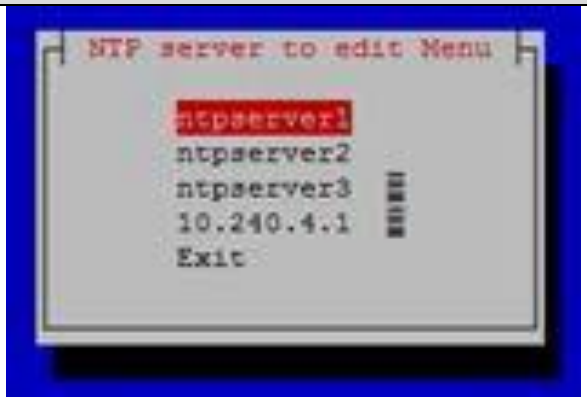
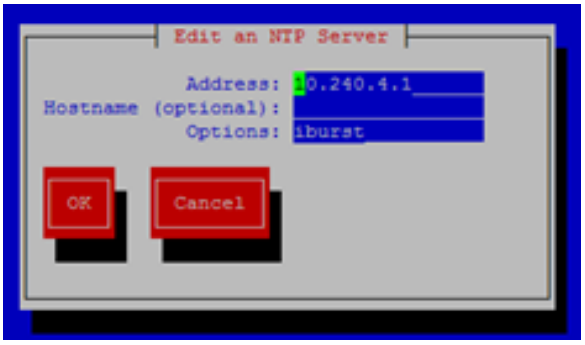
12. ☐	**TVOE Management Server**: Verify the NetBackup route
	(optional)
		If the NetBackup network is a unique network for NetBackup data, verify the existence of the appropriate NetBackup route.
		Note: The output shown is for illustrative purposes only to show the route on the NetBackup bridge is configured.
		If the NetBackup route is to be a network route, then:
		`$ sudo /usr/TKLC/plat/bin/netAdm query --route=net --device=<TVOE_NetBackup_Bridge>`
		`Routes for TABLE: main and DEVICE: netbackup`
		`* NETWORK: net`
		`GATEWAY: 169.254.253.1`
		If the NetBackup route is to be a host route then:

Step #	Procedure	Description

		`$ sudo /usr/TKLC/plat/bin/netAdm query --route=host --device=<TVOE_NetBackup_Bridge>`
		`Routes for TABLE: main and DEVICE: netbackup`
		`* NETWORK: host`
		`GATEWAY: 169.254.253.1`
		If the route has been configured, skip to the next step.
		For this example, add the network route on the management network.
		`$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --device=<TVOE_Management_Bridge> --gateway=<NetBackup_gateway_address> --address=<NetBackup_network_IP> --netmask=<TVOE_NetBackup_Netmask_or_prefix>`
		`Route to <TVOE_NetBackup_Bridge> added`
		For this example, add the host route on the management network.
		Note: For configuration of a host route, the <TVOE_NetBackup_Netmask> is set to 255.255.255.255.
		`$ sudo /usr/TKLC/plat/bin/netAdm add --route=host --device=<TVOE_Management_Bridge> --gateway=<NetBackup_Server_IP> --address=<NetBackup_Server_IP> --netmask=<TVOE_NetBackup_Netmask_or_prefix>`
		`Route to <TVOE_NetBackup_Bridge> added`

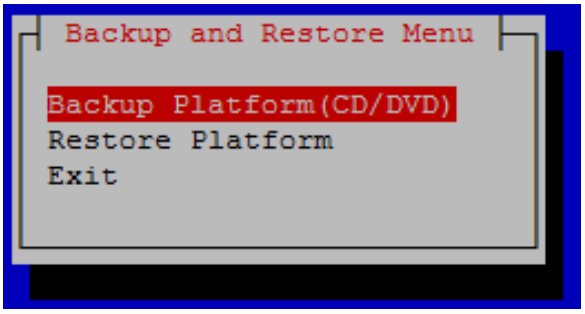
13. ☐	**TVOE Management Server**: Set hostname	`$ sudo /bin/su – platcfg` 1. Navigate to **Server Configuration** > **Hostname** and set the hostname. 2. Set TVOE Management Server hostname. 3. Press **OK**. 4. Navigate out of Hostname.
14. ☐	**TVOE Management Server**: Set time zone and/or hardware clock	1. Navigate to **Server Configuration > Time Zone**. 2. Click **Edit**. 3. Set the time zone and/or hardware clock to GMT (Greenwich Mean Time). 4. Press **OK**. 5. Navigate out of Server Configuration.
15. ☐	Configure NTP servers for a server based on TPD	***Note***: Three NTP sources are configured in this step. Refer to 3.4 NTP Strategy. 1. Login as **platcfg** on the server. 2. Navigate to the Network Configuration -> NTP. 3. Click **Edit** to update NTP information.

Step #	Procedure	Description
		 4. Select the appropriate Edit Time Servers Menu option. 5. When all Time Server actions are complete, exit the Edit Time Servers Menu. Remember that three (or more) NTP sources are required. ***Note***: If NTP servers already exit, go to step 8; otherwise, continue with the next step to add an NTP server. 6. If adding a new NTP server, click **Add a New NTP Server**.  7. Enter data and click **OK**.  ***Note***: The default NTP option is iburst. Addition NTP options are listed in the ntp.conf main page. Some valid option are burst, minpoll, and maxpoll. 8. If editing an existing NTP server, click **Edit an existing NTP Server**. 9. Select the appropriate NTP server.

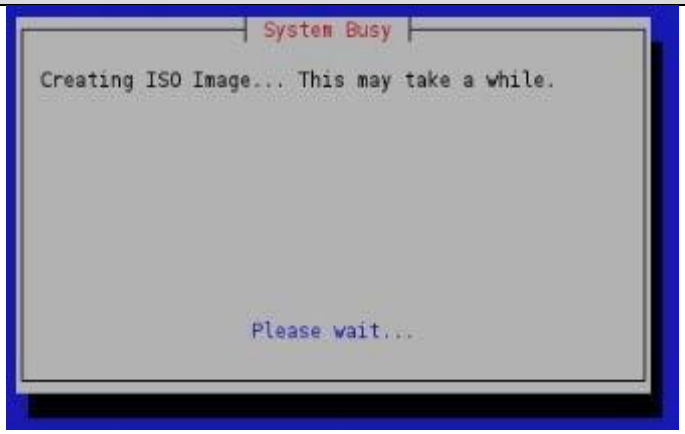
Step #	Procedure	Description
		 10. Enter data and click **OK**.  11. If deleting an existing NTP server, click **Delete an existing NTP Server**. 12. Select the appropriate NTP server. 13. Restart the NTP server. 14. Exit platcfg by clicking **Exit** on each menu until platcfg has been exited.
16. ☐	**Server**: Add an SNMP trap destination	Add an SNMP trap destination to a server based on TPD. All alarm information is set to the NMS located at the destination. Follow Procedure 29.

Step #	Procedure	Description
17. ☐	**TVOE Management Server**: Verify server health	`$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus` Alarms may be observed if network connectivity has not been established.

18. ☐	**TVOE Management Server**: Ensure time is set correctly	Set time based on NTP server.
		`$ sudo /sbin/service ntpd stop`
		`$ sudo /usr/sbin/ntpdate ntpserver1`
		`$ sudo /sbin/service ntpd start`
		Reboot the server.
		`$ sudo /sbin/init 6`

19. ☐	Back up system files	This step backs up system files to be used to restore a failed system. ***Note***: Store the backup image on a customer-provided medium. 1. Login as **platcfg** user. 2. Navigate to **Maintenance > Backup and Restore > Back Platform**. 3. Click **Backup Platform (CD/DVD)**.  ***Note***: If this operation is attempted on a system without media, the following message displays: 4. Click **Build ISO file only** to build the backup ISO image.

Step #	Procedure	Description

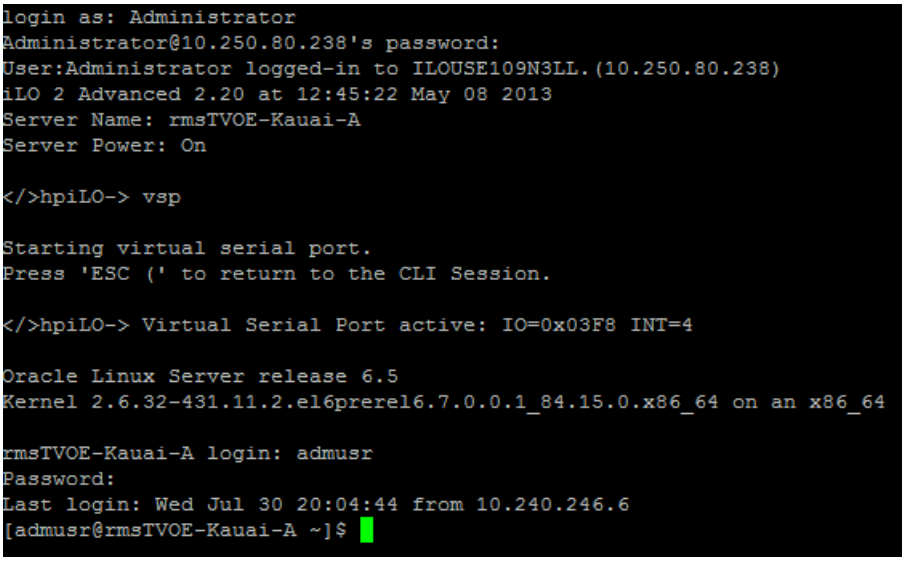
		
		Note: Creating the ISO image may happen so quickly that this screen may only appear for an instant.
		After the ISO is created, platcfg returns to the Backup TekServer menu as shown in step 2. The ISO has now been created and is located in the `/var/TKLC/bkp/` directory. An example filename of a backup file that was created is: "hostname1307466752-plat-app-201104171705.iso".
		5. Exit platcfg by clicking **Exit** on each menu until platcfg has been exited.
		The SSH connection to the TVOE server is terminated.
		6. Log into the customer server and copy the backup image to the customer server where it can be safely stored.
		• From a Linux system, execute the following command to copy the backup image to the customer system.
		`# scp tvoexfer@<TVOE IP Address>:backup/* /path/to/destination/`
		When prompted, enter the tvoexfer user password and press Enter.
		An example of the output looks like:
		`# scp tvoexfer@<TVOE IP Address>:backup/* /path/to/destination/`
		`tvoexfer@10.24.34.73's password:`
		`hostname1301859532-plat-app-301104171705.iso 100% 134MB 26.9MB/s 00:05`
		• From a Windows system, refer to Appendix Fto copy the backup image to the customer system.

4.2 Install PMAC

4.2.1 Deploy PMAC

The pmac-deploy script deploys a PMAC guest. This is all done at build time and the system disk image is kept on the PMAC media, along with this script. Once the PMAC media is mounted, the pmac-deploy script can be found in the upgrade directory of the media.

Procedure 2. Deploy PMAC Guest

Step #	Procedure	Description
This procedure creates the PMAC guest and installs the OS and application. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**TVOE Management Server iLO**: Login	1. Log into the management server iLO on the remote console using application provided passwords via Appendix C. 2. Log into the iLO in Internet Explorer using password provided by application: `http://<management_server_iLO_IP>` 3. Click the Remote Console tab and open the Integrate Remote Console on the server.  4. Click **Yes** if the security alert displays.

2. ☐	**TVO Management Server**: Mount PMAC media	Mount PMAC media to the TVOE management server. Alternatively, you can log into the management console through PuTTY.
		For a sample of mounting a USB media.
		`$ sudo /bin/ls /media/*/*.iso`
		`/media/usb/872-2441-104-5.0.0_50.8.0-PMAC-x86_64.iso`
		`$ sudo /bin/mount -o loop /media/usb/872-2441-104-5.0.0_50.8.0-PMAC-x86_64.iso /mnt/upgrade`

Step #	Procedure	Description

3. ☐	**TVOE Management Server**: Validate PMAC media	Execute the self-validating media script.
		`$ cd /mnt/upgrade/upgrade`
		`$ sudo .validate/validate_cd`
		`Validating cdrom...`
		`UMVT Validate Utility v2.2.2, (c)Tekelec, June 2012`
		`Validating <device or ISO>`
		`Date&Time: 2012-10-25 10:07:01`
		`Volume ID: tklc_872-2441-106_Rev_A_50.11.0`
		`Part Number: 872-2441-106_Rev_A`
		`Version: 50.11.0`
		`Disc Label: PMAC`
		`Disc description: PMAC`
		`The media validation is complete, the result is: PASS`
		`CDROM is Valid`
		If the media validation fails, the media is not valid and should not be used.

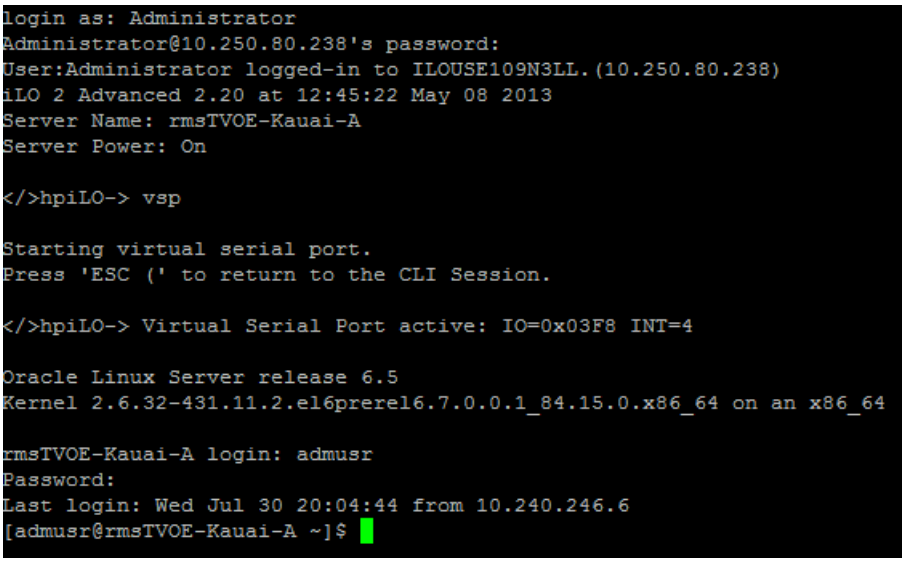
Step #	Procedure	Description
4. ☐	**TVOE Management Server**: Deploy OM&C instance	Using the pmac-deploy script, deploy the PMAC instance using the configuration detailed by the completed NAPD. For this example, deploy a PMAC without the NetBackup feature. `$ cd /mnt/upgrade/upgrade` `$ sudo ./pmac-deploy --guest=<PMAC_Name> --hostname=<PMAC_Name> --controlBridge=<TVOE_Control_Bridge> --controlIP=<PMAC_Control_ip_address> --controlNM=<PMAC_Control_netmask> --managementBridge=<PMAC_Management_Bridge> --managementIP=<PMAC_Management_ip_address> --managementNM=<PMAC_Management_netmask_or_prefix> --routeGW=<PMAC_Management_gateway_address> --ntpserver=<TVOE_Management_server_ip_address> --isoimagesVolSizeGB=20` Deploying a PMAC with the NetBackup feature requires the **--netbackupVol** option, which creates a separate NetBackup logical volume on the TVOE host of PMAC. If the NetBackup feature's source interface is different from the management interface include the **--bridge** and the **--nic** as shown in the example below. `$ cd /mnt/upgrade/upgrade` `$ sudo ./pmac-deploy --guest=<PMAC_Name> --hostname=<PMAC_Name> --controlBridge=<TVOE_Control_Bridge> --controlIP=<PMAC_Control_ip_address> --controlNM=<PMAC_Control_netmask> --managementBridge=<PMAC_Management_Bridge> --managementIP=<PMAC_Management_ip_address> --managementNM=<PMAC_Management_netmask_or_prefix> --routeGW=<PMAC_Management_gateway_address> --ntpserver=<TVOE_Management_server_ip_address> --netbackupVol --bridge=<TVOE_NetBackup_Bridge> --nic=netbackup` ***Note***: If a mistake in the pmac-deploy is identified during this step, the operator under the advisement of customer service can remove the guest with the following command: `$ sudo /usr/TKLC/plat/bin/guestMgr --remove <PMAC_Name>` The PMAC deploys and boots. The management and control network displays based on the settings provided to the pmac-deploy script

5. ☐	**TVOE Management Server**: Unmount and remove PMAC media	`$ cd /`
		`$ sudo /bin/umount /mnt/upgrade`
		Remove the PMAC media.

4.2.2 Set Up PMAC

At the conclusion of this section, the PMAC application environment is sufficiently configured to allow configuration of system network assets associated with the Management Server.

Procedure 5. Set Up PMAC

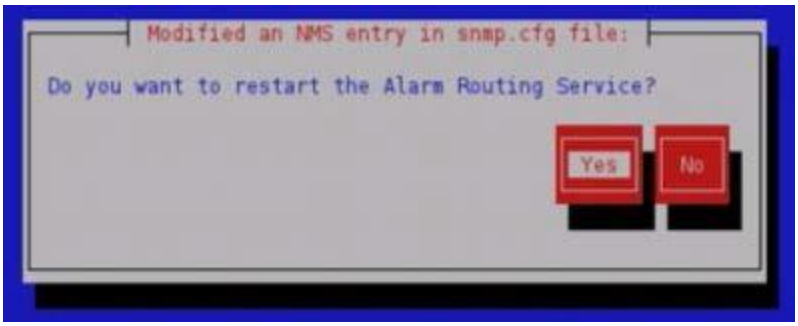
Step #	Procedure	Description
This procedure configures the PMAC application guest environment on the management server TVOE hos and initializes the PMAC application. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**TVOE Management Server iLO**: Login	1. Log into the management server iLO on the remote console using application provided passwords via Appendix C. 2. Log into the using a web browser and the password provided by the application. `http://<management_server_iLO_IP>` 3. Click the Remote Console tab and open the Integrate Remote Console on the server.  4. Click **Yes** if the security alert displays.

Step #	Procedure	Description

2. ☐	**TVO Management Server**: Login	Log into PMAC with admusr credentials.
		Note: On a TVOE host, if you open the virsh console, for example, `$ sudo /usr/bin/virsh console X` or from the virsh utility `virsh # console X` command and you get garbage characters or the output is not correct, then there is likely a stuck **virsh console** command already being run on the TVOE host. Exit out of the virsh console, run `ps -ef |grep virsh`, and then kill the existing process "`kill -9 <PID>`. Then execute the `virsh console X` command. Your console session should now run as expected.
		Login using virsh and wait until you see the login prompt. If a login prompt does not display after the guest is finished booting, press **Enter** to make one display:
		`$ sudo /usr/bin/virsh`
		`virsh # list`
		`Id Name State`
		`4 pmacU17-1 running`
		`virsh # console pmacU17-1`
		`[Output Removed]`
		`####################`
		`1371236760: Upstart Job readahead-collector: stopping`
		`1371236767: Upstart Job readahead-collector: stopped`
		`####################`
		`CentOS release 6.4 (Final)`
		`Kernel 2.6.32-358.6.1.el6prerel6.5.0_82.16.0.x86_64 on an x86_64`
		`pmacU17-1 login:`

3. ☐	Verify PMAC configuration	Verify the PMAC configured correctly on first boot. Run the following command (there should be no output): `$ sudo /bin/ls /usr/TKLC/plat/etc/deployment.d/`

4. ☐	Set the time zone	1. Determine the time zone to use for PMAC.
		Note: Valid time zones can be found on the server in the /usr/share/zoneinfo directory. Only time zones within the sub-directories (for example, America, Africa, Pacific, Mexico, etc.) are valid with platcfg.
		2. Set the time zone.
		`$ sudo /usr/TKLC/smac/bin/set_pmac_tz.pl <timezone>`
		For example:
		`$ sudo set_pmac_tz.pl America/New_York`
		3. Verify the time zone has been updated.
		`$ sudo /bin/date`

Step #	Procedure	Description
5.	**Server**: Add SNMP trap destination	This step adds an SNMP trap destination to a server based on TPD. See section 3.3 to configure SNMP traps such that all alarm information is sent to the NMS located at the destination. 1. Login as **platcfg** user on the server. Navigate to Network Configuration > SNMP Configuration >NMS Configuration. 1. Click **Edit**. 2. Click **Add a New NMS Server** and enter data about the SNMP trap destination. Click **OK**. 3. Click **Exit** and then **Yes** to restart the Alarm Routing Service.  4. Exit platcfg by clicking **Exit** on each menu until platcfg has been exited.

Step #	Procedure	Description
6. ☐	**Server**: Reboot the server	Log into PMAC with **admusr** credentials, if needed. Reboot the server. `$ sudo /sbin/init 6`
Steps 7. through 12. gather and prepare configuration files required to proceed with the DSR installation. These files must reside on the PMAC to proceed with the application installation after the PMAC has been deployed, but before it has been initialized. These files are usually located within a given ISO on physical media. ***Needed Material***: • HP Misc. Firmware ISO • DSR application ISO • Release Notes for the HP Solutions Firmware Upgrade Pack, version 2.x.x [2]		
7. ☐	**PMAC Server**: Login	Log into PMAC with **admusr** credentials on the management server iLO.

8. ☐	**PMAC Server**: Mount media	Make the media available to the TVOE host server by mounting the media.
		1. Insert the USB with the DSR application ISO into an available USB slot on the TVOE host server.
		`$ sudo /bin/ls /media/*/*.iso`
		For example:
		`/media/sdd1/872-2507-111-4.1.0_41.16.2-DSR-x86_64.iso`
		Note: The USB device is immediately added to the list of media devices once it is inserted into a USB slot on the TVOE host server.
		2. Determine its location and the ISO to mount.
		3. Note the device directory name under the media directory.
		This could be sdb1, sdcl, sddl, or sdel depending on the USB slot into which the media was inserted.
		4. Loop mount the ISO to the standard TVOE host mount point (if it is not already in use).
		`$ sudo /bin/mount -o loop /media/<device directory>/<ISO Name>.iso /mnt/upgrade`

9. ☐	**PMAC Server**: Copy files	Execute the following commands on the PMAC guest to copy the required files from the TVOE host to the PMAC guest.
		Wildcards can be used as necessary.
		`$ sudo /usr/bin/scp -r admusr@<TVOE_management_ip_address>:/mnt/upgrade/upgrade/overlay/*`
		`/usr/TKLC/smac/etc/`

Step #	Procedure	Description

10. ☐	**PMAC Server**: Change permissions	Change the permission of TVOEclean.sh and TVOEcfg.sh file
		`$ sudo chmod 555 /usr/TKLC/smac/etc/TVOEclean.sh`
		`$ sudo chmod 555 /usr/TKLC/smac/etc/TVOEcfg.sh`
		`$ sudo chmod 555 /usr/TKLC/smac/etc/DSR_NOAM_FD_Blade.xml`
		`$ sudo chmod 555 /usr/TKLC/smac/etc/DSR_NOAM_FD_RMS.xml`

11.	**PMAC Server**: Unmount the application media	Remove the application media from the TVOE host: `$ sudo /bin/umount /mnt/upgrade`

12. ☐	**PMAC Server**: Copy IOS images	Copy IOS images into place (this copies both the 4948E and 3020 IOS images into place).
		5. Insert the Misc. Firmware media into the CD or USB drive of the management server.
		Insert the USB with the Firmware into an available USB slot on the TVOE host server.
		Note: The USB device is immediately added to the list of media devices once it is inserted into a USB slot on the TVOE host server.
		For this step, be sure to use the correct IOS version specified by the Release Notes of the HP Solutions Firmware Upgrade Pack, version 2.x.x [2]. Copy each IOS image called out by the Release Notes.
		6. Execute the following commands to copy the required files. Note that the <PMAC Management_IP Address> is the one used to deploy PMAC in section 4.1.3.
		`$ sudo /usr/bin/scp -r admusr@<PMAC_management_ip_address>:/media/<device directory>/files/<4948EF_IOS_image_filename> /var/TKLC/smac/image/`
		`$ sudo /usr/bin/scp -r admusr@<PMAC_management_ip_address>:/media/<device directory>/files/<2030(6120)_IOS_image_filename> /var/TKLC/smac/image/`
		7. Make sure you copy the images for all type of enclosure switches present by re-running the previous command.
		8. Remove the Misc. Firmware media from the drive.

13. ☐	Initialize PMAC application	1. Run the following commands:
		Note: If performing the setup on a redundant PMAC, do not initialize; skip this step and continue to step 17. .
		• If using IPv4:
		`$ sudo /usr/TKLC/smac/bin/pmacadm applyProfile --fileName=TVOE`
		`Profile successfully applied.`
		`$ sudo /usr/TKLC/smac/bin/pmacadm getPmacFeatureState`
		`PMAC Feature State = InProgress`

Step #	Procedure	Description

		$ sudo /usr/TKLC/smac/bin/pmacadm addRoute --gateway=<mgmt_IPv4gateway_address>
		--ip=0.0.0.0 --mask=0.0.0.0 --device=management
		Successful add of Admin Route
		$ sudo /usr/TKLC/smac/bin/pmacadm finishProfileConfig
		Initialization has been started as a background task
		• If using IPv6:
		$ sudo /usr/TKLC/smac/bin/pmacadm applyProfile --fileName=TVOE
		Profile successfully applied.
		$ sudo /usr/TKLC/smac/bin/pmacadm getPmacFeatureState
		PMAC Feature State = InProgress
		$ sudo /usr/TKLC/smac/bin/pmacadm addRoute --gateway=<IPv6mgmt_gateway_address>
		--ip=:: --mask=0 --device=management
		Successful add of Admin Route
		$ sudo /usr/TKLC/smac/bin/pmacadm finishProfileConfig
		Initialization has been started as a background task
		2. Wait for the background task to successfully complete.
		The command shows **IN_PROGRESS** for a short time.
		Run the following command until a **COMPETE** or **FAILED** response is seen similar to the following:
		$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks
		1: Initialize PMAC COMPLETE - PMAC initialized
		Step 2: of 2 Started: 2012-07-13 08:23:55 running: 29 sinceUpdate: 47
		taskRecordNum: 2 Server Identity:
		Physical Blade Location:
		Blade Enclosure:
		Blade Enclosure Bay:
		Guest VM Location:
		Host IP:
		Guest Name:
		TPD IP:
		Rack Mount Server:
		IP:
		Name:
		Note: Some expected networking alarms may display.

Step #	Procedure	Description

14. ☐	Perform system health check on PMAC	`$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus`
		This command should return no output on a healthy system.
		Note: An NTP alarm is detected if the system switches are not configured.
		`$ sudo /usr/TKLC/smac/bin/sentry status`
		All processes should be running and displaying output similar to the following:
		`PMAC Sentry Status`
		`sentryd started: Mon Jul 23 17:50:49 2012`
		`Current activity mode: ACTIVE`
		`Process PID Status StartTS NumR`
		`smacTalk 9039 running Tue Jul 24 12:50:29 2012 2`
		`smacMon 9094 running Tue Jul 24 12:50:29 2012 2`
		`hpiPortAudit 9137 running Tue Jul 24 12:50:29 2012 2`
		`snmpEventHandler 9176 running Tue Jul 24 12:50:29 2012 2`
		`eclipseHelp 9196 running Tue Jul 24 12:50:30 2012 2`
		`Fri Aug 3 13:16:35 2012`
		`Command Complete.`

15. ☐	Verify product release	Verify the PMAC application product release is as expected.
		`$ sudo /usr/TKLC/plat/bin/appRev`
		For example:
		`Install Time: Fri Sep 28 15:54:04 2012`
		`Product Name: PMAC`
		`Product Release: 5.0.0_50.10.0`
		`Part Number ISO: 872-2441-905`
		`Part Number USB: 872-2441-105`
		`Base Distro Product: TPD`
		`Base Distro Release: 6.0.0_80.22.0`
		`Base Distro ISO: TPD.install-6.0.0_80.22.0-CentOS6.2-x86_64.iso`
		`OS: OracleLinux 6.2`

16. ☐	Logout	Logout of the virsh console. Press **Ctrl-]** to exit the virtual PMAC console.
17. ☐	**PMAC Server**: Exit TVOE console	`$ logout` You may now close the iLO browser window.

4.2.3 Backup PMAC

Procedure 3. Set Up PMAC

Step #	Procedure	Description
This procedure configures the PMAC application guest environment on the management server TVOE hos and initializes the PMAC application. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**PMAC**: Login to PMAC	Login to PMAC as admusr.

2.
☐
	PMAC:
	Back up PMAC application
		`$ sudo /usr/TKLC/smac/bin/pmacadm backup`
		`PMAC backup has been successfully initiated as task ID 7`
		Note: The backup runs as a background task. To check the status of the background task use the PMAC GUI Task Monitor screen, or issue the command `$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`. The result should eventually be **PMAC Backup successful** and the background task should indicate **COMPLETE**.
		Note: The **pmacadm backup** command uses a naming convention that includes a date/time stamp in the filename (for example, backupPmac_20111025_100251.pef). In the example provided, the backup filename indicates it was created on 10/25/2011 at 10:02:51 am server time.

3.
☐
	PMAC:
	Verify backup was successful
		Note: If the background task shows the backup failed, then the backup did not complete successfully. STOP and contact My Oracle Support (MOS).
		The output of pmaccli getBgTasks should look similar to the example below:
		`$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`
		`2: Backup PMAC COMPLETE - PMAC Backup successful`
		`Step 2: of 2 Started: 2012-07-05 16:53:10 running: 4`
		`sinceUpdate: 2 taskRecordNum:`
		`2 Server Identity:`
		`Physical Blade Location:`
		`Blade Enclosure:`
		`Blade Enclosure Bay:`
		`Guest VM Location:`
		`Host IP:`
		`Guest Name:`
		`TPD IP:`
		`Rack Mount Server:`
		`IP:`
		`Name:`
		`::`

Step #	Procedure	Description
4.	**PMAC**: Save the backup	The PMAC backup must be moved to a remote server. Transfer (sftp, scp, rsync, or preferred utility), the PMAC backup to an appropriate remote server. The PMAC backup files are saved in the following directory: **/var/TKLC/smac/backup**.

4.3 Configure netConfig Repository

This procedure configures the netConfig repository for all required services and for each switch to be configured.

At any time, you can view the contents of the netConfig repository by using one of the following commands:

- For switches, use the command:

```
sudo /usr/TKLC/plat/bin/netConfig --repo listDevices
```

- For services, use the command:

```
sudo /usr/TKLC/plat/bin/netConfig --repo listServices
```

Users returning to this procedure after initial installation should run the above commands and note any devices and/or services that have already been configured. Duplicate entries cannot be added; if changes to a device repository entry are required, use the editDevice command. If changes to a services repository entry are necessary, you must delete the original entry first and then add the service again.

Terminology

The term **netConfig server** refers to the entity where netConfig is executed. This may be a virtualized or physical environment. **Management server** may also accurately describe this location, but has been historically used to describe the physical environment while **Virtual PMAC** was used to describe the virtualized netConfig server. Use of the term **netConfig server** to describe dual scenarios of physical and virtualized environments allow for future simplification of network configuration procedures.

Procedure Reference Tables

Steps within this procedure and subsequent procedures that require this procedure may refer to variable data indicated by text within "<>". Fill in these worksheets based on NAPD, and then refer back to these tables for the proper value to insert depending on your system type.

Variable	Value
<management_server_iLO_IP>	
<management_server_mgmt_IP_address>	
<netConfig_server_mgmt_IP_address>	
<switch_backup_user>	admusr
<switch_backup_user_password>	
<serial console type>	U=USB, c=PCIe

For the first aggregation switch (4948, 4948E, or 4948E-F), fill in the appropriate value for this site:

Variable	Value
<switch_hostname>	
<device_model>	

Variable	Value
<console_name>	
<switch_console_password>	
<switch_platform_username>	
<switch_platform_password>	
<switch_enable_password>	
<switch_mgmt_IP_address>	
<switch_mgmt_netmask>	
<mgmt_vlanID>	
<control_vlanID>	
<IOS_filename>	
<IP_version>	

For the second aggregation switch (4948, 4948E, or 4948E-F), fill in the appropriate value for this site:

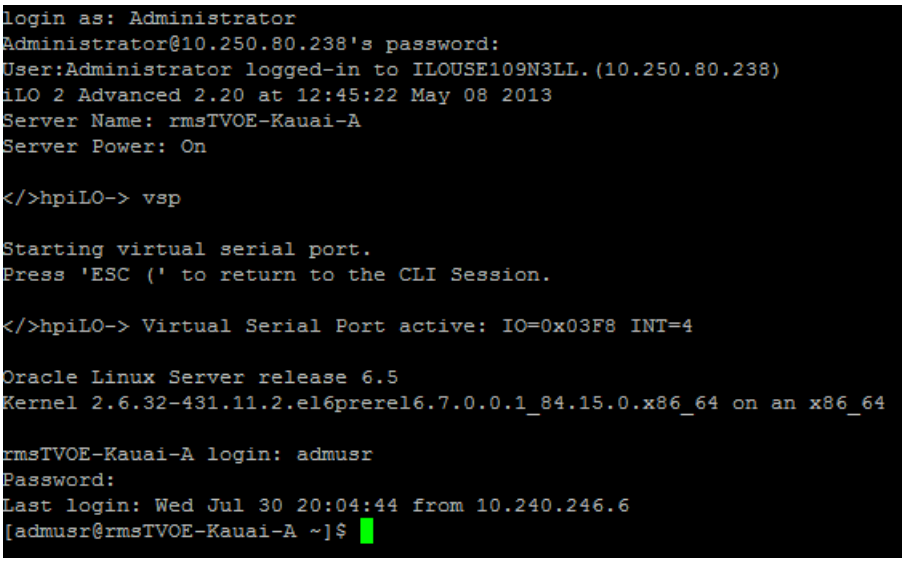
Variable	Value
<switch_hostname>	
<device_model>	
<console_name>	
<switch_console_password>	
<switch_platform_username>	
<switch_platform_password>	
<switch_enable_password>	
<switch_mgmt_IP_address>	
<switch_mgmt_netmask>	
<mgmt_vlanID>	
<control_vlanID>	
<IOS_filename>	
<IP_version>	

For each enclosure switch (6120XG, 6125G, 6125XLG, 6127XLG or 3020), fill in the appropriate value for this site (make as many copies of this table as needed).

Variable	Value
<switch_hostname>	

Variable	Value
<enclosure_switch_IP>	
<switch_platform_username>	
<switch_platform_password>	
<switch_enable_password>	
<io_bay>	
<OA1_enX_IP_address>	X= the enclosure #
<OA_password>	
<FW_image>	

Procedure 7. Configure netConfig Repository

Step #	Procedure	Description
This procedure configures the netConfig repository for all required services and for each switch to be configured. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Management Server iLO**: Login	1. Log into the management server iLO on the remote console using application provided passwords via Appendix C. 2. Log into the iLO in Internet Explorer using password provided by application: `http://<management_server_iLO_IP>` 3. Click the Remote Console tab and open the Integrate Remote Console on the server.  4. Click **Yes** if the security alert displays.

Step #	Procedure	Description

2. ☐	**Management Server**: Pre-check	If the installation is not designed for a virtual PMAC, go to step 3. .
		If there is a virtual PMAC, log into the console of the virtual PMAC.
		1. Verify virtual PMAC installation by issuing the following commands as **admusr** on the management server:
		`$ sudo /usr/bin/virsh list --all`
		`Id  Name  State`
		`6  vm-pmac1A running`
		2. If this command provides no output, it is likely that a virtual instance of PMAC is not installed.
		• If there is a virtual PMAC, log in to the console of the virtual PMAC.
		• If the installation is not designed for a virtual PMAC, go to step 3. .
		3. From the management server, log into the console of the virtual PMAC instance found above.
		Example:
		`$ sudo /usr/bin/virsh console vm-pmac1A`
		`Connected to domain vm-pmac1A`
		`Escape character is ^]`
		`<Press ENTER key>`
		`CentOS release 6.2 (Final)`
		`Kernel 2.6.32-220.7.1.el6prerel6.0.0_80.13.0.x86_64 on an x86_64`
		If the root user is already logged in, log out and log back in as **admusr**.
		`[root@pmac ~]# logout`
		`vm-pmac1A login: admusr`
		`Password:`
		`Last login: Fri May 25 16:39:04 on ttyS4`
		• If this command fails, it is likely that a virtual instance of PMAC is not installed.
		• If this is unexpected, refer to application documentation or My Oracle Support (MOS).

Step #	Procedure	Description

3. ☐	**netConfig Server**: Check switch templates directory	Make sure the switch templates directory exists.
		`$ /bin/ls -i /usr/TKLC/smac/etc/switch/xml`
		If the command returns an error:
		`ls: cannot access /usr/TKLC/smac/etc/switch/xml/: No such file or directory`
		Create the directory:
		`$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/switch/xml`
		Change directory permissions:
		`$ sudo /bin/chmod go+rx /usr/TKLC/smac/etc/switch/xml`
		Change directory ownership:
		`$ sudo /bin/chown -R pmacd:pmacbackup /usr/TKLC/smac/etc/switch`

4. ☐	**netConfig Server**: Set up netConfig repository with ssh information	Set up netConfig repository with necessary ssh information.
		1. Use netConfig to create a repository entry that uses the ssh service. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here.
		For a non-PMAC system:
		`$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=ssh_service`
		`Service type? (tftp, ssh, conserver, oa) ssh`
		`Service host? <netConfig_server_mgmt_IP_address>`
		`Enter an option name <q to cancel>: user`
		`Enter the value for user: <switch_backup_user>`
		`Enter an option name <q to cancel>: password`
		`Enter the value for password: <switch_backup_user_password>`
		`Verify Password: <switch_backup_user_password>`
		`Enter an option name <q to cancel>: q`
		`Add service for ssh_service successful`
		For a PMAC system:
		`admusr@belfast-pmac-1 ~]$ sudo netConfig --repo addService name=ssh_service`
		`Service type [ssh, oa, tftp, dhcp, conserver, oobm]? ssh`
		`SSH host IP :<IP_Address>SSH username : admusr`
		`SSH password :<admusr_password>`
		`Verify Password: <admusr_password>`
		`Add service for ssh_service successful`
		2. To ensure you entered the information correctly, use the following command and inspect the output, which is similar to the one shown below.
		`$ sudo /usr/TKLC/plat/bin/netConfig --repo showService name=ssh_service`
		`Service Name: ssh_service`

Step #	Procedure	Description
		Type: ssh Host: 10.250.8.4 Options: password: C20F7D639AE7E7 user: admusr
5. ☐	**netConfig Server**: Set up netConfig repository with tftp information	Set up netConfig repository with necessary tftp information. ***Note***: If there are no new Cisco (3020, 4948, 4948E or 4948E-F) switches to be configured, go to the next step. Use netConfig to create a repository entry that uses the tftp service. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here. • For a PMAC system: $ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=tftp_service Service type [dhcp, oa, oobm, ssh, tftp, conserver]? tftp TFTP host IP? : <netConfig_server_mgmt_IP_address> Directory on host? : /var/TKLC/smac/image/ Add service for tftp_service successful • For a non-PMAC system: $ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=tftp_service Service type? [tftp, ssh, conserver, oa] tftp TFTP host IP? : <netConfig_server_mgmt_IP_address> Directory on host? /var/lib/tftpboot/ Add service for tftp_service successful

Step #	Procedure	Description

6. ☐	**netConfig Server**: Set up netConfig repository with OA information	Set up netConfig repository with necessary OA information.
		Note: If there are no new HP 6125G/6125XLG/6120XG/6127XLG switches to configure, go to the next step.
		Use netConfig to create a repository entry that uses the OA service. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here.
		`$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=oa_service_en<enclosure #>`
		`Service type? [ssh, oa, tftp, dhcp, conserver, oobm]? oa`
		`Primary OA IP? <OA1_enX_ip_address>`
		`Secondary OA IP? <OA2_enX_ip_address>`
		`OA username? root`
		`OA password? <OA_password>`
		`Verify password:<OA_password>`
		`Add service for oa_service_en<enclosure #> successful`

7. ☐	**netConfig Server**: Run conserverSetup command, if aggregation switch is deployed	`$ sudo /usr/TKLC/plat/bin/conserverSetup –<serial console type> -s <management_server_mgmt_IP_address>`
		You are asked for the platcfg credentials.
		Example:
		`[admusr@vm-pmac1A]$ sudo /usr/TKLC/plat/bin/conserverSetup -u –s <management_server_mgmt_IP_address>`
		`Enter your platcfg username, followed by [ENTER]:platcfg`
		`Enter your platcfg password, followed by [ENTER]:<platcfg_password>`
		`Checking Platform Revision for local TPD installation...`
		`The local machine is running:`
		`Product Name: PMAC`
		`Base Distro Release: 7.6.1.0.0_88.55.0`
		`Checking Platform Revision for remote TPD installation...`
		`The remote machine is running:`
		`Product Name: TVOE`
		`Base Distro Release: 3.6.1.0.0_88.55.0`
		`Configuring switch 'switch1A_console' console server...Configured.`
		`Configuring switch 'switch1B_console' console server...Configured.`
		`Configuring iptables for port(s) 782...Configured.`
		`Configuring iptables for port(s) 1024:65535...Configured.`
		`Configuring console repository service...`
		`Repo entry for "console_service" already exists; deleting entry for:`

Step #	Procedure	Description

		`Service Name: console_service`
		`Type: conserver`
		`Host: <management_server_mgmt_IP_address>`
		`...Configured.`
		`Slave interfaces for bond0:`
		`bond0 interface: eth01`
		`bond0 interface: eth02`
		• If this command fails, contact My Oracle Support (MOS).
		• Verify the output of the script.
		• Verify your Product Release is based on Tekelec Platform 7.6.
		• Note the slave interface names of bond interfaces (<ethernet_interface_1> and <ethernet_interface_2>) for use in subsequent steps.

8. ☐	**netConfig Server**: Mount the HP Misc Firmware ISO	***Note***: If this is a Software Centric deployment, skip this step and proceed to step 9.
		`$ sudo /bin/mount -o loop /var/TKLC/upgrade/<misc_ISO> /mnt/upgrade`
		Example:
		`$ sudo /bin/mount -o loop /var/TKLC/upgrade/ 872-2161-113-2.1.10_10.26.0.iso /mnt/upgrade`

9. ☐	**netConfig Server**: Copy Cisco switch	***Note***: If there are no Cisco switches, skip to the next step.
		Copy Cisco switch FW to the `tftp_directory`.
		Note: If this is a Software Centric deployment, the customer must place the FW files for the Cisco switches (C3020, 4948/E/E-F) into the tftp directory listed below. Otherwise, perform the commands to copy the file from the FW ISO.
		For each Cisco switch model (C3020, 4948/E/E-F) present in the solution, copy the FW identified by `<FW_image>` in the aggregation switch variable table (4948) or enclosure switch variable table (C3020) to the `tftp_service` directory and change the permissions of the file:
		• For a PMAC system:
		`<tftp_directory> = /var/TKLC/smac/image/`
		• For a non-PMAC system:
		`<tftp_directory> = /var/lib/tftpboot/`
		`$ sudo /bin/chmod 644 <tftp_directory/<FW_image>`
		Example:
		`$ sudo /bin/chmod 644 /var/TKLC/smac/image/cat4500e-entservicesk9-mz.122-54.XO.bin`

Step #	Procedure	Description

10. ☐	**netConfig Server**: Copy HP switch	***Note***: If there are no HP switches, skip to the next step.
		Copy HP switch FW to the `ssh` directory
		Note: If this is a Software Centric deployment, the customer must place the FW files for the HP switches into ssh directory listed below. Otherwise, perform the commands to copy the file from the FW ISO.
		For each HP switch model (HP6125G/XLG, HP6120XG, 6127XLG) present in the solution, copy the FW identified by `<FW_image>` in the enclosure switch variable tables to the `ssh_service` directory and change the permissions of the file:
		`$ sudo /bin/cp /mnt/upgrade/files/<FW_image> ~<switch_backup_user>/`
		`$ sudo /bin/chmod 644 ~<switch_backup_user>/<FW_image>`
		Example:
		`$ sudo /bin/cp /mnt/upgrade/files/Z_14_37.swi ~admusr/`
		`$ sudo /bin/chmod 644 ~admusr/Z_14_37.swi`

11. ☐	**netConfig Server**: Unmount ISO	`$ sudo /bin/umount /mnt/upgrade`

12. ☐	**netConfig Server**: Set up netConfig repository	***Note***: If there are no new aggregation switches to be configured, go to the next step.
		Set up netConfig repository with aggregation switch information.
		Use netConfig to create a repository entry for each switch. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here.
		• The <device_model> can be 4948, 4948E, or 4948E-F depending on the model of the device. If you do not know, stop now and contact My Oracle Support (MOS).
		• The device name must be 20 characters or less.
		`$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname> --reuseCredentials`
		`Device Vendor [Cisco, HP]? Cisco`
		`Device Model [3020, 4948, 4948E, 4948E-F, 9372TX-E]? <device_model>`
		`What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management?: <switch_mgmt_IP_address>`
		`Is the management interface a port or a vlan? [vlan]: [Enter]`
		`What is the VLAN ID of the management VLAN? [2]: [mgmt_vlanID]`
		`What is the name of the management VLAN? [management]: [Enter]`
		`What switchport connects to the management server? [GE40]: [Enter]`

Step #	Procedure	Description

		What is the switchport mode (access|trunk) for the management server port? [trunk]: [Enter]
		What are the allowed vlans for the management server port? [1,2]: <control_vlanID>, <mgmt_vlanID>
		Enter the name of the firmware file [cat4500e-entservicesk9-mz.122-54.XO.bin]: <IOS_filename>
		Firmware file to be used in upgrade: <IOS_filename>
		Enter the name of the upgrade file transfer service: tftp_service
		File transfer service to be used in upgrade: tftp_service
		Should the init oob adapter be added (y/n)? y
		Adding consoleInit protocol for <switch_hostname> using oob...
		What is the name of the service used for OOB access? console_service
		What is the name of the console for OOB access? <console name>
		What is the platform access username? root
		What is the device console password? <switch_console_password>
		Verify password: <switch_console_password>
		What is the platform user password? <switch_platform_password>
		Verify password: <switch_platform_password>
		What is the device privileged mode password? <switch_enable_password>
		Verify password: <switch_enable_password>
		Should the live network adapter be added (y/n)? y
		Adding cli protocol for <switch_hostname> using network...
		Network device access already set: <switch_mgmt_IP_address>
		Should the live oob adapter be added (y/n)? y
		Adding cli protocol for <switch_hostname> using oob...
		OOB device access already set: console_service
		Device named <switch_hostname> successfully added.
		Refer to Step 7 to know the console details
		To check you entered the information correctly, use the following command:
		$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname>
		and check the output, which is similar to the one shown:
		$ sudo /usr/TKLC/plat/bin/netConfig –-repo showDevice name=<switch_hostname>
		Device: <switch_hostname>
		Vendor: Cisco
		Model: <device_model>
		Platform Rev: 0

Step #	Procedure	Description
		FW Ver: 0 FW Filename: <IOS_image> FW Service: tftp_service Initialization Management Options mgmtIP: <switch_mgmt_IP_address> mgmtInt: vlan mgmtVlan: <mgmt_vlanID> mgmtVlanName: management interface: GE40 mode: trunk allowedVlans: <control_vlanID>, <mgmt_vlanID> Access: Network: <switch_mgmt_IP_address> Access: OOB: Service: console_service Console: <console_name> Init Protocol Configured Live Protocol Configured Repeat this step for each 4948/4948E /4948 E-F, using appropriate values for those switches.
13. ☐	**netConfig Server**: Set up netConfig repository	***Note***: If there are no new 3020s to be configured, go to the next step. Set up netConfig repository with 3020 switch information. ***Note***: The Cisco 3020 is not compatible with IPv6 management configuration. Use netConfig to create a repository entry for each 3020. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here. • If you do not know any of the required answers, stop now and contact My Oracle Support (MOS). • The device name must be 20 characters or less. $ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname> --reuseCredentials Device Vendor? Cisco Device Model? 3020 What is the management address? <enclosure_switch_ip> Enter the name of the firmware file [cbs30x0-ipbasek9-tar.122-58.SE1.tar]: <FW_image> Firmware file to be used in upgrade: <IOS_image> Enter the name of the upgrade file transfer service: <tftp_service> File transfer service to be used in the upgrade: <tftp_service> Should the init network adapter be added (y/n)? y

Step #	Procedure	Description

		Adding netBootInit protocol for <switch_hostname> using network...
		Network device access already set: <enclosure_switch_ip>
		What is the platform access username?
		<switch_platform_username>
		What is the platform user password?
		<switch_platform_password>
		Verify password: <switch_platform_password>
		What is the device privileged mode password?
		<switch_enable_password>
		Verify password: <switch_enable_password>
		Should the init file adapter be added (y/n)? y
		Adding netBootInit protocol for <switch_hostname> using file...
		What is the name of the service used for TFTP access?
		tftp_service
		Should the live network adapter be added (y/n)? y
		Adding cli protocol for <switch_hostname> using network...
		Network device access already set: <enclosure_switch_ip>
		Device named <switch_hostname> successfully added.
		To check you entered the information correctly, use the following command:
		$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname>
		and check the output, which is similar to the one shown below.
		$ sudo /usr/TKLC/plat/bin/netConfig –-repo showDevice name=<switch_hostname>
		Device: <switch_hostname>
		Vendor: Cisco
		Model: <device_model>
		FW Ver: 0
		FW Filename: <FW_image>
		FW Service: tftp_service
		Access: Network: <enclosure_switch_IP>
		Init Protocol Configured
		Live Protocol Configured
		Repeat this step for each 3020, using appropriate values for those 3020s.
		Note: If you receive this WARNING, it means the <FW_image> is not found in the directory named in the FW Service. For the ssh_service, it is the user's home directory. For tftp_service, it is normally /var/TKLC/smac/image:
		WARNING: Could not find firmware file on local host. If using a local service, please update the device entry using the editDevice command or copy the file to the correct location.

Step #	Procedure	Description

14. ☐	**netConfig Server**: Set up netConfig repository	***Note***: If there are no 6120XGs to be configured, stop and continue with the appropriate switch configuration procedure.
		
		Set up netConfig repository with HP 6120XG switch information.
		
		Use netConfig to create a repository entry for each 6120XG. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here.
		
		• If you do not know any of the required answers, stop now and contact My Oracle Support (MOS).
		
		• The device name must be 20 characters or less.
		
		`$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname> --reuseCredentials`
		`Device Vendor? HP`
		`Device Model? 6120`
		`What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management?: <switch_mgmt_IP_address>`
		`Enter the name of the firmware file [Z_14_37.swi]: <FW_image>`
		`Firmware file to be used in upgrade: <FW_image>`
		`Enter the name of the upgrade file transfer service: ssh_service`
		`File transfer service to be used in upgrade: ssh_service`
		`Should the init oob adapter be added (y/n)? y`
		`Adding consoleInit protocol for <switch_hostname> using oob...`
		`What is the name of the service used for OOB access? oa_service_en<enclosure #>`
		`What is the name of the console for OOB access? <io_bay>`
		`What is the platform access username? <switch_platform_username>`
		`What is the device console password? <switch_platform_password>`
		`Verify password: <switch_platform_password>`
		`What is the platform user password? <switch_platform_password>`
		`Verify password: <switch_platform_password>`
		`What is the device privileged mode password? <switch_platform_password>`
		`Verify password: <switch_platform_password>`
		`Should the live network adapter be added (y/n)? y`
		`Adding cli protocol for <switch_hostname> using network...`
		`Network device access already set: <switch_mgmt_IP_address>`
		`Should the live oob adapter be added (y/n)? y`
		`Adding cli protocol for <switch_hostname> using oob...`

Step #	Procedure	Description

		`OOB device access already set: oa_service_en<enclosure #>`
		`Device named <switch_hostname> successfully added`
		The image is being unpacked and validated. This takes approximately 4 minutes. Once the unpacking, validation, and rebooting have completed, you are returned to the normal prompt. Proceed with the next step.
		To verify you entered the information correctly, use the following command:
		`$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname>`
		and check the output, which is similar to the one shown:
		`$ sudo /usr/TKLC/plat/bin/netConfig –-repo showDevice name=<switch_hostname>`
		`Device: <switch_hostname>`
		`Vendor: HP`
		`Model: 6120`
		`FW Ver: 0`
		`FW Filename: <FW_image>`
		`FW Service: ssh_service`
		`Initialization Management Options`
		`mgmtIP: <enclosure_switch_IP>`
		`Access: Network: <enclosure_switch_IP>`
		`Access: OOB:`
		`Service: oa_service`
		`Console: <console_name>`
		`Init Protocol Configured`
		`Live Protocol Configured`
		Repeat this step for each 6120, using appropriate values for those 6120s.
		Note: If you receive this WARNING, it means the <FW_image> is not found in the directory named in the FW Service. For the ssh_service, it is the user's home directory. For tftp_service, it is normally /var/TKLC/smac/ image:
		WARNING: Could not find firmware file on local host. If using a local service, please update the device entry using the editDevice command or copy the file to the correct location.

Step #	Procedure	Description

15. ☐	**netConfig Server**: Set up netConfig repository	***Note***: If there are no 6125Gs to be configured, stop and continue with the appropriate switch configuration procedure.
		
		Set up netConfig repository with HP 6125G switch information.
		
		Use netConfig to create a repository entry for each 6125G. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here.
		
		• If you do not know any of the required answers, stop now and contact My Oracle Support (MOS).
		
		• The device name must be 20 characters or less.
		
		`$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname> --reuseCredentials`
		`Device Vendor? HP`
		`Device Model? 6125`
		`What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management? <switch_mgmt_IP_address>`
		`Enter the name of the firmware file [6125-CMW520-R2105.bin]: <FW_image>`
		`Firmware file to be used in upgrade: <FW_image>`
		`Enter the name of the upgrade file transfer service: ssh_service`
		`Should the init oob adapter be added (y/n)? y`
		`Adding consoleInit protocol for <switch_hostname> using oob...`
		`What is the name of the service used for OOB access? oa_service_en<enclosure #>`
		`What is the name of the console for OOB access? <io_bay>`
		`What is the platform access username? <switch_platform_username>`
		`What is the device console password? <switch_platform_password>`
		`Verify password: <switch_platform_password>`
		`What is the platform user password? <switch_platform_password>`
		`Verify password: <switch_platform_password>`
		`What is the device privileged mode password? <switch_platform_password>`
		`Verify password: <switch_platform_password>`
		`Should the live network adapter be added (y/n)? y`
		`Adding cli protocol for <switch_hostname> using network...`
		`Network device access already set: <switch_mgmt_IP_address>`
		`Should the live oob adapter be added (y/n)? y`
		`Adding cli protocol for <switch_hostname> using oob...`
		`OOB device access already set: oa_service_en<enclosure #>`

Step #	Procedure	Description

		`Device named <switch_hostname> successfully added.`
		Note: If you receive this WARNING, it means the <FW_image> is not found in the directory named in the FW Service. For the ssh_service, it is the user's home directory. For tftp_service, it is normally /var/TKLC/smac/image:
		WARNING: Could not find firmware file on local host. If using a local service, please update the device entry using the editDevice command or copy the file to the correct location.
		To verify you entered the information correctly, use the following command:
		`$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname>`
		and check the output, which is similar to the one shown:
		`$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname>`
		`Device: <switch_hostname>`
		`Vendor: HP`
		`Model: 6125`
		`FW Ver: 0`
		`FW Filename: <FW_image>`
		`FW Service: ssh_service`
		`Access: Network: <enclosure_switch_IP>`
		`Access: OOB:`
		`Service: oa_service`
		`Console: <io_bay>`
		`Init Protocol Configured`
		`Live Protocol Configured`

16.	**netConfig Server**: Set up netConfig repository	***Note***: If there are no 6125XLGs to be configured, stop and continue with the appropriate switch configuration procedure.
		Set up netConfig repository with HP 6125XLG switch information.
		Use netConfig to create a repository entry for each 6125XLG. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here.
		• If you do not know any of the required answers, stop now and contact My Oracle Support (MOS).
		• The device name must be 20 characters or less.
		`$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname> --reuseCredentials`
		`Device Vendor? HP`
		`Device Model? 6125XLG`
		`What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management?: <switch_mgmt_IP_address>`

Step #	Procedure	Description
		Enter the name of the firmware file [6125XLG-CMW710-R2403.ipe]: <FW_image> Firmware file to be used in upgrade: <FW_image> Enter the name of the upgrade file transfer service: ssh_service File transfer service to be used in upgrade: ssh_service Should the init oob adapter be added (y/n)? y Adding consoleInit protocol for <switch_hostname> using oob... What is the name of the service used for OOB access? oa_service_en<enclosure#> What is the name of the console for OOB access? <io_bay> What is the platform access username? <switch_platform_username> What is the device console password? <switch_platform_password> Verify password: <switch_platform_password> What is the platform user password? <switch_platform_password> Verify password: <switch_platform_password> What is the device privileged mode password? <switch_platform_password> Verify password: <switch_platform_password> Should the live network adapter be added (y/n)? y Adding cli protocol for <switch_hostname> using network... Network device access already set: <switch_mgmt_IP_address> Should the live oob adapter be added (y/n)? y Adding cli protocol for <switch_hostname> using oob... OOB device access already set: oa_service_en<enclosure #> Device named <switch_hostname> successfully added ***Note***: If you receive this WARNING, it means the <FW_image> is not found in the directory named in the FW Service. For the ssh_service, it is the user's home directory. For tftp_service, it is normally /var/TKLC/smac/image: ***WARNING***: Could not find firmware file on local host. If using a local service, please update the device entry using the editDevice command or copy the file to the correct location. To verify you entered the information correctly, use the following command: $ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname> and check the output, which is similar to the one shown: $ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname> Device: <switch_hostname> Vendor: HP Model: 6125XLG

Step #	Procedure	Description
		FW Ver: 0 FW Filename: <FW_image> FW Service: ssh_service Access: Network: <enclosure_switch_IP> Access: OOB: Service: oa_service Console: <io_bay> Init Protocol Configured
17.	**netConfig Server:** Set up netConfig repository	***Note***: If there are no 6127XLGs to be configured, stop and continue with the appropriate switch configuration procedure. Set up netConfig repository with HP 6127XLG switch information. Use netConfig to create a repository entry for each 6127XLG. This command provides the user with several prompts. The prompts shown with <variables> asthe answers are site specific that the user MUST modify. Other prompts that donot have a <variable> shown as the answer must be entered EXACTLY as they are shown here. • If you do not know any of the required answers, stop now and contact My Oracle Support (MOS). • The device name must be 20 characters or less. $ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname> --reuseCredentials Device Vendor? HP Device Model? 6127XLG What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management?: <switch_mgmt_IP_address> Enter the name of the firmware file [6127XLG-CMW710-R2403.ipe]: <FW_image> Firmware file to be used in upgrade: <FW_image> Enter the name of the upgrade file transfer service: ssh_service File transfer service to be used in upgrade: ssh_serviceShould the init oob adapter be added (y/n)? y Adding consoleInit protocol for <switch_hostname> using oob... What is the name of the service used for OOB access? oa_service_en<enclosure#> What is the name of the console for OOB access? <io_bay> What is the platform access username? <switch_platform_username> What is the device console password? <switch_platform_password> Verify password: <switch_platform_password>What is the platform user password? <switch_platform_password> Verify password: <switch_platform_password> What is the device privileged mode password? <switch_platform_password> Verify password: <switch_platform_password>

```
Should the live network adapter be added (y/n)? y
Adding cli protocol for <switch_hostname> using network...
Network device access already set: <switch_mgmt_IP_address>
Should the live oob adapter be added (y/n)? y
Adding cli protocol for <switch_hostname> using oob...
OOB device access already set: oa_service_en<enclosure #>
Device named <switch_hostname> successfully added
```

Note: If you receive this WARNING, it means the <FW_image> is not found inthe directory named in the FW Service. For the ssh_service, it is the user's home directory. For tftp_service, it is normally /var/TKLC/smac/ image:

WARNING: Could not find firmware file on local host. If using a local service, please update the device entry using the editDevicecommand or copy the file to the correct location.

To verify you entered the information correctly, use the following command:

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice
name=<switch_hostname>
```

and check the output, which is similar to the one shown:

```
$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice
name=<switch_hostname>
  Device: <switch_hostname>
      Vendor: HP

Model: 6127XLG
      FW Ver: 0
      FW Filename: <FW_image>
      FW Service: ssh_service
      Access: Network: <enclosure_switch_IP>
      Access: OOB:
                  Service: oa_service
                  Console: <io_bay>

Init Protocol Configured
```

4.3.1 Configure Aggregation Switches

4.3.1.1 Configure Cisco 4948/4948E-F Aggregation Switches (PMAC Installed) (netConfig)

This procedure configures 4948/4948E/4948E-F switches with an appropriate IOS and configuration from a single management server and virtual PMAC for use with the c-Class or RMS platform.

Procedure Reference Tables

Steps within this procedure may refer to variable data indicated by text within "<>". Refer to this table for the proper value to insert depending on your system type. Fill in the appropriate value from HP Solutions Firmware Upgrade Pack, version 2.x.x [2].

Variable	Cisco 4948	Cisco 4948E	Cisco 4948E-F
<IOS_image_file>			

Fill in the appropriate value for this site.

Variable	Value
<switch_platform_username>	See referring application documentation

<switch_platform_password>	
<switch_console_password>	
<switch_enable_password>	
<management_server_mgmt_IP_address>	
<pmac_mgmt_IP_address>	
<switch_mgmtVLAN_ID>	
<switch1A_mgmtVLAN_IP_address>	
<mgmt_Vlan_subnet_ID>	
<netmask>	
<switch1B_mgmtVLAN_IP_address>	
<switch_Internal_VLANS_list>	
<management_server_mgmtInterface>	

Variable	Value
<management_server_iLO_IP>	
<customer_supplied_ntp_server_address>	
<platcfg_password> Initial password as provided by Oracle	
<management_server_mgmtInterface> Value gathered from NAPD	
<switch_backup_user>	admusr
<switch_backup_user_password> Check application documentation	

Notes:

- The onboard administrators are not available during the configuration of Cisco 4948/4948E/4948E-F switches.
- Uplinks must be disconnected from the customer network before executing this procedure. One of the steps in this procedure instructs when to reconnect these uplink cables. Refer to the application appropriate schematic or procedure for determining which cables are used for customer uplink.

Procedure 8. Configure Cisco

Step #	Procedure	Description
This procedure configures 4948/4948E/4948E-F switches with an appropriate IOS and configuration from a single management server and virtual PMAC for use with the c-Class or RMS platform. ***Needed Material***: • HP MISC firmware ISO image • Release Notes of the HP Solutions Firmware Upgrade Pack, version 2.x.x [2] • Template xml files on the application media. ***Note***: Filenames and sample command line input/output throughout this section do not specifically reference the 4948E-F. Template settings are identical between the 4948E and 4948E-F. The original 4948 switch – as opposed to the 4948E or the 4948E-F is referred to simply by the model number 4948. Where all three switches are referred to, this is made clear by reference to 4948/4948E/4948E-F switches. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Virtual PMAC**: Verify IOS image is on the system	Determine if the IOS image for the 4948/4948E/4948E-F is on the PMAC. `$ /bin/ls -i /var/TKLC/smac/image/<IOS_image_file>` If the file exists, skip the remainder of this step and continue with the next step. If the file does not exist, copy the file from the firmware media and ensure the file is specified by the Release Notes of the HP Solutions Firmware Upgrade Pack, version 2.x.x [2].

Step #	Procedure	Description

2. ☐	**Virtual PMAC**: Modify P&C feature to allow TFTP	Enable the DEVICE.NETWORK.NETBOOT feature with the management role to allow tftp traffic:
		`$ sudo /usr/TKLC/smac/bin/pmacadm editFeature --featureName=DEVICE.NETWORK.NETBOOT --enable=1`
		`$ sudo /usr/TKLC/smac/bin/pmacadm resetFeatures`
		Note: Ignore the sentry restart instructions.
		Note: This may take up to 60 seconds to complete.

3. ☐	**Virtual PMAC > Management Server**: Manipulate host server physical interfaces	Exit from the virtual PMAC console, by pressing **ctrl-]** and you are returned to the server prompt.
		Ensure the interface of the server connected to switch1A is the only interface up and obtain the IP address of the management server management interface by performing the following commands:
		`$ sudo /sbin/ifup <ethernet_interface_1>`
		`$ sudo /sbin/ifdown <ethernet_interface_2>`
		`$ sudo /sbin/ip addr show <management_server_mgmtInterface> | grep inet`
		The command output should contain the IP address of the variable, <management_server_mgmt_IP_address>
		`$ sudo /usr/bin/virsh console vm-pmac1A`
		Note: On a TVOE host, if you open the virsh console, i.e., $ `sudo virsh console X`" or from the virsh utility "virsh # `console X`" command and you get garbage characters or output is not correct, then more than likely there is a stuck "virsh console" command already being run on the TVOE host. Exit the virsh console, and run `ps -ef |grep virsh`, then kill the existing process"$ `sudo kill -9 <PID>`. Execute the $ `sudo virsh console X` command again. Your console session should now run as expected.

Step #	Procedure	Description
4. ☐	**Virtual PMAC**: Determine if switch1A PROM upgrade is required	***Note***: ROM & PROM are intended to have the same meaning for this procedure. Connect to switch1A, check the PROM version. Connect serially to switch1A by issuing the following command. `$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg switch1A_console` `Enter platcfg@pmac5000101's password: <platcfg_password>` `[Enter `^Ec?' for help]` `Press Enter` `Switch> show version | include ROM` `ROM: 12.2(31r)SGA1` `System returned to ROM by reload` ***Note***: If the console command fails, contact My Oracle Support (MOS). Note the IOS image and ROM version for comparison in a following step. Exit from the console by pressing **<ctrl-e><c><.>** and you are returned to the server prompt. Verify the version from the previous command against the version from the release notes referenced. If the versions are different, perform the procedure in Appendix G to upgrade the PROM for switch1A.

Step #	Procedure	Description

5. ☐	**Virtual PMAC**: Extract configuration files	Extract the configuration files from the ZIP file copied in Step 9. of Procedure 5.
		`$ cd /usr/TKLC/smac/etc`
		`$ sudo unzip DSR_NetConfig_Templates.zip`
		`$ sudo chown -R admusr.admgrp DSR_NetConfig_Templates`
		This creates a directory called **DSR_NetConfig_Templates**, which contains the configuration files for all the supported deployments. Copy the necessary init file from **init/Aggregation** and the necessary config files from **config/TopoX** (where X refers to the appropriate topology) using the following commands. Make sure to replace **X** with the appropriate Topology number.
		Note: The following workaround is needed:
		Remove the double right brackets for:
		DSR_NetConfig_Templates/Topo1_L2/4948E-F_L2_configure.xml: <option name="type">access</option>>
		DSR_NetConfig_Templates/Topo4/6125XLG_Pair-2_template_configure.xml: <!-- Multiple VLANs can be entered by stringing the VLANs in the setAllowedVlans option, i.e., 1-5 or 1,2,3,4,5 -->>
		DSR_NetConfig_Templates/Topo1_L3/3020_template_configure.xml: <!-- 'mode' is required on Cisco when adding interfaces -->>
		Replace <configure> with <configure apiVersion="1.1"> within: DSR_NetConfig_Templates/utility/addQOS_trafficeTemplate_6120XG.x ml
		`# sudo cp DSR_NetConfig_Templates/init/Aggregation/* /usr/TKLC/smac/etc/switch/xml/`
		`# sudo cp DSR_NetConfig_Templates/config/TopoX/* /usr/TKLC/smac/etc/switch/xml/`

6. ☐	**Virtual PMAC**: Modify switch1A_4948_4948E.xml and switch1B_4948_4948E.xml	Modify switch1A_4948_4948E_init.xml and switch1B_4948_4948E_init.xml files for information needed to initialize the switch. Update the init.xml files for all values preceded by a dollar sign. For example, if a value has $some_variable_name, that value is modified and the dollar sign must be removed during the modification. When done editing the file, save and exit to return to the command prompt
7. ☐	**Virtual PMAC**: Modify 4948E-F_configure.xml	Modify 4948E-F_configure.xml for information needed to configure the switches. Update the configure.xml file for all values preceded by a dollar sign. For example, if a value has $some_variable_name, that value is modified and the dollar sign must be removed during the modification. When done editing the file, save and exit to return to the command prompt. ***Note***: For IPv6 Configurations, IPv6 over NTP is NOT currently supported on the Cisco 4948E-F aggregation switches. This function must be configured for IPv4.

Step #	Procedure	Description

8. ☐	**Virtual PMAC**: Initialize switch1A	Initialize switch1A by issuing the following command:
		`$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml`
		`Processing file: /usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml`
		Note: This step takes about 5-10 minutes to complete. Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact My Oracle Support (MOS).
		A successful completion of netConfig returns you to the prompt.
		Use netConfig to get the hostname of the switch, to verify the switch was initialized properly, and to verify netConfig can connect to the switch.
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getHostname`
		`Hostname: switch1A`
		Note: If this command fails, stop this procedure and contact My Oracle Support (MOS).

9. ☐	**Virtual PMAC**: Verify IOS image	Verify the switch is using the proper IOS image per Platform version by issuing the following commands:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getFirmware`
		`Version: 122-54.XO`
		`License: entservicesk9`
		`Flash: cat4500e-entservicesk9-mz.122-54.XO.bin`

Step #	Procedure	Description

10. ☐	**Virtual PMAC > Management Server**: Manipulate host server physical interfaces	Exit from the virtual PMAC console, by pressing **ctrl-]** and you are returned to the server prompt.
		Ensure the interface of the server connected to switch1B is the only interface up and obtain the IP address of the management server management interface by performing the following commands:
		`$ sudo /sbin/ifup <ethernet_interface_1>`
		`$ sudo /sbin/ifdown <ethernet_interface_2>`
		`$ sudo /sbin/ip addr show <management_server_mgmtInterface> | grep inet`
		The command output should contain the IP address of the variable, <management_server_mgmt_IP_address>
		Connect to the Virtual PMAC by logging into the console of the virtual PMAC instance found in Step 2. of Procedure 7.
		`$ sudo /usr/bin/virsh console vm-pmac1A`
		Note: On a TVOE host, if you open the virsh console, for example, `$ sudo /usr/bin/virsh console X` or from the virsh utility `virsh # console X` command and you get garbage characters or the output is not correct, then there is likely a stuck **virsh console** command already being run on the TVOE host. Exit out of the virsh console, run `ps -ef |grep virsh`, and then kill the existing process `"kill -9 <PID>`. Then execute the `virsh console X` command. Your console session should now run as expected.

11. ☐	**Virtual PMAC**: Determine if switch1B PROM upgrade is required	***Note***: ROM & PROM are intended to have the same meaning for this procedure. Connect to switch1A, check the PROM version. Connect serially to switch1A by issuing the following command. `$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg switch1A_console` `Enter platcfg@pmac5000101's password: <platcfg_password>` `[Enter `^Ec?' for help]` `Press Enter` `Switch> show version | include ROM` `ROM: 12.2(31r)SGA1` `System returned to ROM by reload` ***Note***: If the console command fails, contact My Oracle Support (MOS). Note the IOS image and ROM version for comparison in a following step. Exit from the console by pressing **<ctrl-e><c><.>** and you are returned to the server prompt. Verify the version from the previous command against the version from the release notes referenced. If the versions are different, perform the procedure in Appendix G to upgrade the PROM for switch1B.

Step #	Procedure	Description

12. ☐	**Virtual PMAC**: Initialize switch1B	Initialize switch1B by issuing the following command:
		`$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml`
		`Processing file: /usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml`
		Note: This step takes about 5-10 minutes to complete. Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact My Oracle Support (MOS).
		A successful completion of netConfig returns you to the prompt.
		Use netConfig to get the hostname of the switch, to verify the switch was initialized properly, and to verify netConfig can connect to the switch.
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getHostname`
		`Hostname: switch1B`
		Note: If this command fails, stop this procedure and contact My Oracle Support (MOS).

13. ☐	**Virtual PMAC**: Verify IOS image	Verify the switch is using the proper IOS image per Platform version by issuing the following commands:
		`$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getFirmware`
		`Version: 122-54.XO`
		`License: entservicesk9`
		`Flash: cat4500e-entservicesk9-mz.122-54.XO.bin`

14. ☐	**Virtual PMAC**: Disable TFTP	Modify PMAC Feature to disable TFTP.
		Disable the DEVICE.NETWORK.NETBOOT feature.
		`$ sudo /usr/TKLC/smac/bin/pmacadm editFeature --featureName=DEVICE.NETWORK.NETBOOT --enable=0`
		`$ sudo /usr/TKLC/smac/bin/pmacadm resetFeatures`
		Note: This may take up to 60 seconds to complete.

15. ☐	**Virtual PMAC**: Configure both switches	Configure both switches by issuing the following command:
		`$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch/xml/4948_4948E_configure.xml`
		`Processing file: /usr/TKLC/smac/etc/switch/xml/4948_4948E_configure.xml`
		Note: This may take up to 2-3 minutes to complete.
		Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact My Oracle Support (MOS).
		A successful completion of netConfig returns the user to the prompt.

Step #	Procedure	Description

16. ☐	**Management Server**: Ensure interface are enabled on the TVOE host	Press **Ctrl-]** to exit the virtual PMAC console. This returns the terminal to the server prompt.
		Ensure the interfaces of the server connected to switch1A and switch1B are up by performing the following commands:
		`$ sudo /sbin/ifup <ethernet_interface_1>`
		`$ sudo /sbin/ifup <ethernet_interface_2>`

17. ☐	**Cabinet**: Connect cables from customer network	Attach switch1A customer uplink cables. Refer to application documentation for which ports are uplink ports. ***Note***: If the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active.

18. ☐	**Virtual PMAC**: Verify access to customer network	Verify connectivity to the customer network by issuing the following command:
		`$ /bin/ping <customer_supplied_ntp_server_address>`
		`PING ntpserver1 (10.250.32.51) 56(84) bytes of data.`
		`64 bytes from ntpserver1 (10.250.32.51): icmp_seq=0 ttl=62 time=0.150 ms`
		`64 bytes from ntpserver1 (10.250.32.51): icmp_seq=1 ttl=62 time=0.223 ms`
		`64 bytes from ntpserver1 (10.250.32.51): icmp_seq=2 ttl=62 time=0.152 ms`

19. ☐	**Cabinet**: Connect cables from customer network	Attach switch1B customer uplink cables and detach switch1A customer uplink cables. Refer to application documentation for which ports are uplink ports. ***Note***: If the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active.

20. ☐	**Virtual PMAC**: Verify access to customer network	Verify connectivity to the customer network by issuing the following command:
		`$ /bin/ping <customer_supplied_ntp_server_address>`
		`PING ntpserver1 (10.250.32.51) 56(84) bytes of data.`
		`64 bytes from ntpserver1 (10.250.32.51): icmp_seq=0 ttl=62 time=0.150 ms`
		`64 bytes from ntpserver1 (10.250.32.51): icmp_seq=1 ttl=62 time=0.223 ms`
		`64 bytes from ntpserver1 (10.250.32.51): icmp_seq=2 ttl=62 time=0.152 ms`

21. ☐	**Cabinet**: Connect cables from customer network	Re-attach switch1A customer uplink cables. Refer to application documentation for which ports are uplink ports. ***Note***: If the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active.
22. ☐	**Management Server**: Restore the TVOE host back to its original state	Press **Ctrl-]** to exit the virtual PMAC console. This returns the terminal to the server prompt. Restore the server networking back to original state: `$ sudo /sbin/service network restart`

Step #	Procedure	Description
23. ☐	Back up switch and/or enclosure switch	Perform Appendix H.2 for each switch configured in this procedure.

4.4 Configure PMAC for NetBackup (Optional)

4.4.1 Configure NetBackup Feature

If the PMAC application is configured with the optional NetBackup feature and NetBackup client is installed on this server, execute Procedure 9 with the appropriate NetBackup feature data; otherwise, continue to Procedure 10 which installs and configures the NetBackup client software on PMAC.

Procedure 8. Configure PMAC Application

Step #	Procedure	Description
Configuration of the PMAC application is typically performed using the PMAC GUI. This procedure defines application and network resources. At a minimum, you should define network routes and DHCP pools. Unlike initialization, configuration is incremental, so you may execute this procedure to modify the PMAC configuration. ***Note***: The installer must know the network and application requirements. The final step configures and restarts the network and the PMAC application; network access is briefly interrupted. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as pmacadmin user. Navigate to **Administration > PMAC Configuration**.

Step #	Procedure	Description
2. ☐	**PMAC GUID**: Select a profile	Click **Feature Configuration**.
3. ☐	**PMAC GUID**: Configure optional features	If NetBackup is to be used, enable the NetBackup feature; otherwise, use the selected features as is. This image is for reference only. The **Enabled** checkbox selects the desired features. The **Role** field provides a list of known network roles the feature may be associated with. The **Description** may be edited if desired. If the feature should be applied to a new network role (e.g., NetBackup), click **Add Role**. Enter the name of the new role and click **Add**. ***Note***: Role names are not significant, they are only used to associate features with networks. The new role name displays in the **Role** list for features. When done, click **Apply**. This foreground task takes a few moments, and then refreshes the view with an Info or Error notice to verify the action. To discard changes, navigate away from the view.

Step #	Procedure	Description
4. ☐	**PMAC GUI**: Reconfigure PMAC networks	***Note***: The network reconfiguration enters a tracked state. After you click Reconfigure, click **Cancel** to abort. 1. Click **Network Configuration** and follow the wizard through the configuration task. 2. Click **Reconfigure** to display the network view. The default management and control networks should be configured correctly. Networks may be added, deleted, or modified from this view. They are defined with IPv4 dotted-quad address and netmasks, or with IPv6 colon hex address and a prefix. When complete, click **Next**. 3. Click **Network Roles** to change the role of a network. Network associations can be added (for example, NetBackup) or deleted. You cannot add a new role since roles are driven from features. When complete, click **Next**. 4. Click **Network Interfaces** to add or delete interfaces, and change the IP address within the defined network space. If you add a network (for example, NetBackup), the Add Interface view displays when you click **Add**. This view provides an editable list of known interfaces. You may add a new device here if necessary. The Address must be an IPv4 or IPv6 host address in the network. When complete, click **Next**. 5. Click **Routes** to add or delete route destinations. The initial PMAC deployment does not define routes. Most likely, you want to add a default route — the route already exists, but this action defines it to PMAC so it may be displayed by PMAC. Click **Add**. The Add Route view provides an editable list of known devices. Select the egress device for the route. Enter an IPv4 dotted-quad address and netmask or an IPv6 colon hex address and prefix for the route destination and next-hop gateway. Click **Add Route**. When complete, click **Next**. 6. Click **DHCP Ranges** to define DHCP pools used by servers that PMAC manages. Click **Add**. Enter the starting and ending IPv4 address for the range on the network used to control servers (by default, the control network). Click **Add DHCP Range**. Only one range per network may be defined. When all pools are defined, click **Next**. 7. Click **Configuration Summary** for a view of your reconfigured PMAC. Click **Finish** to open the background task that reconfigures the PMAC application. A Task and Info or Error notice displays to verify your action. 8. Verify your reconfiguration task completes. Navigate to **Task Monitoring**. As the network is reconfigured, you will have a brief network interruption. From the Background Task Monitoring view, verify the **Reconfigure PMAC** task succeeds.
5. ☐	**PMAC GUI**: Set site settings	Navigate to **Administration > GUI Site Settings**. Set the **Site Name** to a descriptive name, set the **Welcome Message** to display when logging in.

Step #	Procedure	Description

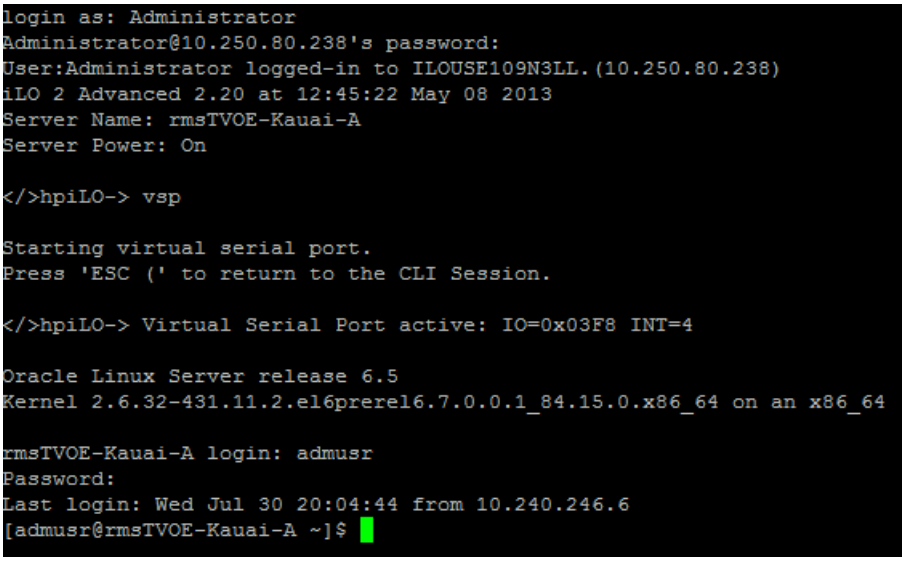
6. ☐	**PMAC**: Application backup	`$ sudo /usr/TKLC/smac/bin/pmacadm backup`
		`PMAC backup has been successfully initiated as task ID 7`
		Note: The backup runs as a background task. To check the status of the background task use the PMAC GUI Task Monitor screen, or issue the command `$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`. The result should eventually be **PMAC Backup successful** and the background task should indicate **COMPLETE**.
		Note: The **pmacadm backup** command uses a naming convention that includes a date/time stamp in the filename (for example, backupPmac_20111025_100251.pef). In the example provided, the backup filename indicates it was created on 10/25/2011 at 10:02:51 am server time.

7. ☐	**PMAC**: Verify backup was successful	***Note***: If the background task shows the backup failed, then the backup did not complete successfully. STOP and contact My Oracle Support (MOS).
		The output of pmaccli getBgTasks should look similar to the example below:
		`$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`
		`2: Backup PMAC COMPLETE - PMAC Backup successful`
		`Step 2: of 2 Started: 2012-07-05 16:53:10 running: 4 sinceUpdate: 2 taskRecordNum:`
		`2 Server Identity:`
		`Physical Blade Location:`
		`Blade Enclosure:`
		`Blade Enclosure Bay:`
		`Guest VM Location:`
		`Host IP:`
		`Guest Name:`
		`TPD IP:`
		`Rack Mount Server:`
		`IP:`
		`Name:`
		`::`

8. ☐	**PMAC**: Save the backup	The PMAC backup must be moved to a remote server. Transfer (sftp, scp, rsync, or preferred utility), the PMAC backup to an appropriate remote server. The PMAC backup files are saved in the following directory: **/var/TKLC/smac/backup**.

4.4.2 Install and Configure NetBackup Client on PMAC

Procedure 10. Install and Configure PMAC NetBackup Client

Step #	Procedure	Description
This procedure installs and configures the NetBackup client software on a PMAC application. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**PMAC GUI**	Verify the PMAC application guest has been configured with NetBackup virtual disk by executing Procedure 49.
2. ☐	**TVOE Management Server iLO**: Login with PMAC admusr credentials	1. Log into the management server iLO on the remote console using application provided passwords via Appendix C. 2. Log into the iLO in Internet Explorer using password provided by application: `http://<management_server_iLO_IP>` 3. Click the Remote Console tab and open the Integrate Remote Console on the server.  4. Click **Yes** if the security alert displays.

Step #	Procedure	Description

3. ☐	**TVO Management Server**: Login	Log into PMAC with **admusr** credentials.
		Note: On a TVOE host, if you open the virsh console, for example, `$ sudo /usr/bin/virsh console X` or from the virsh utility `virsh # console X` command and you get garbage characters or the output is not correct, then there is likely a stuck **virsh console** command already being run on the TVOE host. Exit out of the virsh console, run `ps -ef |grep virsh`, and then kill the existing process "`kill -9 <PID>`. Then execute the `virsh console X` command. Your console session should now run as expected.
		Login using virsh and wait until you see the login prompt. If a login prompt does not display after the guest is finished booting, press **ENTER** to make one display:
		`$ sudo /usr/bin/virsh`
		`virsh # list`
		`Id Name State`
		`----------`
		`4 pmacU17-1 running`
		`virsh # console pmacU17-1`
		`[Output Removed]`
		`####################`
		`1371236760: Upstart Job readahead-collector: stopping`
		`1371236767: Upstart Job readahead-collector: stopped`
		`####################`
		`CentOS release 6.4 (Final)`
		`Kernel 2.6.32-358.6.1.el6prerel6.5.0_82.16.0.x86_64 on an x86_64`
		`pmacU17-1 login:`

Step #	Procedure	Description

4. ☐	**PMAC**: Install NetBackup client	Perform Appendix J.1.
		The following data is required to perform Procedure 45.
		• NetBackup support:
		  • PMAC 6.5.0 supports NetBackup client software versions 7.6 and 7.7.
		• The PMAC is a 64 bit application; the appropriate NetBackup client software versions are 7.6 and 7.7.
		• The PMAC application NetBackup user is "NetBackup". See appropriate documentation for the password.
		• The paths to the PMAC application software NetBackup notify scripts are:
		  • /usr/TKLC/smac/sbin/bpstart_notify
		  • /usr/TKLC/smac/sbin/bpend_notify
		• For the PMAC application the following is the NetBackup server policy files list:
		  • /var/TKLC/smac/image/repository/*.iso
		  • /var/TKLC/smac/backup/backupPmac*.pef
		After executing the Appendix J.1, the NetBackup installation and configuration on the PMAC application server is complete.
		Note: At the NetBackup server, the NetBackup policy (ies) can now be created to perform the NetBackup backups of the PMAC application.

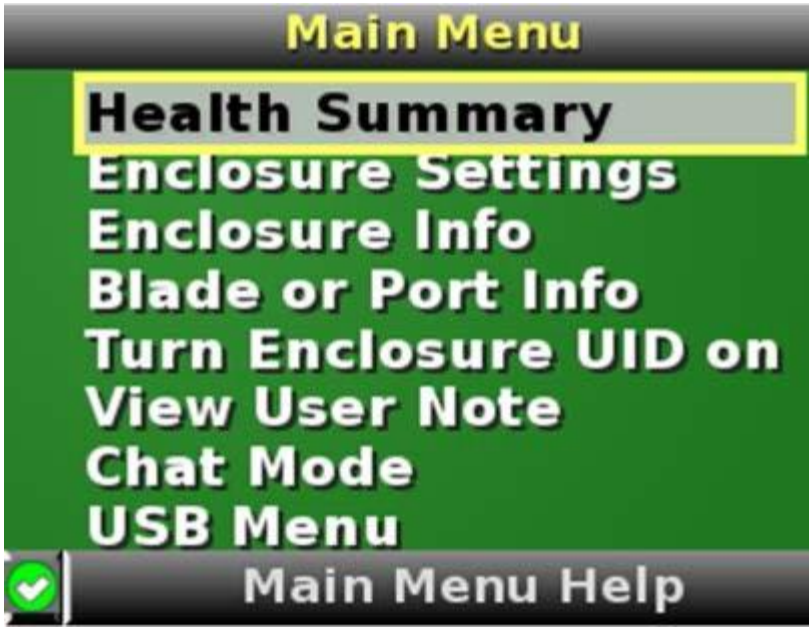
4.5 HP C-7000 Enclosure Configuration

This section applies if the installation includes one or more HP C-7000 Enclosures. It uses the HP Onboard Administrator user interfaces (insight display, and OA GUI) to configure the enclosure settings. This procedure determines the health and status of the DSR network and servers.

4.5.1 Configure Initial OA IP

Provision the enclosure with two onboard administrators. Executed this procedure only for OA Bay 1, regardless of the number of OAs installed in the enclosures.

Procedure 11. Configure Initial OA IP

Step #	Procedure
This procedure sets the initial IP address for the onboard administrator in location OA Bay 1 (left as viewed from rear) and Bay 2 using the front panel display. ***Note***: The enclosure should be provisioned with two Onboard Administrators. This procedure needs to be executed only for OA Bay 1, regardless of the number of OAs installed in the enclosure. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Configure OA Bay 1 address using the insight display on the front side of the enclosure. 
2. ☐	Navigate to **Enclosure Settings**.

<table>
<tr><th>Step #</th><th colspan="2">Procedure</th></tr>
<tr><td>3.
</td><td colspan="2">Navigate to the OA1 IP menu settings and press OK.

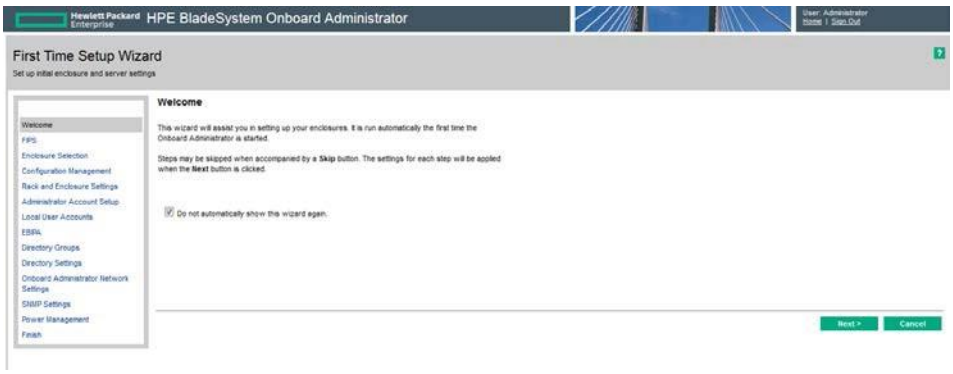
Note: The OA1 IP and OA2 IP menu settings in this procedure may indicate OA1 IPv4 or OA1 IPv6. In either case, select this menu setting to set the OA IP address.</td></tr>
<tr><td>4.
</td><td>If setting the IPv4 address:
1. Navigate to the OA1 IPv4 and press OK.
2. On the OA1 Network Mode screen, select static and press OK.
3. Select Accept and press OK.
4. On the Change:OA1 IP address screen, fill in data below and press OK.
• IP
• MASK
• gateway
5. Select Accept and press OK.
6. Navigate to OA2 IP menu setting on the Insight display and repeat the above steps to assign the IP parameters of OA2.</td><td>If setting the IPv6 address:
1. Navigate to the OA1 IPv6 and press OK.
2. On the Change: OA1 IPv6 Status menu, select Enabled and press OK.
3. Select Accept and press OK.
4. On the Change:OA1 IPv6 Settings screen, fill in appropriate data below and press OK.
5. Set the Static IPv6 address to the globally scoped address and prefix and press OK.
6. Leave the DHCPv6 option as Disabled.
7. Leave the SLAAC option as Disabled.
8. If a static Gateway address needs to be configured, navigate to Static Gateway and press OK.
a. Select the Static Gateway IPv6 Address and press OK.
b. Select Set and press OK.
9. Navigate to OA2 IP menu setting on the Insight display and repeat the above steps to assign the IP parameters of OA2.
10. Select Accept All and press OK.</td></tr>
</table>

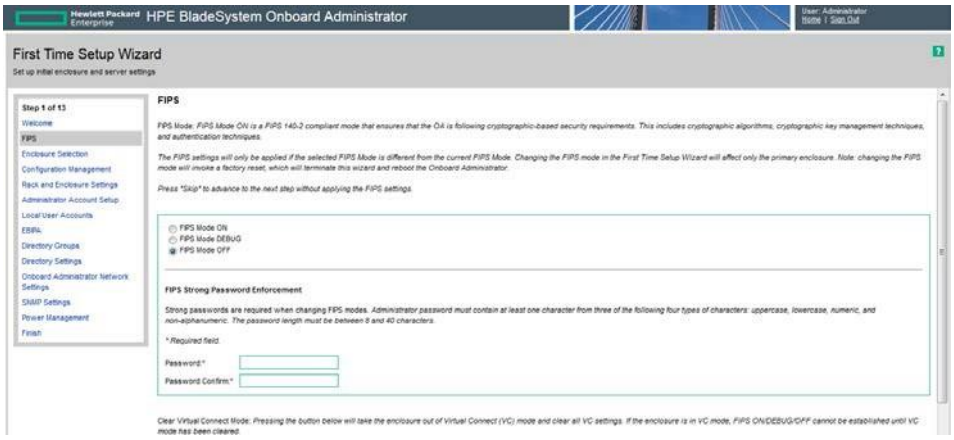
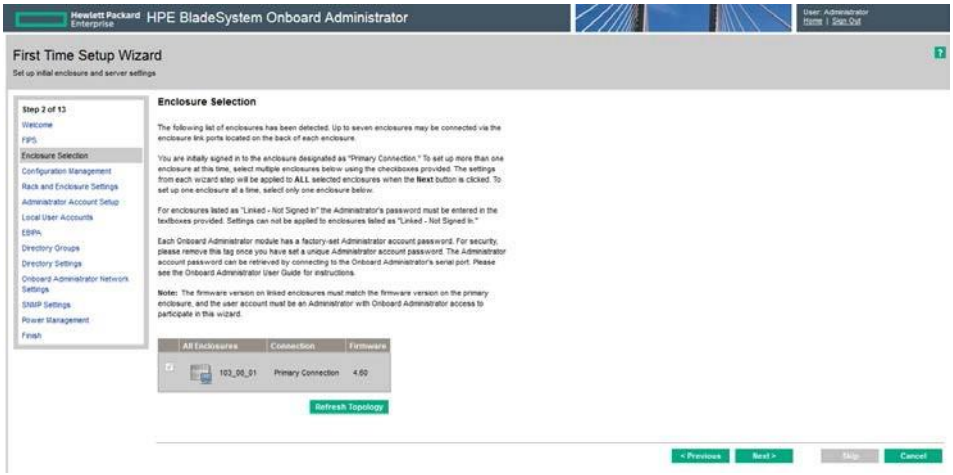
4.5.2 Configure Initial OA Settings Using the Configuration Wizard

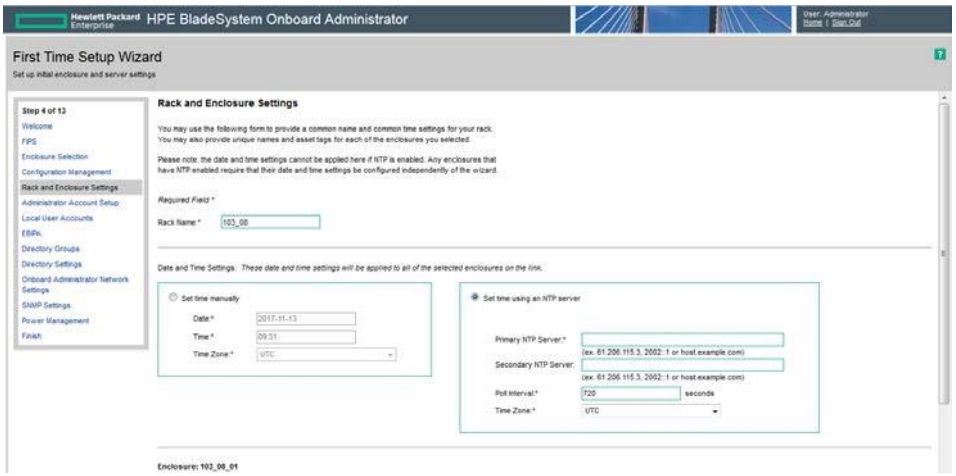
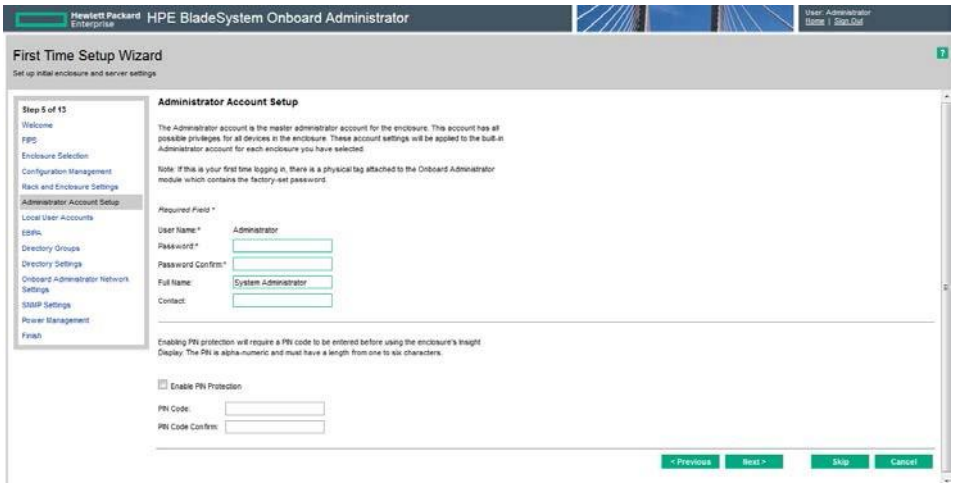
This procedure is for initial configuration only and should be executed when the onboard administrator in OA Bay 1 (left as viewed from rear) is installed and active. Follow Appendix I to learn how to replace one of the onboard administrators correctly.

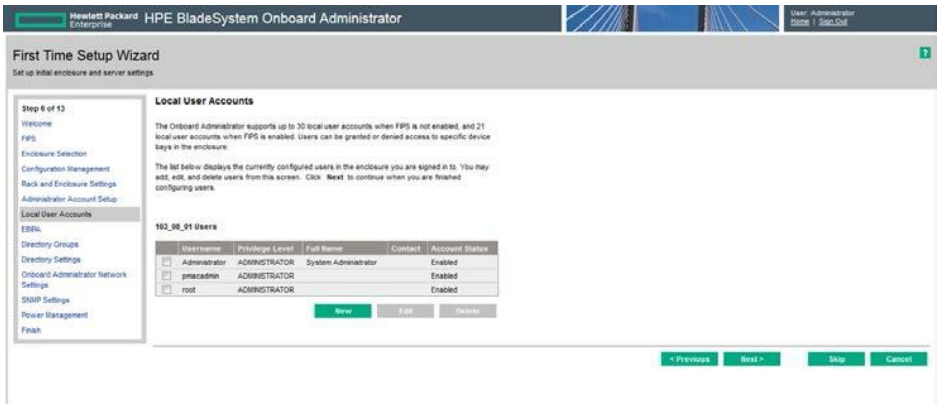
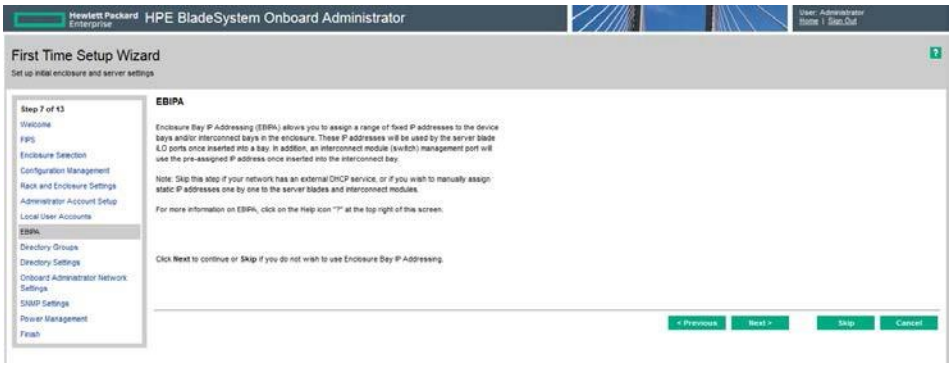
Provision the enclosure with two onboard administrators. The OA in Bay 2 automatically acquires its configuration from the OA in Bay 1 after the configuration is complete.

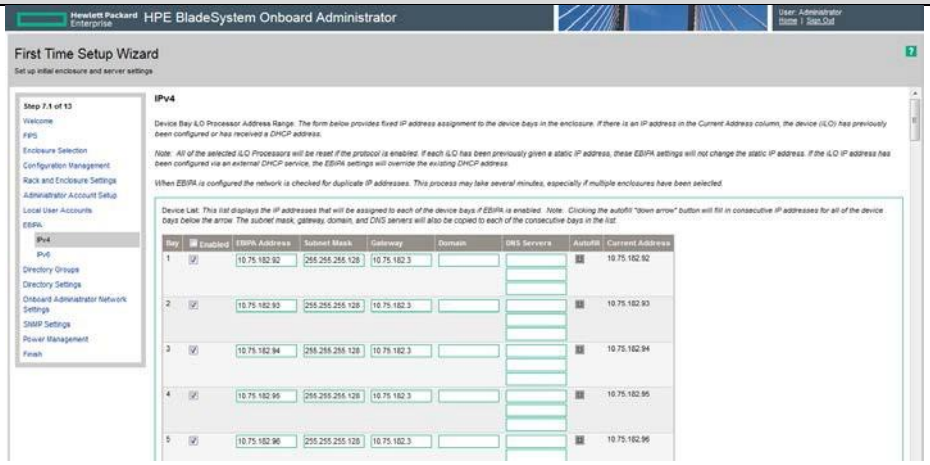
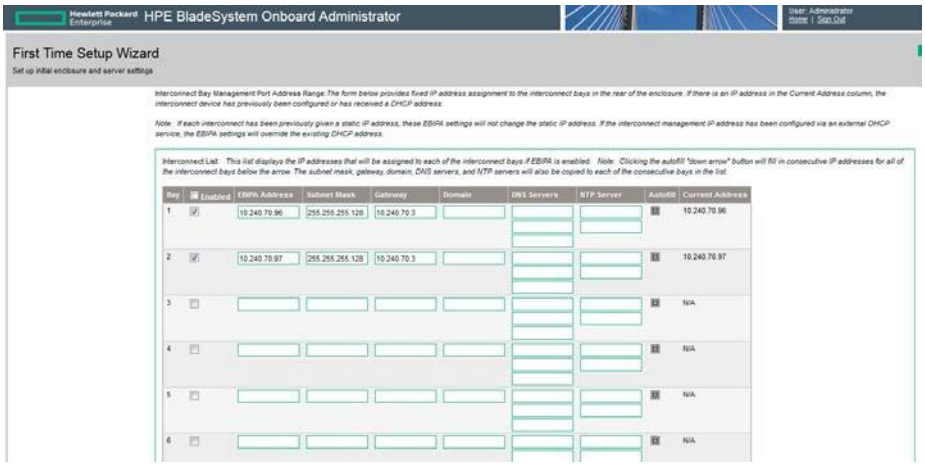
Procedure 11. Configure Initial OA Settings Using the Configuration Wizard

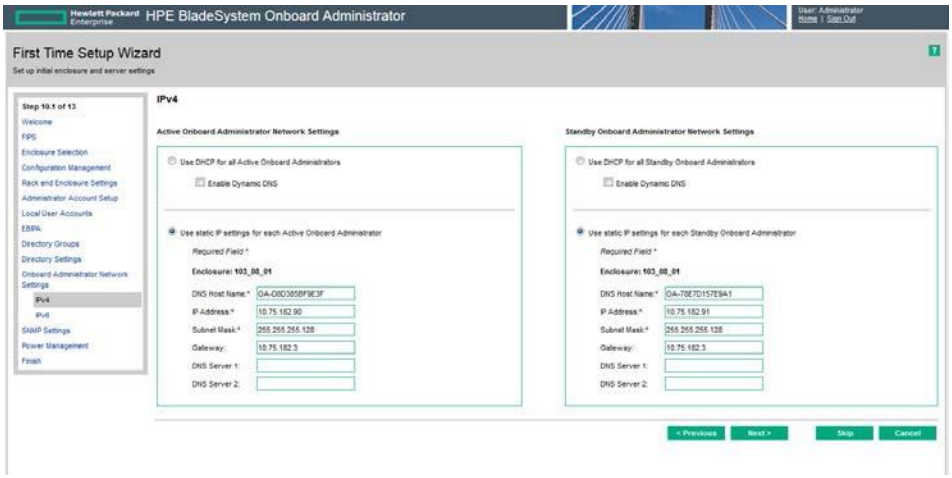
Step #	Procedure	Description
This procedure configures the initial OA settings using a configuration wizard. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**OA GUI**: Login	Open you web browser and navigate to the OA Bay 1 IP address assigned in Procedure 11. `http://<OA_IP>` Login as an administrative user. The original password is on a paper card attached to each OA.
2. ☐	**OA GUI**: Run First Time Setup wizard	If needed, navigate to Wizards > First Time Setup. 

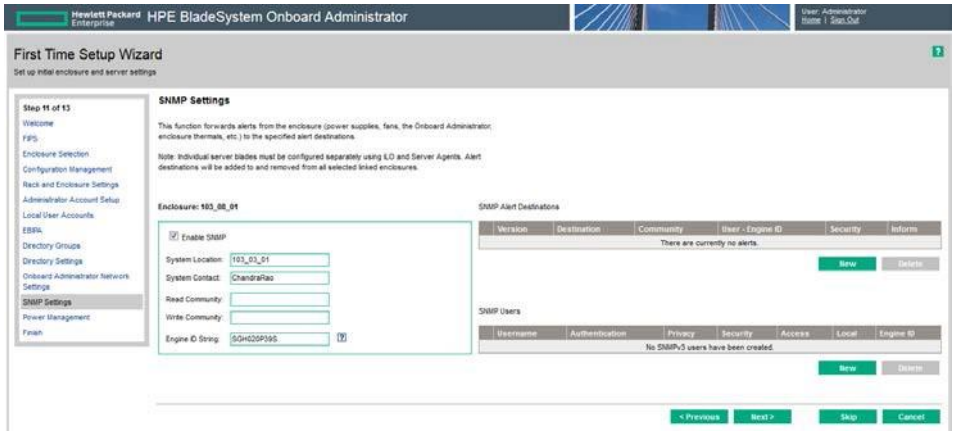
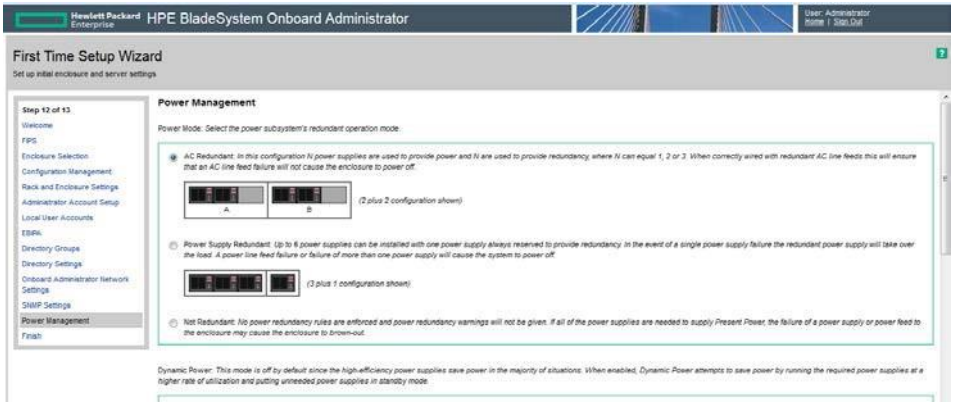
Step #	Procedure	Description
3.	**OA GUI**: FIPS	Click **Next**. FIPS mode is not currently supported. 
4.	**OA GUI**: Enclosure Selection	Click **Next** to select an enclosure. 
5.	**OA GUI**: Configuration Management	Click **Next**. Skip configuration management.

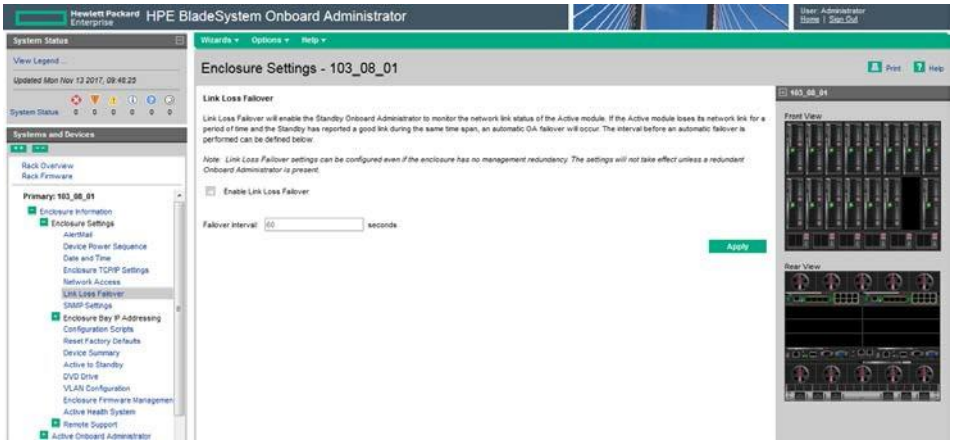
Step #	Procedure	Description
6. ☐	**OA GUI**: Rack and Enclosure Settings	Click **Next** to configure the Rack and Enclosure.  Type the **Rack Name** in format xxx_xx. Type the **Enclosure name** in format <rack name>_<position> Example: Rack Name: 500_03 Enclosure Name: 500_03_03 ***Note***: Enclosure positions are numbered from 1 at the bottom of the rack to 4 at the top. Check **Set time using an NTP server** option and type the **Primary NTP Server** (recommended to be set to the <customer_supplied_ntp_server_address>). Set **Poll interval** to **720**. Set **Time Zone** to **UTC** if the customer does not have any specific requirements.
7. ☐	**OA GUI**: Administrator Account Setup	Click **Next** to change the administrator password. 

Step #	Procedure	Description
8. ☐	**OA GUI**: Local User Accounts	Click **Next** to create pmacadmin and admusr user.  On the Local User Accounts screen, click **New** to add **pmacadmin** user. From the User Settings screen, type the **User Name** and **Password**. Set the **Privilege Level** to **Administrator**. Refer to the application documentation for the password. Verify all of the blades have been checked before proceeding to mark the checkbox for **Onboard Administrator Bays** under the **User Permissions** section. Click **Add User**. In the same way, create the **admusr** user.
9. ☐	**OA GUI**: Enclosure Bay IP Addressing (EBIPA)	Click **Next** to set up the EBIPA addresses.  ***Note***: Setting up the EBIPA is required. 1. Select the First Time Setup Wizard **EBIPA: IPv4** or **EBIPA: IPv6** and enter the appropriate data.

Step #	Procedure	Description
		 2. Go to the Device List section of the EBIPA Settings Screen (at the top) and type the iLO IP, Subnet Mask, and Gateway fields for Device Bays 1-16. Do not fill in the iLO IP, subnet Mask, or Gateway fields for Device Bays 1A-16A and 1B-16B. ***Note***: Bays 1A-16A and 1B-16B are used for double-density blades (i.e., BL2x220c), which are not supported in this release. 3. Mark the **Enabled** checkbox for each Device Bay 1 through 16 that is in use. ***Note***: Any unused slots should have an IP address assigned, but should be disabled. ***Note***: Do not use autofill since this fills the entries for the Device Bays 1A through 16B. 4. Scroll down to the Interconnect List (below Device Bay 16B) and type the EBIPA Address, Subnet Mask, and Gateway fields for Interconnect Bay in use. 5. Mark the **Enabled** checkbox for each Interconnect Bay in use.  Click **Next** to apply the settings. The system may restart devices such as interconnect devices or iLOs to apply new addresses. Ager finishing, check the IP addresses to ensure the settings were successful.

Step #	Procedure	Description
10.	**OA GUI**: Directory Groups and Settings	Click **Next** to skip Directory Groups and Directory Settings.
11.	**OA GUI**: Onboard Administrator Network Settings	Click **Next** to assign or modify the IP address and other network settings for the onboard administrator.  The Active Administrator Network Settings pertain to the active OA (OA Bay 1 location during initial configuration). If the second Onboard Administrator is present, the Standby Onboard Administrator Network Settings are displayed as well. Select **Use static IP settings for each Standby Onboard Administrator**. Type the IP Address, Subnet Mask, and Gateway for the Standard OA. Click **Next**. ***Note***: If you change the IP address of the active OA, you are disconnected. Then, you must close your browser and sign in again using the new IP address.

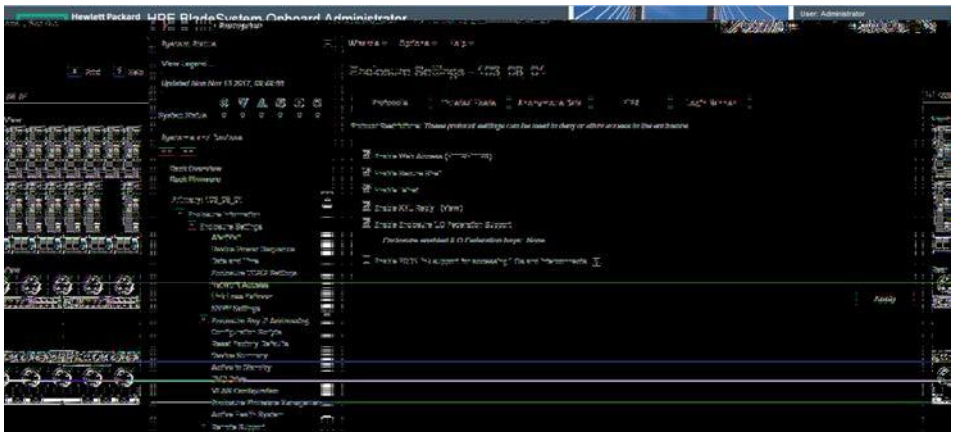
Step #	Procedure	Description
12. ☐	**OA GUI**: SNMP Settings	By default, the **Enable SNMP** checkbox should be checked. If you do not want to have SNMP enabled, see Appendix K.  Type the **System Location** that is equal to the **Enclosure Name** you used in step 6. Do not set **Read Community** and **Write Community**. ***Note***: This step does not set an SNMPP Trap Destination. To set an SNMP Trap Destination, see Procedure 15.
13. ☐	**OA GUI**: Power Management	Click **Next** to configure power supply redundancy. The first available setting on the Power Management screen is either **AC Redundant** or **Redundant**, depending on whether the Enclosure is powered by AC or DC. In either case, select the **Power Supply Redundant** option. AC/DC-Powered Enclosures:  For all other settings on the Power Management screen, leave the default settings unchanged.
14. ☐	**OA GUI**: Finish First Time Setup Wizard	Click **Next** and **Finish**.

Step #	Procedure	Description
15. ☐	**OA GUI**: Set Link Loss Failover	Navigate to **Enclosure Information > Enclosure Settings > Link Loss Failover**.  Mark the **Enable Link Loss Failover** checkbox and specify the **Failover Interval** as **180** seconds. Click **Apply**.

4.5.3 Configure OA Security

Procedure 10. Configure OA Security

Steps #	Procedure	Description
This procedure disables telnet access to OA. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Active OA GUI**: Login	Navigate to the IP address of the active OA using Appendix I Determine which Onboard Administrator is Active. Login as an administrative user.

Steps #	Procedure	Description
2. ☐	**OA GUI**: Disable telnet	Navigate to **Enclosure Information > Enclosure Settings > Network Access**. Unmark the **Enable Telnet** checkbox. 
3. ☐	**OA GUI**: Apply changes	Click **Apply**.

4.5.4 Upgrade or Downgrade OA Firmware

Software Centric Customers: If Oracle Consulting Services or any other Oracle Partner is providing services to a customer that includes installation and/or upgrade then, as long as the terms of the scope of those services include that Oracle Consulting Services is employed as an agent of the customer (including update of Firmware on customer provided services), then Oracle consulting services can install FW they obtain from the customer who is licensed for support from HP.

Provision the enclosure with two onboard administrators. This procedure installs the same firmware version on both onboard administrators.

Use this procedure to upgrade or downgrade firmware or to ensure both OAs have the same firmware version. When the firmware update is initiated, the standby OA is automatically updated first.

Procedure 11. Upgrade or Downgrade OA Firmware

Step #	Procedure	Description
This procedure updates the firmware on the OAs. ***Needed Material***: • HP MISC firmware ISO image • Release Notes from HP Solutions Firmware Upgrade Pack, version 2.x.x [2] Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Add firmware	Execute section 4.9.2 Add ISO Images to the PMAC Image Repository to add the HP Miscellaneous firmware ISO image

Step #	Procedure	Description
2. ☐	**OA GUI**: Login	Navigate to the IP address of the active OA using Appendix I. Login as an administrative user.
3. ☐	**OA GUI**: Check OA firmware versions	Navigate to **Enclosure Information > Active Onboard Administrator > Firmware Update**. Examine the firmware version shown in the Firmware Information table. Verify the version meets the minimum requirement specified by the Release Notes of the HP Solutions Firmware Upgrade Pack, version 2.x.x [2] and that the firmware versions match for both OAs. If the versions match, then the firmware does not need to be changed. Skip the rest of this procedure.
4. ☐	Save all OA configuration	If one of the two OAs has a later version of firmware than the version provided by the HP Solutions Firmware Upgrade Pack, version 2.x.x [2], this procedure downgrades it to that version. A firmware downgrade can result in the loss of OA configuration. Before proceeding, ensure you have a record of the initial OA configuration necessary to execute the following OA configuration procedures, as required by the customer and application. 1. Configure Initial OA IP 2. Configure Initial OA Settings Using the Configuration Wizard 3. Configure OA Security 4. Store Configuration on Management Server

5. ☐	**OA GUI**: Initiate OA firmware upgrade	Firmware obtained from a Software Centric Customer is located at:
		`https://<PMAC_Management_Network_IP>/TPD/<OA_firmware_version>`
		If the firmware needs to be upgraded, click **Firmware Update** in the left navigation area.
		Enter the appropriate URL in the bottom text box labeled “Image URL”. The syntax is:
		`https://<PMAC_Management_Network_IP>/TPD/<HPFW_mount_point>/files/<OA_firmware_version>.bin`
		For example:
		`https://10.240.4.198/TPD/HPFW--872-2488-XXX--HPFW/files/hpoa300.bin`
		Check the Force Downgrade box if present.
		Click **Apply**.
		If a confirmation dialog is displayed, click **OK**.
		Note: The upgrade may take up to 25 minutes.

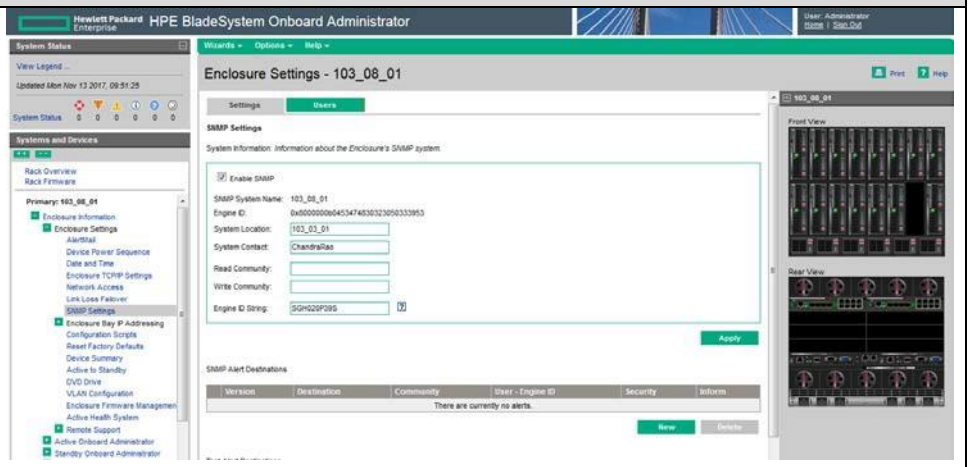
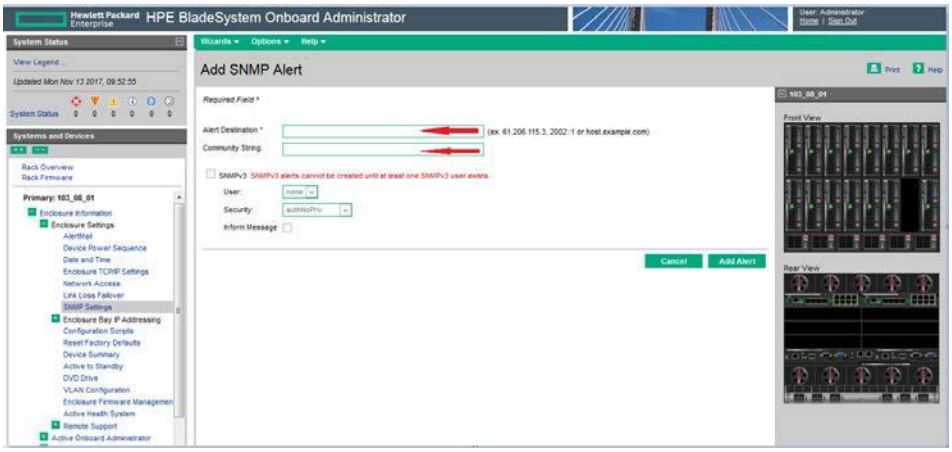
Step #	Procedure	escription
6. ☐	**OA GUI**: Reload the HP OA application	The upgrade is complete when the following displays: It is recommended that you clear your browser's cache before continuing to use this application. If the bowser's cache is not cleared after a firmware update, the application my not function properly. Click here to reload the application. Clear you browser's cache and click to reload the application. The login page displays momentarily
7. ☐	**OA GUI**: Verify the firmware upgrade	Log into the OA again. It may take few minutes before the OA is fully functional and accepts the credentials. Navigate to **Enclosure Information > Active Onboard Administrator > Firmware Update**. Examine the firmware version shown in the Firmware Information table and verify the firmware version information is correct.
8. ☐	**OA GUI**: Check/Re-establish OA configuration	Ensure all OA configuration established by the following procedures is still intact after the firmware update. Re-establish any settings by performing the procedure(s). 1. Configure Initial OA IP 2. Configure Initial OA Settings Using the Configuration Wizard 3. Configure OA Security 4. Store Configuration on Management Server

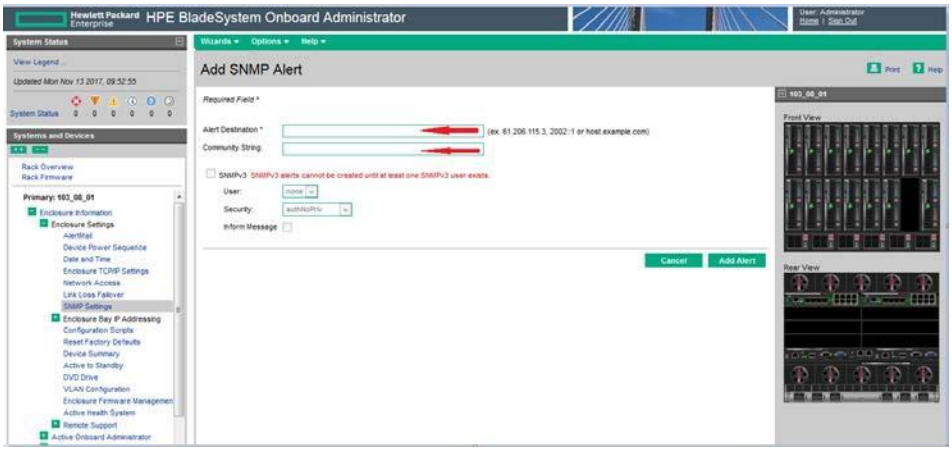
4.5.5 Add SNMP Trap Destination on OA

An SNMP trap destination must be added and configured using the Onboard Administrator (OA), or the SNMP must be disabled. One of these actions must be completed as described in this procedure.

Procedure 10. Add/Disable SNMP Trap Destination on OA

Step #	Procedure	Description
This procedure adds an SNMP destination on OA. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Active OA GUI**: Login	1. To add an SNMP trap destination, navigate to the IP address of the active OA. Use Appendix I to determine the active OA. 2. Login as an administrative user.
2. ☐	**Active OA GUI**: Enter system information	1. Navigate to **Enclosure Information > Enclosure Settings > SNMP Settings**.

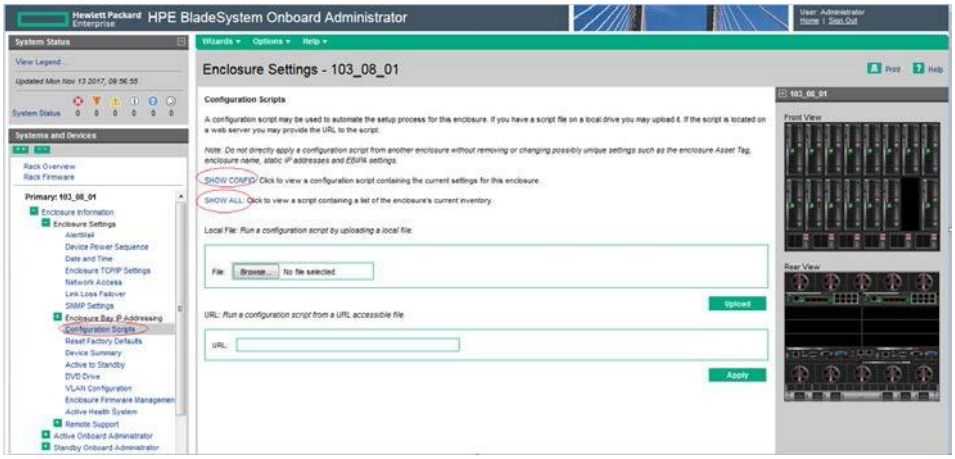
Step #	Procedure	Description
		 2. Enable SNMP and populate **System Information**. If SNMP is not already enabled, mark the **Enable SNMP** checkbox. Enter the **Enclosure Name** (shown in the title bar) or your preferred name into the **System Location** box.  Do not set **Read Community** and **Write Community**. 3. Click **Apply** to save the system information.

Step #	Procedure	Description
3. ☐	**Active OA GUI**: Add SNMP Alert Destinations	1. Click **New**. 2. Type the destination information into the **Alert Destination** box (for example, 61.206.115.3, 2002::1 or host.example.com). 3. Type the community string into the **Community String** box. 4. Click **Add Alert** to add the destination to the system. 
4. ☐	**Active OA GUI**: Login	1. To disable SNMP, log into the active OA. 2. Navigate to Enclosure Information > Enclosure Settings > SNMP Settings. 3. Unmark the **Enable SNMP** checkbox. 4. Click **Apply** to save the system information.

4.5.6 Store Configuration on Management Server

Procedure 10. Store OA Configuration on Management Server

Step #	Procedure	Description
This procedure backs up OA settings on the management server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**OA GUI**: Login	1. Navigate to the IP address of the active OA. Use Appendix I to determine the active OA. 2. Login as root.

Step #	Procedure	Description
2. ☐	**OA GUI**: Store configuration file	1. Navigate to Enclosure Information > Enclosure Settings > Configuration scripts. 2. Open the first configuration file (current settings for enclosure) and store it on a local disk.  3. Click **Show Config**. 4. Copy all text on the page and save it in a text file. Or, select **File > Save As** select a file name and path, and select **Text file** for the type. <enclosure_ID>_<timetag>.conf

3. ☐	**PMAC**: Back up the configuration file	Do the following to back up the file on the PMAC:
		1. Under **/usr/TKLC/smac/etc** directory you can create your own subdirectory structure. Log into the management server as **admusr** using ssh and create the target directory:
		`$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/OA_backups/OABackup`
		2. Change the directory permissions:
		`$ sudo /bin/chmod go+x /usr/TKLC/smac/etc/OA_backups/OABackup`
		3. Copy the configuration file to the created directory.
		For UNIX users:
		`# scp ./<cabinet_enclosure_backup file>.conf \admusr@<pmac_management_network_ip>:/home/admusr`
		Windows users, refer to Appendix E to copy the file to the management server.
		4. On the PMAC, move the configuration file to the OA Backup folder that you created under **/usr/TKLC/smac/etc**.
		`$ sudo /bin/mv /home/admusr/<cabinet_enclosure_backup file>.conf /usr/TKLC/smac/etc/OA_backups/OABackup`

Step #	Procedure	Description

4. ☐	**PMAC**: Back up PMAC application to capture the OA backup	`$ sudo /usr/TKLC/smac/bin/pmacadm backup`
		`PMAC backup has been successfully initiated as task ID 7`
		Note: The backup runs as a background task. To check the status of the background task use the PMAC GUI Task Monitor screen, or issue the command `$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`. The result should eventually be **PMAC Backup successful** and the background task should indicate **COMPLETE**.
		Note: The **pmacadm backup** command uses a naming convention that includes a date/time stamp in the filename (for example, backupPmac_20111025_100251.pef). In the example provided, the backup filename indicates it was created on 10/25/2011 at 10:02:51 am server time.

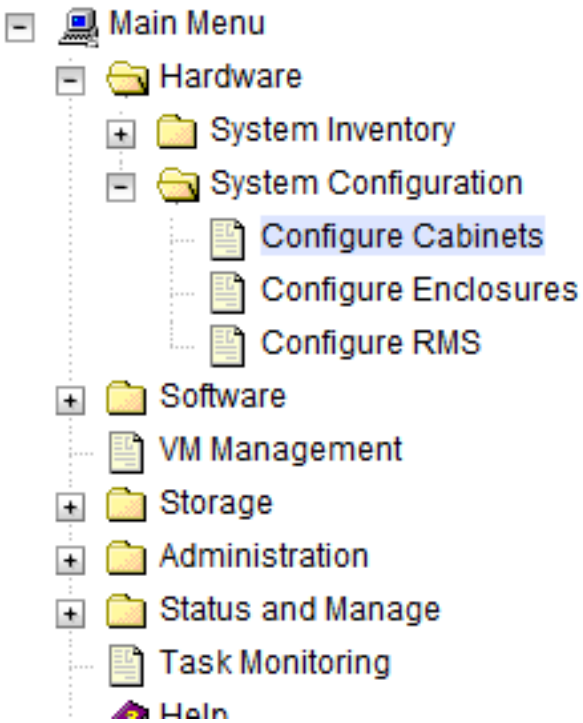
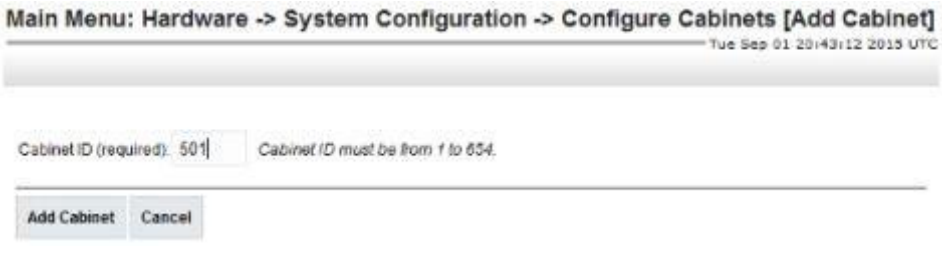
5. ☐	**PMAC**: Verify backup	***Note***: If the background task shows the backup failed, then the backup did not complete successfully. STOP and contact My Oracle Support (MOS).
		The output of pmaccli getBgTasks should look similar to the example below:
		`$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`
		`2: Backup PMAC COMPLETE - PMAC Backup successful`
		`Step 2: of 2 Started: 2012-07-05 16:53:10 running: 4`
		`sinceUpdate: 2 taskRecordNum:`
		`2 Server Identity:`
		`Physical Blade Location:`
		`Blade Enclosure:`
		`Blade Enclosure Bay:`
		`Guest VM Location:`
		`Host IP:`
		`Guest Name:`
		`TPD IP:`
		`Rack Mount Server:`
		`IP:`
		`Name:`
		::

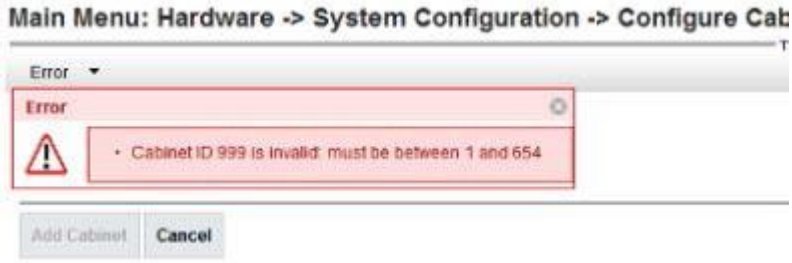
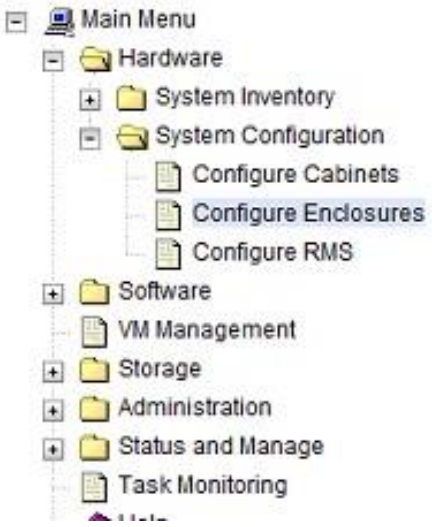
6. ☐	**PMAC**: Save the backup	The PMAC backup must be moved to a remote server. Transfer (sftp, scp, rsync, or preferred utility), the PMAC backup to an appropriate remote server. The PMAC backup files are saved in the following directory: **/var/TKLC/smac/backup**.
7. ☐	**OA GUI**: Logout	Logout from the OA by clicking **Sign Out** at the top right corner.

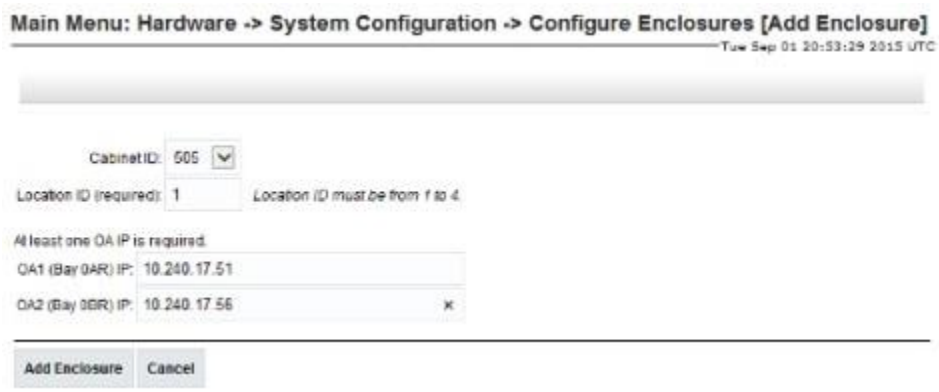
4.6 Enclosure and Blades Setup

Procedure 11. Add Cabinet and Enclosure to the PMAC System Inventory

Step #	Procedure	Description
This procedure adds a cabinet and an enclosure to the PMAC system inventory. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as pmacadmin user.

Step #	Procedure	Description
2. ☐	**PMAC GUI**: Navigate to Configure cabinets	Navigate to **Hardware > System Configuration > Configure Cabinets**. 
3. ☐	**PMAC GUI**: Add cabinet	Click **Add Cabinet**.
4. ☐	**PMAC GUI**: Enter cabinet ID	Type the **Cabinet ID** and click **Add Cabinet**. 

Step #	Procedure	Description
5. ☐	**PMAC GUI**: Check errors	If no errors are reported, the Info box states it is successful. Or an error message displays: 
6. ☐	**PMAC GUI**: Navigate to Configure Enclosures	Navigate to **Hardware > System Configuration > Configure Enclosures**. 

Step #	Procedure	Description
7. ☐	**PMAC GUI**: Add enclosure	Click **Add Enclosure**.
8. ☐	**PMAC GUI**: Provide enclosure details	Type the **Cabinet ID**, **Location**, and two **OA IP** addresses (the enclosure's active and standby OAs).  ***Note***: The Location ID uniquely identifies an enclosure within a cabinet. It can have a value of 1, 2, 3, or 4. The cabinet ID and location ID is combined to create a globally unique ID for the enclosure (for example, an enclosure in cabinet 502 at location 1 has an enclosure ID of 50201). Click **Add Enclosure**.

Step #	Procedure	Description
9. ☐	**PMAC GUI**: Monitor add enclosure	The Configure Enclosures screen displays again with a new background task entry in the Tasks table. Access this table by clicking **Tasks** on the toolbar under the Configure Enclosures heading. When the tasks completes and is successful, the text changes to green and its Progress column indicates 100%.

10. ☐	**PMAC**: Verify backup was successful	***Note***: If the background task shows the backup failed, then the backup did not complete successfully. STOP and contact My Oracle Support (MOS).
		The output of pmaccli getBgTasks should look similar to the example below:
		`$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`
		`2: Backup PMAC COMPLETE - PMAC Backup successful`
		`Step 2: of 2 Started: 2012-07-05 16:53:10 running: 4`
		`sinceUpdate: 2 taskRecordNum:`
		`2 Server Identity:`
		`Physical Blade Location:`
		`Blade Enclosure:`
		`Blade Enclosure Bay:`
		`Guest VM Location:`
		`Host IP:`
		`Guest Name:`
		`TPD IP:`
		`Rack Mount Server:`
		`IP:`
		`Name:`
		`::`

Step #	Procedure	Description
11. ☐	**PMAC**: Save the backup	The PMAC backup must be moved to a remote server. Transfer (sftp, scp, rsync, or preferred utility), the PMAC backup to an appropriate remote server. The PMAC backup files are saved in the following directory: **/var/TKLC/smac/backup**.

Procedure 18. Configure Blade Server iLO Password for Administrator Account

Step #	Procedure	Description
This procedure changes the blade server iLO password for Administrator account for blade server in an enclosure. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**PMAC GUI**: Login	Log into PMAC as **admusr** using ssh.

2. ☐	**PMAC GUI**: Create xml file	In the **/usr/TKLC/smac/html/public-configs** directory, create an xml file with information similar to the following example. Change the Administrator password field to a user-defined value.
		`<RIBCL VERSION="2.0">`
		`<LOGIN USER_LOGIN="admusr" PASSWORD="password">`
		`<USER_INFO MODE="write">`
		`<MOD_USER USER_LOGIN="Administrator">`
		`<PASSWORD value="<new Administrator password>"/>`
		`</MOD_USER>`
		`</USER_INFO>`
		`</LOGIN>`
		`</RIBCL>`
		Save this file as **change_ilo_admin_passwd.xml**.
		Change the permission of the file:
		`$ sudo chmod 644 change_ilo_admin_passwd.xml`

Step #	Procedure	Description

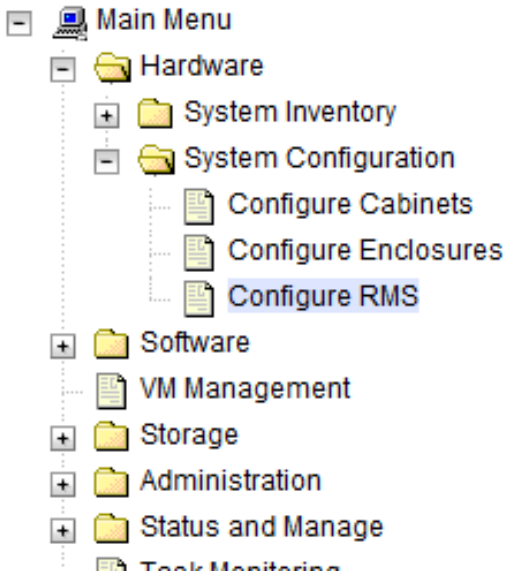
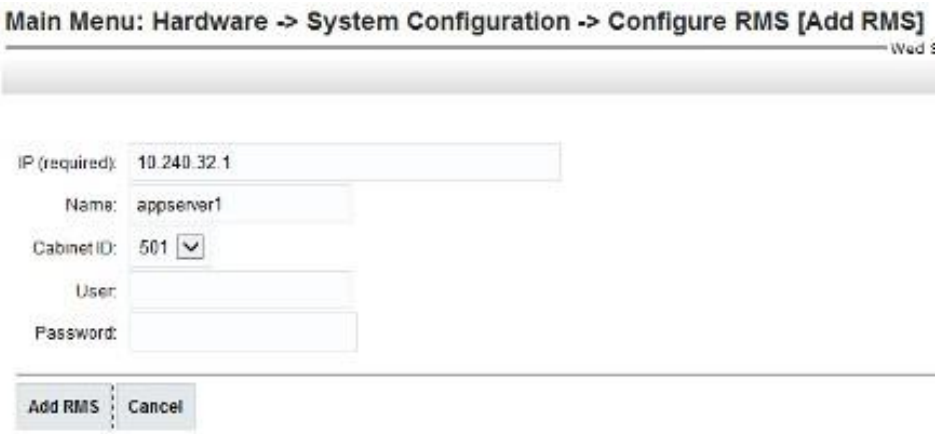
3. ☐	**OA Shell**: Login	Log into the active OA using ssh as root user.
		`login as: root`
		`----------`
		`WARNING: This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law.`
		`----------`
		`Firmware Version: 3.00`
		`Built: 03/19/2010 @ 14:13 OA`
		`Bay`
		`Number: 1 OA`
		`Role: Active`
		`admusr@10.240.17.51's password:`
		If the OA role is not active, log into the other OA of the enclosure system.

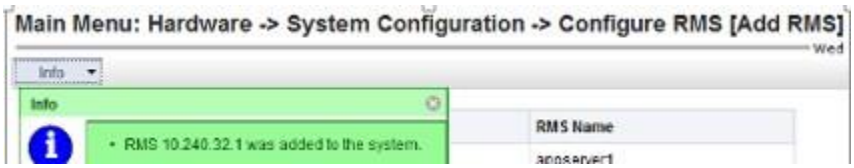
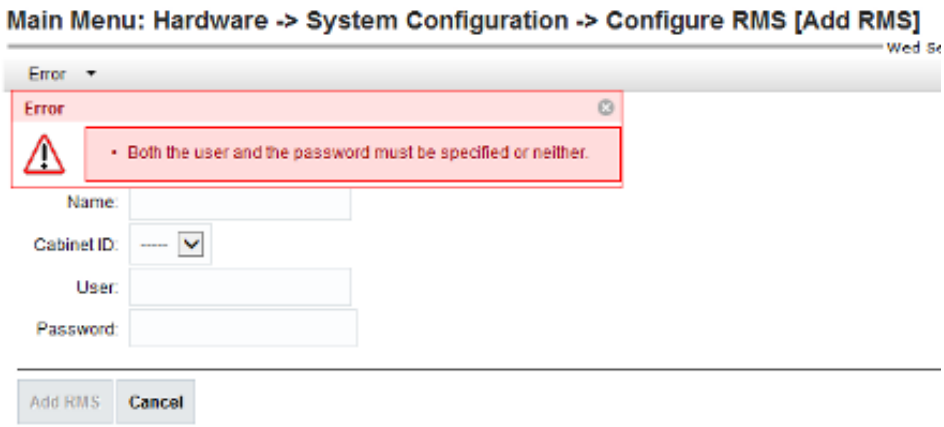
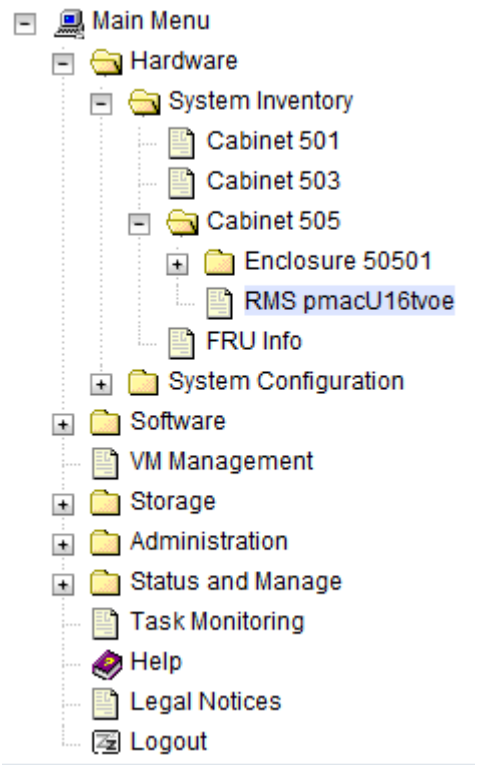
4. ☐	**OA Shell**: Run hponcfg command	`> hponcfg all https://<pmac_ip>/public-configs/change_ilo_admin_passwd.xml`
5. ☐	**OA Shell**: Check output	Observe the output for any error messages and refer to the *HP Integrated Lights-Out Management Processor Scripting and Command Line Resource Guide* for troubleshooting.
6. ☐	**OA Shell**: Logout	Logout from the OA.
7. ☐	**PMAC**: Remove temporary file	On the PMAC, remove the configuration file you created. This is done for security reasons so that no one can reuse the file: `$ sudo /bin/rm –rf /usr/TKLC/smac/html/public-configs/change_ilo_admin_passwd.xml`

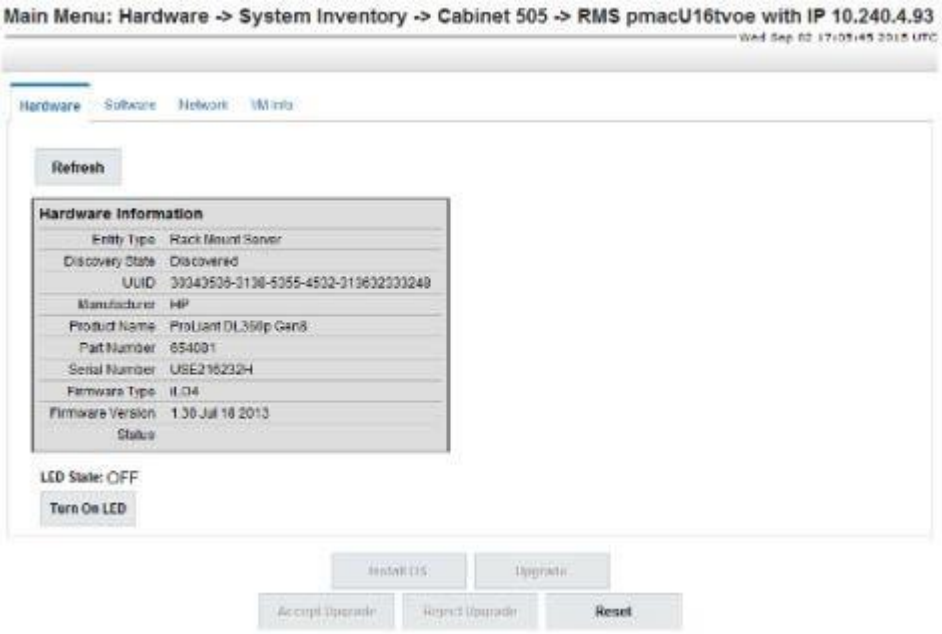
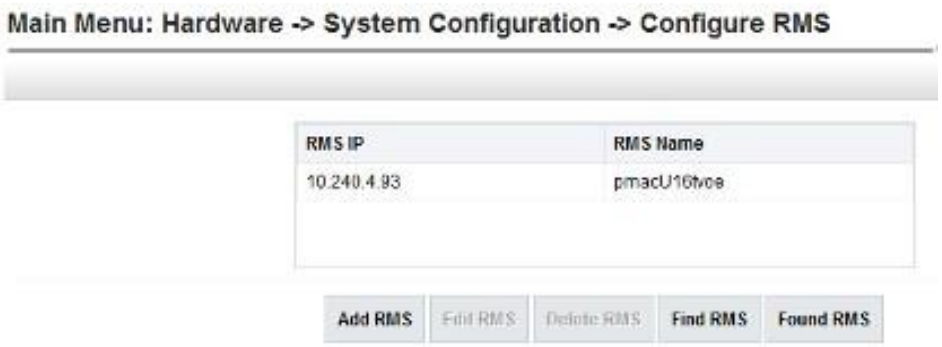
4.6.1 Add PMAC Host Rack Mount Server to PMAC System Inventory

Procedure 18. Add Rack Mount Server to PMAC System Inventory

Step #	Procedure	Description
This procedure adds a PMAC Host rack mount server to the PMAC system inventory. ***Prerequisite***: Complete Procedure 9. ***Note***: You cannot edit the RMS iLO IP address. To change this address, delete and then add the RMS with the correct address. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as pmacadmin user.

Step #	Procedure	Description
2. ☐	**PMAC GUI**: Configure RMS	Navigate to **Hardware > System Configuration > Configure RMS**. 
3. ☐	**PMAC GUI**: Add RMS	Click **Add RMS button** On **Main Menu: Hardware -> System Configuration -> Configure RMS**
4. ☐	**PMAC GUI**: Enter information	Enter the IP address of the rack mount server management port (iLO). All other fields are optional. Click **Add RMS**. Put name as desired but something meaningful.  ***Note***: If the initial credentials provided by Oracle have been changed, enter valid credentials (not to be confused with OS or application credentials) for the rack mount server management port.

Step #	Procedure	Description
5. ☐	**PMAC GUI**: Check for errors	If no error is reported to the user, the following displays:  Or, an error message displays: 
6. ☐	**PMAC GUI**: Verify RMS discovered	Navigate to **Hardware > System Inventory > Cabinet xxx > RMS yyy** where **xxx** is the cabinet ID selected when adding RMS (or unspecified) and **yyy** is the name of the RMS. 

Step #	Procedure	Description
		Periodically refresh the hardware information using the double arrow to the right of the Hardware Information title until the **Discovery State** changes from **Undiscovered** to **Discovered**. If **Status** displays an error, contact My Oracle Support (MOS) for assistance.  Check RMS on **Main Menu: Hardware -> System Configuration -> Configure RMS** 

4.7 Configure Enclosure Switches

If the enclosure switches used are Cisco 3020, execute Procedure 20.

If the switches used are HP 6120XG, execute Procedure 21.

If the enclosure switches used are HP6125G, execute Procedure 22.

If the enclosure switches used are HP6125XLG, execute Procedure 23.

If the enclosure switches used are HP6127XLG, execute Procedure 24.

Procedure 10. Configure 3020 Switches (netConfig)

Step #	Procedure	Description
This procedure configures 3020 switches from the PMAC server and the command line interface using templates included with an application. If the aggregation switches are supported by Oracle, then the Cisco 4948/4948E/4948E-F switches must be configured using section 4.3.1 Configure Aggregation Switches Configure Cisco 4948/4948E-F Aggregation Switches (PMAC Installed) (netConfig). If the aggregation switches are provided by the customer, ensure the customer aggregation switches are configured as per requirements provided in the NAPD. If there is any doubt as to whether the aggregation switches are provided by Oracle or the customer, contact My Oracle Support (MOS) and ask for assistance. Make sure no IPM activity is occurring or will occur during the execution of this procedure. ***Needed Material***: • HP Misc firmware ISO image • Release Notes of the HP Solutions Firmware Upgrade Pack, version 2.x.x [2] • Application specific documentation (documentation that referred to this procedure) • Template xml files in an application ISO on application media Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Virtual PMAC**: Prepare for switch configuration	Log into PMAC with admusr credentials and run: `$ /bin/ping -w3 <mgmtVLAN_gateway_address>`
2. ☐	**Virtual PMAC**: Verify network connective to 3020 switches	For each 3020 switch, verify network reachability. `$ /bin/ping -w3 <enclosure_switch_IP>`

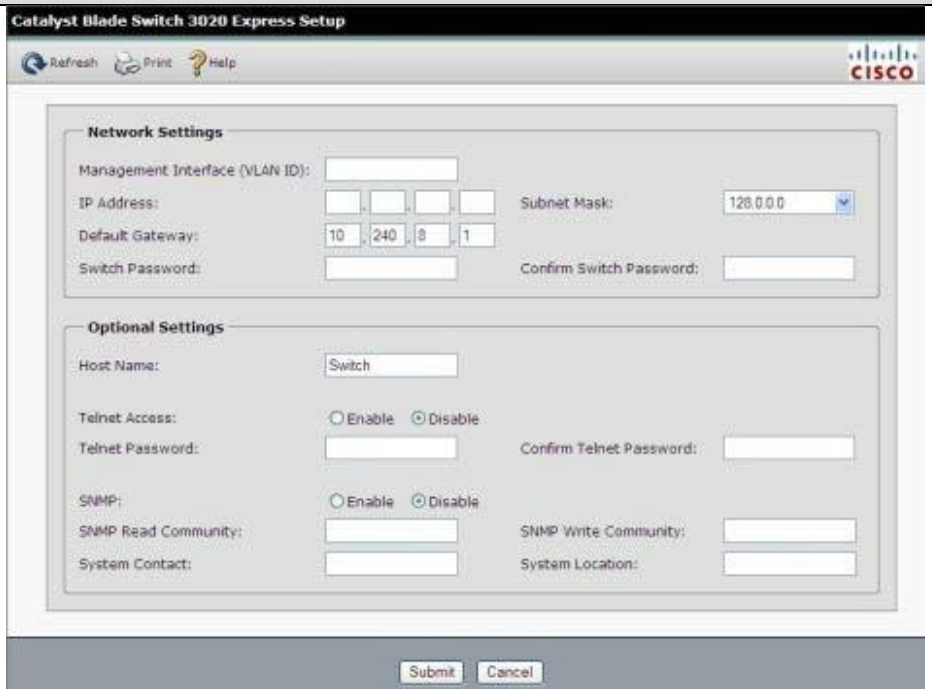
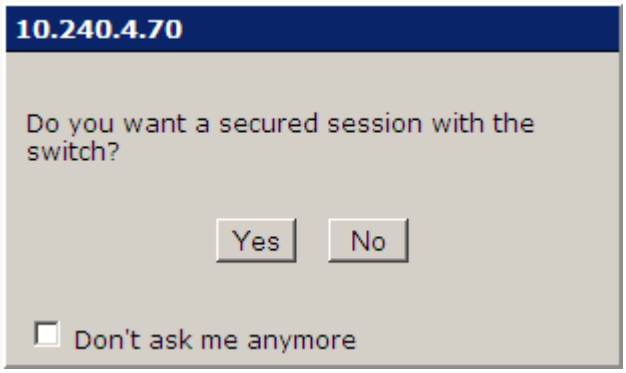
Step #	Procedure	Description

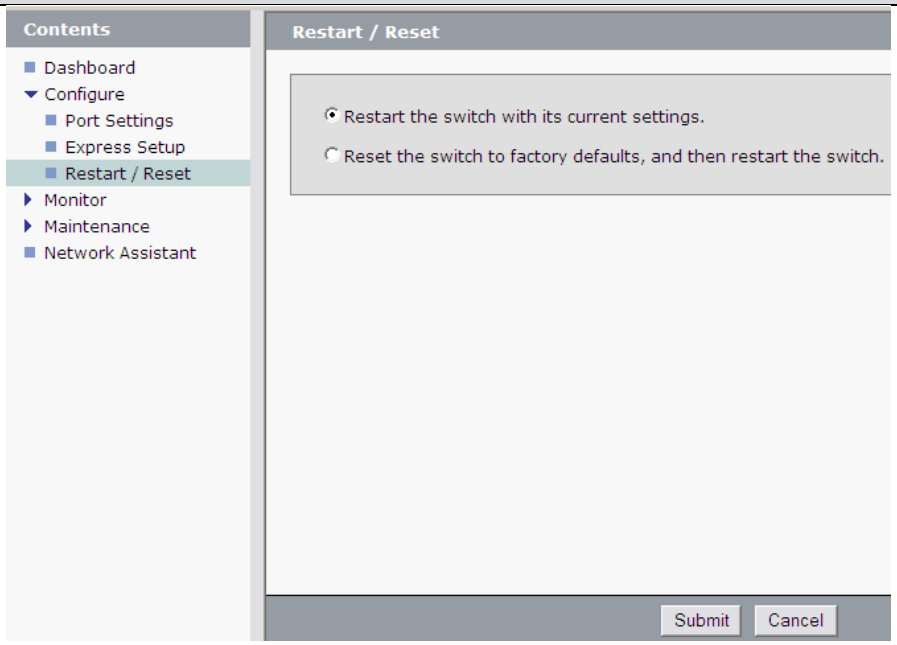
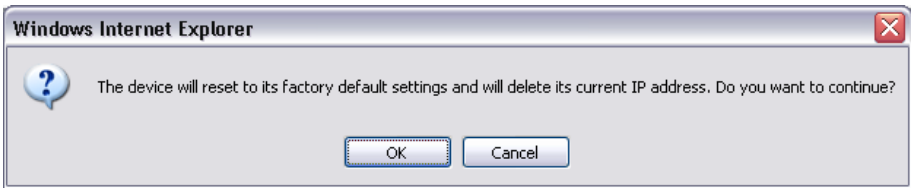
3. ☐	**Virtual PMAC**: Modify PMAC feature to allow TFTP	Enable the DEVICE.NETWORK.NETBOOT feature with the management role to allow tftp traffic:
		`$ sudo /usr/TKLC/smac/bin/pmacadm editFeature --featureName=DEVICE.NETWORK.NETBOOT --enable=1`
		`$ sudo /usr/TKLC/smac/bin/pmacadm resetFeatures`
		Note: This may take up to 60 seconds to complete.

4. ☐	**Virtual PMAC**: Verify the template xml files exist	Verify the initialization xml template file and configuration xml template file are present on the system and are the correct version for the system.
		Note: The XML files prepared in advance with the NAPD can be used as an alternative.
		`$ /bin/more /usr/TKLC/smac/etc/switch/xml/3020_init.xml`
		`$ /bin/more /usr/TKLC/smac/etc/switch/xml/3020_configure.xml`
		If either file does not exist, copy the files from the application media into the directory.
		If 3020_init.xml file exists, page through the contents to verify it is devoid of any site specific configuration information other than the device name. If the template file is appropriate, then skip step 5. and continue with step 6.
		If 3020_configure.xml file exists, page through the contents to verify it is the appropriate file for this site and edited for this site. All network information is necessary for this activity. If the template file is appropriate, then skip step 5. and continue with step 6.

5. ☐	**Virtual PMAC**: Modify 3020 xml files to configure the switch	Update the 3020_init.xml and 3020_configure.xml files. When done editing the file, save and quit.
		`$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/3020_init.xml`
		`$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/3020_config.xml`

6. ☐	**Virtual PMAC/OA GUI**: Reset switch to factory defaults	***Note***: Do not wait for the switch to finish reloading before proceeding to step 7. 1. If the switch has been previously configured using netConfig or previous attempts at initialization have failed, use netConfig to reset the switch to factory defaults by executing this command: `$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> setFactoryDefault` 2. If the above command failed, use Internet Explorer to navigate to <enclosure_switch_ip_address>. If you are asked for a username and password, leave the username blank and use the appropriate password provided by the application documentation. Click **OK**. 3. If the Express Setup screen displays, click **Refresh**.

Step #	Procedure	Description
		 4. Click **No** if asked you want a secured session.  The new Catalyst Blade Switch 3020 Device Manager opens. 5. Navigate to **Configure > Restart/Reset**. 6. Click the **Reset the switch to factory defaults . . .** option and click **Submit**.

Step #	Procedure	Description
		 7. Click **OK** to reset to factory default settings. 

7. ☐	**Virtual PMAC**: Remove old ssh key and initial switch	To remove the old ssh key type:
		`$ sudo /usr/bin/ssh-keygen -R <enclosure_switch_ip>`
		The following command must be entered at least 60 seconds and at most 5 minutes after the previous step is completed.
		`$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch/xml/3020_init.xml`
		`Processing file: /usr/TKLC/smac/etc/switch/xml/3020_init.xml`
		`Waiting to load the configuration file...`
		`loaded.`
		`Attempting to login to device...`
		`Configuring....`
		Note: This step takes about 10-15 minutes to complete, it is imperative that you wait until returned to the command prompt. DO NOT PROCEED UNTIL RETURNED TO THE COMMAND PROMPT.
		Check the output of this command for any errors. A successful completion of netConfig returns the user to the prompt. Due to strict host checking and the narrow window of time in which to perform the command, this command is prone to user error. Most issues are corrected by returning to the previous step and continuing. If this step has failed for a second time, stop the procedure and contact My Oracle Support (MOS).

Step #	Procedure	Description

8. ☐	**Virtual PMAC**: Reboot switch using netConfig	`$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> reboot save=no`
		Wait 2-3 minutes for the switch to reboot. Verify it has completed rebooting and is reachable by pinging it.
		`$ /bin/ping <enclosure_switch_IP>`
		`From 10.240.8.48 icmp_seq=106 Destination Host Unreachable`
		`From 10.240.8.48 icmp_seq=107 Destination Host Unreachable`
		`From 10.240.8.48 icmp_seq=108 Destination Host Unreachable`
		`64 bytes from 10.240.8.13: icmp_seq=115 ttl=255 time=1.13 ms`
		`64 bytes from 10.240.8.13: icmp_seq=116 ttl=255 time=1.20 ms`
		`64 bytes from 10.240.8.13: icmp_seq=117 ttl=255 time=1.17 ms`

9. ☐	**Virtual PMAC**: Configure switches	Configure both switches by issuing the following command:
		`$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch/xml/3020_configure.xml`
		`Processing file: /usr/TKLC/smac/etc/switch/xml/3020_configure.xml`
		Note: Following message is expected and can safely be ignored:
		NOTE: Command addVlan is deprecated!
		Note: This step takes about 2-3 minutes to complete.
		Check the output of this command for any errors. If the file fails to configure the switch, please review/troubleshoot the file first. If troubleshooting is unsuccessful, stop this procedure and contact My Oracle Support (MOS).
		A successful completion of netConfig returns the user to the prompt.

10. ☐	**Virtual PMAC**: Verify switch configuration	To verify the configuration was completed successfully, execute the following command and review the configuration:
		`# sudo /usr/TKLC/plat/bin/netConfig showConfiguration --device=<switch_name>`
		`Configuration: = (`
		`Building configuration...`
		`Current configuration : 3171 bytes`
		`!`
		`! Last configuration change at 23:54:24 UTC Fri Apr 2 1993 by plat`
		`!`
		`version 12.2`
		`<output removed to save space >`
		`monitor session 1 source interface Gi0/2 rx`
		`monitor session 1 destination interface Gi0/1 encapsulation replicate`
		`end`
		`)`
		Return to step 4. and repeat for each 3020 switch.

Step #	Procedure	Description

11. ☐	**Virtual PMAC**: Modify PMAC feature to disable tftp	Disable the DEVICE.NETWORK.NETBOOT feature:
		`$ sudo /usr/TKLC/smac/bin/pmacadm editFeature --featureName=DEVICE.NETWORK.NETBOOT --enable=0`
		`$ sudo /usr/TKLC/smac/bin/pmacadm resetFeatures`
		Note: This may take up to 60 seconds to complete.

12. ☐	Back up switches	Perform Appendix H.2 Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig) for each switch configured in this procedure.
13. ☐	**Virtual PMAC**: Clean up FW file	Remove the FW file from the tftp directory. `$ sudo /bin/rm -f /var/TKLC/smac/image/<FW_image>`

Procedure 11. Configure HP 6120XG Switch (netConfig)

Step #	Procedure	Description
This procedure configures HP 6120XG switches from the PMAC server and the command line using templates included with an application. The HP 6120XG enclosure switch supports configuration of IPv6 addresses, but it does not support configuration of a default route for those IPv6 interfaces. Instead, the device relies on router advertisements to obtain default route(s) for those interfaces. For environments where IPv6 routes are needed (NTP, etc.), router advertisements need to be enabled either on the aggregation switch or customer network. ***Needed Material***: • HP Misc firmware ISO image • Release Notes of the HP Solutions Firmware Upgrade Pack, version 2.x.x [2] • Application specific documentation (documentation that referred to this procedure) • Template xml files in an application ISO on application media Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		

1. ☐	**Virtual PMAC**: Prepare for switch configuration	If the aggregation switches are supported by Oracle, log into the management server, then run:
		`$ /bin/ping -w3 <switch1A_mgmtVLAN_address>`
		`$ /bin/ping -w3 <switch1B_mgmtVLAN_address>`
		`$ /bin/ping -w3 <switch_mgmtVLAN_VIP>`
		If the aggregation switches are provided by the customer, log into the management server, then run:
		`$ /bin/ping -w3 <mgmtVLAN gateway address>`

Step #	Procedure	Description
2. ☐	**Virtual PMAC**: Verify network connective to 6120XG switches	For each 6120XG switch, verify network reachability. `$ /bin/ping -w3 <enclosure_switch_IP>`

3. ☐	**Virtual PMAC/OA GUI**: Reset switch to factory defaults	If the 6120XG switch has been configured before this procedure, clear the configuration using the following command:
		`$ /usr/bin/ssh <username>@<enclosure_switch_IP>`
		`Switch# config`
		`Switch(config)# no password all`
		`Password protection for all will be deleted, continue [y/n]? y`
		`Switch(config)# end`
		`Switch# erase startup-config`
		`Configuration will be deleted and device rebooted, continue [y/n]? y`
		`(switch will automatically reboot, reboot takes about 120-180 seconds)`
		Note: You may need to press **Enter** twice. You may also need to use previously configured credentials.
		If the above procedures fails, login using telnet and reset the switch to manufacturing defaults. If the above ssh procedures fails, login using telnet and reset the switch to manufacturing defaults.
		`$ /usr/bin/telnet <enclosure_switch_IP>`
		`Switch# config`
		`Switch(config)# no password all (answer yes to question)`
		`Password protection for all will be deleted, continue [y/n]? y`
		`Switch(config)# end`
		`Switch# erase startup-config`
		`(switch will automatically reboot, reboot takes about 120-180 seconds)`
		Note: The console connection to the switch must be closed, or the initialization fails.

Step #	Procedure	Description

4. ☐	**Virtual PMAC**: Copy switch configuration template from the media to the tftp directory	Copy the switch initialization template and configuration template from the media to the tftp directory.
		`$ sudo /bin/cp -i /<path to media>/6120XG_template_init.xml /usr/TKLC/smac/etc/switch/xml`
		`$ sudo /bin/cp -i /<path to media>/6120XG_[single,LAG]Uplink_configure.xml /usr/TKLC/smac/etc/switch/xml`
		`$ sudo /bin/cp –i /usr/TKLC/plat/etc/TKLCnetwork-config-templates/templates/utility/addQOS_trafficTemplate_6120XG.xml /usr/TKLC/smac/etc/switch/xml`
		• Where [single,LAG] are variables for either one of two files.
		  • **6120XG_SingleUplink_configure.xml** is for one uplink per enclosure switch topology
		  • 6120XG_LAGUplink_configure.xml is for LAG uplink topology

5. ☐	**Virtual PMAC**: Verify template files are in the xml directory	Verify the switch initialization template file and configuration file template are in the correct directory.
		`$ sudo /bin/ls -i -l /usr/TKLC/smac/etc/switch/xml/`
		`-rw-r--r-- 1 root root 1955 Feb 16 11:36 /usr/TKLC/smac/etc/switch/xml/6120XG_template_init.xml`
		`-rw-r--r-- 1 root root 1955 Feb 16 11:36 /usr/TKLC/smac/etc/switch/xml/6120XG_[single,LAG]Uplink_configure.xml`
		`-rw-r--r-- 1 root root 702 Sep 10 10:33 addQOS_trafficTemplate_6120XG.xml`

Step #	Procedure	Description

6. ☐	**Virtual PMAC**: Edit files for site specific information	Edit the switch initialization file and switch configuration file template for site specific addresses, VLAN IDs, and other site specific content.
		Note: Note the files that are created in this step can be prepared ahead of time using the NAPD.
		Note: Move the addVlan commands above the configuration of the uplink so all VLANs, which should be allowed on the uplink, exist at the moment the setLinkAggregation command is executed
		`$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/6120XG_template_init.xml`
		`$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/6120XG_[single,LAG]Uplink_configure.xml`
		`$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/addQOS_trafficTemplate_6120XG.xml`
		Note: Following messages are expected and can safely be ignored:
		INFO: "The vlanID option has been deprecated. Use the interface option."
		NOTE: Command addVlan is deprecated!
		Note: For IPv6 configurations, IPv6 configuration for remote syslog is not currently supported on the HP6120XG switches. This function must be configured for IPv4.

7. ☐	**Virtual PMAC**: Apply include-credentials command to switch	Log into the switch using SSH
		`$ /usr/bin/ssh <username>@<enclosure_switch_IP>`
		`Switch# config`
		`Switch(config)# include-credentials`
		If prompted, answer **yes** to both questions.
		Logout of the switch.
		`Switch(config)# logout`
		`Do you want to log out [y/n]? y`
		`Do you want to save current configuration [y/n/^C]? y`

8. ☐	**Virtual PMAC**: Initialize switch	`$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch/xml/6120XG_template_init.xml` This could take up to 5-10 minutes. ***Note***: Upon successful completion of netConfig, the user returns to the PMAC command prompt. If netConfig fails to complete successfully, contact My Oracle Support (MOS).

Step #	Procedure	Description
9. ☐	**Virtual PMAC**: Configure switch	`$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch/xml/6120XG_[single,LAG]Uplink_configure.xml` ***Note***: Following messages are expected and can safely be ignored: INFO: "The vlanID option has been deprecated. Use the interface option." NOTE: Command addVlan is deprecated! This could take up to 2-3 minutes. ***Note***: Upon successful completion of netConfig, the user returns to the PMAC command prompt. If netConfig fails to complete successfully, contact My Oracle Support (MOS)

10. ☐	**Virtual PMAC**: Apply QoS traffic template settings	`$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch/xml/addQOS_trafficTemplate_6120XG.xml`
		Note: The switch reboots after this command. This step takes 2-5 minutes.
		A workaround is provided in case *you get the below output*:
		`<!-- This file creates the 'egressDrop' traffic template on the 6120XG switches to set the egress-discard-threshold for queue 2 to medium. -->`
		`<!-- This ensures that packets are dropped (when necessary) on egress instead of ingress to avoid filling the transmit buffers and losing all traffic. -->`
		Edit the template file as follows:
		1. `$ sudo vim /usr/TKLC/plat/etc/TKLCnetwork-config-templates/templates/utility/addQOS_trafficTemplate_6120XG.xml`
		2. Change configure to configure apiVersion="1.1"

11. ☐	**Virtual PMAC**: Verify configuration	Once each HP 6120XG has finished rebooting, verify network reachability and configuration.
		`$ /bin/ping -w3 <enclosure_switch_IP>`
		`$ /usr/bin/ssh <switch_platform_username>@<enclosure_switch_IP>`
		`<switch_platform_username>@<enclosure_switch_IP>'s password:`
		`<switch_platform_password>`
		`Switch# show run`
		Inspect the output of **show run**, and ensure it is configured as per site requirements.

12. ☐	Repeat	Repeat steps 3. through 11. for each HP 6120XG switch.
13. ☐	Back up switches	Perform Appendix H.1 Back Up HP (6120XG, 6125G, 6125XLG, 6127XLG) Enclosure Switch for each switch configured in this procedure.

Step #	Procedure	Description
14. ☐	**Virtual PMAC**: Clean up FW file	Remove the FW file from the tftp directory. `$ sudo /bin/rm -f ~<switch_backup_user>/<FW_image>`

Procedure 11. Configure HP 6125G Switch (netConfig)

Step #	Procedure	Description
This procedure configures HP 6125G switches from the PMAC server and command line interface using templates included with an application. ***Needed Material***: • Application specific documentation (documentation that referred to this procedure) • Template xml files in an application ISO on application media Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		

1. ☐	**Virtual PMAC**: Prepare for switch configuration	If the aggregation switches are supported by Oracle, log into the management server, then run:
		`$ /bin/ping -w3 <switch1A_mgmtVLAN_address>`
		`$ /bin/ping -w3 <switch1B_mgmtVLAN_address>`
		`$ /bin/ping -w3 <switch_mgmtVLAN_VIP>`
		If the aggregation switches are provided by the customer, log into the management server, then run:
		`$ /bin/ping -w3 <mgmtVLAN gateway address>`

2. ☐	**Virtual PMAC**: Verify connectivity to OAs	For each OA, verify network reachability.
		`$ /bin/ping -w3 <OA1_IP>`
		`$ /bin/ping –w3 <OA2_IP>`

3. ☐	**Virtual PMAC**: Determine active OA	Log into OA1 to determine if it is active.
		`$ /usr/bin/ssh root@<OA1_IP>`
		The OA is active if you see the following:
		`Using username "root".`
		`----------`
		`WARNING: This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law.`
		`----------`
		`Firmware Version: 3.70`
		`Built: 10/01/2012 @ 17:53`
		`OA Bay Number: 2`
		`OA Role: Active`

Step #	Procedure	Description
		root@10.240.8.6's password: If you see the following, it is standby: Using username "root". ---------- WARNING: This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law. ---------- Firmware Version: 3.70 Built: 10/01/2012 @ 17:53 OA Bay Number: 1 OA Role: Standby root@10.240.8.5's password: Press **<ctrl>** + **C** to close the SSH session. If OA1 has a role of Standby, verify OA2 is the active by logging into it: $ /usr/bin/ssh root@<OA2_IP> Using username "root". ---------- WARNING: This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law. ---------- Firmware Version: 3.70 Built: 10/01/2012 @ 17:53 OA Bay Number: 2 OA Role: Active root@10.240.8.6's password: In the following steps, OA means the **active OA** and <active_OA_IP> is the IP address of the active OA. ***Note***: If neither OA reports active, STOP and contact My Oracle Support (MOS). Exit the ssh session.

Step #	Procedure	Description

4. ☐	**Virtual PMAC/OA GUI**: Reset switch to factory defaults	If the 6125G switch has been configured before this procedure, clear the configuration using the following command:
		`$/usr/bin/ssh root@<active_OA_IP>`
		`Using username "root".`
		`----------`
		`WARNING: This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law.`
		`----------`
		`Firmware Version: 3.70`
		`Built: 10/01/2012 @ 17:53`
		`OA Bay Number: 2`
		`OA Role: Active`
		`root@10.240.8.6's password: <OA_password>`
		`> connect interconnect <switch_IOBAY_#>`
		`Press [Enter] to display the switch console:`
		Note: You may need to press **Enter** twice. You may also need to use previously configured credentials.
		`<switch>reset saved-configuration`
		`The saved configuration file will be erased. Are you sure? [Y/N]:y`
		`Configuration file in flash is being cleared.`
		`Please wait ...`
		`MainBoard:`
		`Configuration file is cleared.`
		`<switch>reboot`
		`Start to check configuration with next startup configuration file, please`
		`wait.....DONE!`
		`This command will reboot the device. Current configuration will be lost, save`
		`current configuration? [Y/N]:n`
		`This command will reboot the device. Continue? [Y/N]: y`
		The switch automatically reboots. This takes about 120-180 seconds. The switch reboot is complete when you see the following text:
		`[…Output omitted…]`
		`User interface aux0 is available.`
		`Press ENTER to get started.`
		When the reboot is complete, disconnect from the console by pressing **ctrl** + **shift** + **-**, and then **d**.
		Note: If connecting to the virtual PMAC through the management server iLO, then follow Appendix C. Disconnect from the console by entering **ctrl** + **v**.
		Exit from the OA terminal:

Step #	Procedure	Description
		>exit ***Note***: The console connection to the switch must be closed, or the initialization fails.

5.
☐
	Virtual PMAC: Copy template	Copy switch initialization template and configuration template from the media to the tftp directory.
		`$ sudo /bin/cp -i /<path to media>/6125G_template_init.xml /usr/TKLC/smac/etc/switch/xml`
		`$ sudo /bin/cp -i /<path to media>/6125G_Pair-<#> configure.xml /usr/TKLC/smac/etc/switch/xml`

6.
☐
	Virtual PMAC: Verify template files are in the xml directory	Verify the switch initialization template file and configuration file template are in the correct directory.
		`$ sudo /bin/ls -i -l /usr/TKLC/smac/etc/switch/xml/`
		`-rw-r--r-- 1 root root 1955 Feb 16 11:36 /usr/TKLC/smac/etc/switch/xml/6125G_template_init.xml`
		`-rw-r--r-- 1 root root 1955 Feb 16 11:36 /usr/TKLC/smac/etc/switch/xml/6125G Pair-[#] configure.xml`

7.
☐
	Virtual PMAC: Edit files for site specific information	Edit the switch initialization file and switch configuration file template for site specific addresses, VLAN IDs, and other site specific content.
		Note: Move the addVlan commands above the configuration of the uplink so all VLANs, which should be allowed on the uplink, exist at the moment the setLinkAggregation command is executed
		Note: Following messages are expected and can safely be ignored:
		INFO: "The vlanID option has been deprecated. Use the interface option."
		NOTE: Command addVlan is deprecated!
		`$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/6125G_template_init.xml`
		`$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/6125G_Pair-<#>_configure.xml`
		Note: For IPv6 Configurations, IPv6 over NTP is NOT currently supported on the HP6125G switches. This function must be configured for IPv4.
		Note: Within the 6125G xml netConfig file, change this stanza to the value that represents your XMI VLAN ID:
		`<option name="access">access</option>`
		Example input:
		`<option name="access">$xmi vlan ID</option>`

8. ☐	**Virtual PMAC**: Initialize switch	***Note***: The console connection to the switch must be closed before performing this step. `$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch/xml/6125G_template_init.xml` This could take up to 5-10 minutes.

Step #	Procedure	Description

9. ☐	**Virtual PMAC**: Verify initialization	Verify the initialization succeeded with the following command:
		`$ sudo /usr/TKLC/plat/bin/netConfig getHostname --device=<switch_hostname>`
		`Hostname: <switch_hostname>`
		This could take up to 2-3 minutes.
		Note: Upon successful completion of netConfig, the user returns to the PMAC command prompt. If netConfig fails to complete successfully, contact My Oracle Support (MOS).

10. ☐	**Virtual PMAC**: Verify firmware	Execute Appendix L to verify the existing firmware version and downgrade if required.
11. ☐	**Virtual PMAC**: Configure switch	`$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch/xml/612G_Pair-<#>_configure.xml` ***Note***: Following messages are expected and can safely be ignored: INFO: "The vlanID option has been deprecated. Use the interface option." NOTE: Command addVlan is deprecated! INFO: "Cannot set vlanSTP on this device. Currently unsupported." This could take up to 2-3 minutes. ***Note***: Upon successful completion of netConfig, the user returns to the PMAC command prompt. If netConfig fails to complete successfully, contact My Oracle Support (MOS)
12. ☐	**Virtual PMAC**: Add IPv6 default route (IPv6 network only)	For IPv6 management networks, the enclosure switch requires an IPv6 default route to be configured. Apply the following command using netConfig: `$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> addRoute network=::/0 nexthop=<mgmtVLAN_gateway_address>`

13. ☐	**Virtual PMAC**: Verify configuration	Once each HP 6125G has finished rebooting, verify network reachability and configuration.
		`$ /bin/ping -w3 <enclosure_switch_IP>`
		`PING 10.240.8.10 (10.240.8.10) 56(84) bytes of data.64 bytes from 10.240.8.10:icmp_seq=1 ttl=255 time=0.637 ms64 bytes from 10.240.8.10: icmp_seq=2 ttl=255 time=0.661 ms64 bytes from 10.240.8.10: icmp_seq=3 ttl=255 time=0.732 m`
		`$ /usr/bin/ssh <switch_platform_username>@<enclosure_switch_IP>`
		`<switch_platform_username>@<enclosure_switch_IP>'s password:`
		`<switch_platform_password>`
		`Switch_hostname> display current-configuration`
		Inspect the output to ensure it is configured as per site requirements.

Step #	Procedure	Description
14. ☐	Repeat	Repeat steps 4. through 13. for each HP 6125G switch.
15. ☐	Back up switches	Perform Appendix H.1 Back Up HP (6120XG, 6125G, 6125XLG, 6127XLG) Enclosure Switch for each switch configured in this procedure.
16. ☐	**Virtual PMAC**: Clean up FW file	Remove the FW file from the tftp directory. `$ sudo /bin/rm -f ~<switch_backup_user>/<FW_image>`

Procedure 10. Configure HP 6125XLG Switch (netConfig)

Step #	Procedure	Description
This procedure configures HP 6125XLG switches from the PMAC server and the command line interface using templates included with an application. ***Needed Material***: • Application specific documentation (documentation that referred to this procedure) • Template xml files in an application ISO on application media Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		

1. ☐	**Virtual PMAC**: Prepare for switch configuration	If the aggregation switches are supported by Oracle, log into the management server, then run:
		`$ /bin/ping -w3 <switch1A_mgmtVLAN_address>`
		`$ /bin/ping -w3 <switch1B_mgmtVLAN_address>`
		`$ /bin/ping -w3 <switch_mgmtVLAN_VIP>`
		If the aggregation switches are provided by the customer, log into the management server, then run:
		`$ /bin/ping -w3 <mgmtVLAN gateway address>`

2. ☐	**Virtual PMAC**: Verify connectivity to OAs	For each OA, verify network reachability.
		`$ /bin/ping -w3 <OA1_IP>`
		`$ /bin/ping –w3 <OA2_IP>`

3. ☐	**Virtual PMAC**: Determine active OA	Log into OA1 to determine if it is active.
		`$ /usr/bin/ssh root@<OA1_IP>`
		The OA is active if you see the following:
		`Using username "root".`
		`----------`
		`WARNING: This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law.`
		`----------`
		`Firmware Version: 3.70`

Step #	Procedure	Description
		Built: 10/01/2012 @ 17:53 OA Bay Number: 2 OA Role: Active root@10.240.8.6's password: If you see the following, it is standby: Using username "root". WARNING: This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law. Firmware Version: 3.70 Built: 10/01/2012 @ 17:53 OA Bay Number: 1 OA Role: Standby root@10.240.8.5's password: Press **<ctrl>** + **C** to close the SSH session. If OA1 has a role of Standby, verify OA2 is the active by logging into it: $ /usr/bin/ssh root@<OA2_IP> Using username "root". WARNING: This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law. Firmware Version: 3.70 Built: 10/01/2012 @ 17:53 OA Bay Number: 2 OA Role: Active root@10.240.8.6's password: In the following steps, OA means the **active OA** and <active_OA_IP> is the IP address of the active OA. ***Note***: If neither OA reports active, STOP and contact My Oracle Support (MOS). Exit the ssh session.
4. □	**Virtual PMAC/OA GUI**: Reset switch to factory defaults	If the 6125XLG switch has been configured before this procedure, clear the configuration using the following command: $/usr/bin/ssh root@<active_OA_IP> Using username "root". WARNING: This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law. Firmware Version: 3.70 Built: 10/01/2012 @ 17:53

Step #	Procedure	Description
		OA Bay Number: 2 OA Role: Active root@10.240.8.6's password: <OA_password> > connect interconnect <switch_IOBAY_#> Press [Enter] to display the switch console: ***Note***: You may need to press **Enter** twice. You may also need to use previously configured credentials. <switch>reset saved-configuration The saved configuration file will be erased. Are you sure? [Y/N]:y Configuration file in flash is being cleared. Please wait ... MainBoard: Configuration file is cleared. <switch>reboot Start to check configuration with next startup configuration file, please wait.....DONE! This command will reboot the device. Current configuration will be lost, save current configuration? [Y/N]:n This command will reboot the device. Continue? [Y/N]: y The switch automatically reboots. This takes about 120-180 seconds. The switch reboot is complete when the switch begins the auto configuration sequence. When the reboot is complete, disconnect from the console by pressing **ctrl** + **shift** + **-**, and then **d**. ***Note***: If connecting to the virtual PMAC through the management server iLO, then follow Appendix C. Disconnect from the console by entering **ctrl** + **v**. Exit from the OA terminal: >exit ***Note***: The console connection to the switch must be closed, or the initialization fails.

5. □	**Virtual PMAC**: Copy template	Copy switch initialization template and configuration template from the media to the tftp directory.
		$ sudo /bin/cp -i /<path to media>/6125XLG_template_init.xml /usr/TKLC/smac/etc/switch/xml
		$ sudo /bin/cp -i /<path to media>/6125XLG_configure.xml /usr/TKLC/smac/etc/switch/xml

Step #	Procedure	Description

6. ☐	**Virtual PMAC**: Verify template files are in the xml directory	Verify the switch initialization template file and configuration file template are in the correct directory.
		`$ sudo /bin/ls -i -l /usr/TKLC/smac/etc/switch/xml/`
		`131195 -rw------- 1 root root 248 May 5 11:01 6125XLG_IOBAY3_template_init.xml`
		`131187 -rw------- 1 root root 248 May 5 10:54 6125XLG_IOBAY5_template_init.xml`
		`131190 -rw------- 1 root root 6194 Mar 24 15:04 6125XLG_IOBAY8-config.xml`
		`131189 -rw------- 1 root root 248 Mar 25 09:43 6125XLG_IOBAY8_template_init.xml`

7. ☐	**Virtual PMAC**: Edit files for site specific information	Edit the switch initialization file and switch configuration file template for site specific addresses, VLAN IDs, and other site specific content.
		`$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/6125XLG_init.xml`
		`$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/6125XLG_configure.xml`

8. ☐	**Virtual PMAC**: Initialize switch	***Note***: The console connection to the switch must be closed before performing this step. `$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch/xml/6125XLG_init.xml` This could take up to 5-10 minutes.

9. ☐	**Virtual PMAC**: Verify initialization	Verify the initialization succeeded with the following command:
		`$ sudo /usr/TKLC/plat/bin/netConfig getHostname --device=<switch_hostname>`
		`Hostname: <switch_hostname>`
		This could take up to 2-3 minutes.
		Note: Upon successful completion of netConfig, the user returns to the PMAC command prompt. If netConfig fails to complete successfully, contact My Oracle Support (MOS).

10. ☐	**Virtual PMAC**: Configure switch	`$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch/xml/612XLG_configure.xml` ***Note***: Following messages are expected and can safely be ignored: INFO: "The vlanID option has been deprecated. Use the interface option." NOTE: Command addVlan is deprecated! This could take up to 2-3 minutes. ***Note***: Upon successful completion of netConfig, the user returns to the PMAC command prompt. If netConfig fails to complete successfully, contact My Oracle Support (MOS)

Step #	Procedure	Description
11. ☐	**Virtual PMAC**: Add IPv6 default route (IPv6 network only)	For IPv6 management networks, the enclosure switch requires an IPv6 default route to be configured. Apply the following command using netConfig: `$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> addRoute network=::/0 nexthop=<mgmtVLAN_gateway_address>`

12. ☐	**Virtual PMAC**: Verify configuration	Once each HP 6125XLG has finished rebooting, verify network reachability and configuration.
		`PING 10.240.8.10 (10.240.8.10) 56(84) bytes of data.64 bytes from 10.240.8.10:`
		`icmp_seq=1 ttl=255 time=0.637 ms64 bytes from 10.240.8.10: icmp_seq=2 ttl=255`
		`time=0.661 ms64 bytes from 10.240.8.10: icmp_seq=3 ttl=255 time=0.732 m`
		`$ /usr/bin/ssh <switch_platform_username>@<enclosure_switch_IP>`
		`<switch_platform_username>@<enclosure_switch_IP>'s password:`
		`<switch_platform_password>`
		`Switch_hostname> display current-configuration`
		Inspect the output to ensure it is configured as per site requirements.

13. ☐	**Virtual PMAC**: Configure ports	For HP 6125XLG switches connected by 4x1GE LAG uplink perform Utility procedure Appendix M; otherwise, for deployments with 10GE uplink, continue to the next step.
14. ☐	Repeat	Repeat steps 4. through 13. for each HP 6125XLG switch.
15. ☐	**Virtual PMAC**: Set downlinks	For HP 6125XLG switches with 4x1GE uplink to customer switches, field personnel are expected to work with the customer to set their downlinks to the HP 6125XLG 4x1GE LAG to match speed and duplex set in step 13. For HP 6125XLG switches with 4x1GE LAG uplink to Cisco 4948/E/E-F aggregation switches, perform Appendix M to match speed and duplex settings from step 13. ; otherwise, for deployments with a 10GE uplink, continue to the next step.
16. ☐	Back up switches	Perform Appendix H.1 Back Up HP (6120XG, 6125G, 6125XLG,) Enclosure Switch for each switch configured in this procedure.
17. ☐	**Virtual PMAC**: Clean up FW file	Remove the FW file from the tftp directory. `$ sudo /bin/rm -f ~<switch_backup_user>/<FW_image>`

Procedure 24. **Configure HP 6127XLG Switch (netConfig)**

Step #	Procedure	Description
This procedure configures HP 6127XLG switches from the PMAC server and the command line interface using templates included with an application. ***Needed Material***: • Application specific documentation (documentation that referred to this procedure) • Template xml files in an application ISO on application media Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		

1. ☐	**Virtual PMAC**: Prepare for switch configuration	If the aggregation switches are supported by Oracle, log into the management server, then run:
		`$ /bin/ping -w3 <switch1A_mgmtVLAN_address>`
		`$ /bin/ping -w3 <switch1B_mgmtVLAN_address>`
		`$ /bin/ping -w3 <switch_mgmtVLAN_VIP>`
		If the aggregation switches are provided by the customer, log into the management server, then run:
		`$ /bin/ping -w3 <mgmtVLAN gateway address>`

2. ☐	**Virtual PMAC**: Verify connectivity to OAs	For each OA, verify network reachability.
		`$ /bin/ping -w3 <OA1_IP>`
		`$ /bin/ping -w3 <OA2_IP>`

3. ☐	**Virtual PMAC**: Determine active OA	Log into OA1 to determine if it is active.
		`$ /usr/bin/ssh root@<OA1_IP>`
		The OA is active if you see the following:
		`Using username "root".`
		`WARNING: This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law.`
		`Firmware Version: 3.70`

Step #	Procedure	Description
		Built: 10/01/2012 @ 17:53 OA Bay Number: 2 OA Role: Active root@10.240.8.6's password: If you see the following, it is standby: Using username "root". WARNING: This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can resultin criminal or civil prosecution under applicable law. Firmware Version: 3.70 Built: 10/01/2012 @ 17:53 OA Bay Number: 1 OA Role: Standby root@10.240.8.5's password: Press **<ctrl>** + **C** to close the SSH session. If OA1 has a role of Standby, verify OA2 is the active by logging into it: $ /usr/bin/ssh root@<OA2_IP> Using username "root". WARNING: This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can resultin criminal or civil prosecution under applicable law. Firmware Version: 3.70 Built: 10/01/2012 @ 17:53 OA Bay Number: 2 OA Role: Active root@10.240.8.6's password: In the following steps, OA means the **active OA** and <active_OA_IP> is the IPaddress of the active OA. ***Note***: If neither OA reports active, STOP and contact My Oracle Support (MOS). Exit the ssh session.
4.	**Virtual PMAC/OA GUI**: Reset switch to factory defaults	If the 6127XLG switch has been configured before this procedure, clear the configuration using the following command: $/usr/bin/ssh root@<active_OA_IP> Using username "root". WARNING: This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law. Firmware Version: 3.70 Built: 10/01/2012 @ 17:53

Step #	Procedure	Description
		OA Bay Number: 2 OA Role: Active root@10.240.8.6's password: <OA_password> > connect interconnect <switch_IOBAY_#> Press [Enter] to display the switch console: ***Note***: You may need to press **Enter** twice. You may also need to use previously configured credentials. <switch>reset saved-configuration The saved configuration file will be erased. Are you sure? [Y/N]:y Configuration file in flash is being cleared. Please wait ... MainBoard: Configuration file is cleared. <switch>reboot Start to check configuration with next startup configuration file, please wait..... DONE! This command will reboot the device. Current configuration will be lost, save current configuration? [Y/N]:n This command will reboot the device. Continue? [Y/N]: y The switch automatically reboots. This takes about 120-180 seconds. Theswitch reboot is complete when the switch begins the auto configuration sequence. When the reboot is complete, disconnect from the console by pressing **ctrl** + **shift** + **-**, and then **d**. ***Note***: If connecting to the virtual PMAC through the management server iLO,then follow Appendix C. Disconnect from the console by entering **ctrl** +**v**. Exit from the OA terminal: >exit ***Note***: The console connection to the switch must be closed, or the initialization fails.

5.	**Virtual PMAC**: Copy template	Copy switch initialization template and configuration template from the media tothe tftp directory.
		$ sudo /bin/cp -i /<path to media>/6127XLG_template_init.xml /usr/TKLC/smac/etc/switch/xml
		$ sudo /bin/cp -i /<path to media>/6127XLG_configure.xml /usr/TKLC/smac/etc/switch/xml

Step #	Procedure	Description

6. ☐	**Virtual PMAC**: Verify template files are in the xml directory	Verify the switch initialization template file and configuration file template are inthe correct directory.
		`$ sudo /bin/ls -i -l /usr/TKLC/smac/etc/switch/xml/`
		`6127XLG_<IOBAYx>_template_init.xml`
		`6127XLG_<IOBAYx>_template_init.xml`
		`6127XLG_<IOBAYx>_config.xml`
		`6127XLG_<IOBAYx>_template_init.xml`

7. ☐	**Virtual PMAC**: Edit files for site specific information	Edit the switch initialization file and switch configuration file template for site specific addresses, VLAN IDs, and other site specific content.
		`$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/6127XLG_init.xml`
		`$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/6127XLG_configure.xml`

8. ☐	**Virtual PMAC**: Initialize switch	***Note***: The console connection to the switch must be closed before performingthis step. `$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch/xml/6127XLG_init.xml` This could take up to 5-10 minutes.

9. ☐	**Virtual PMAC**: Verify initialization	Verify the initialization succeeded with the following command:
		`$ sudo /usr/TKLC/plat/bin/netConfig getHostname --device=<switch_hostname>`
		`Hostname: <switch_hostname>`
		This could take up to 2-3 minutes.
		Note: Upon successful completion of netConfig, the user returns to the PMAC command prompt. If netConfig fails to complete successfully, contact My Oracle Support (MOS).

10. ☐	**Virtual PMAC**: Configure switch	`$ sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch/xml/6127XLG_configure.xml` ***Note***: Following messages are expected and can safely be ignored: INFO: "The vlanID option has been deprecated. Use the interface option." NOTE: Command addVlan is deprecated!This could take up to 2-3 minutes. ***Note***: Upon successful completion of netConfig, the user returns to the PMAC command prompt. If netConfig fails to complete successfully, contact My Oracle Support (MOS)

Step #	Procedure	Description
11.	**Virtual PMAC**: Add IPv6 default route (IPv6 network only)	For IPv6 management networks, the enclosure switch requires an IPv6 defaultroute to be configured. Apply the following command using netConfig: `$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> addRoute network=::/0 nexthop=<mgmtVLAN gateway address>`

12.	**Virtual PMAC**: Verify configuration	Once each HP 6127XLG has finished rebooting, verify network reachability and configuration.
		`PING 10.240.8.10 (10.240.8.10) 56(84) bytes of data.64 bytes from 10.240.8.10:`
		`icmp_seq=1 ttl=255 time=0.637 ms64 bytes from 10.240.8.10: icmp_seq=2 ttl=255`
		`time=0.661 ms64 bytes from 10.240.8.10: icmp_seq=3 ttl=255 time=0.732 m`
		`$ /usr/bin/ssh <switch_platform_username>@<enclosure_switch_IP>`
		`<switch_platform_username>@<enclosure_switch_IP>'s password:`
		`<switch_platform_password>`
		`Switch_hostname> display current-configuration`
		Inspect the output to ensure it is configured as per site requirements.

13.	Repeat	Repeat steps 4. through 12. for each HP 6127XLG switch.
14.	Back up switches	Perform Appendix H.1 Back Up HP (6120XG, 6125G, 6125XLG, 6127XLG) Enclosure Switch for each switch configured in this procedure.
15.	**Virtual PMAC**: Clean up FW file	Remove the FW file from the tftp directory. `$ sudo /bin/rm -f ~<switch_backup_user>/<FW_image>`

4.8 Server Blades Installation Preparation

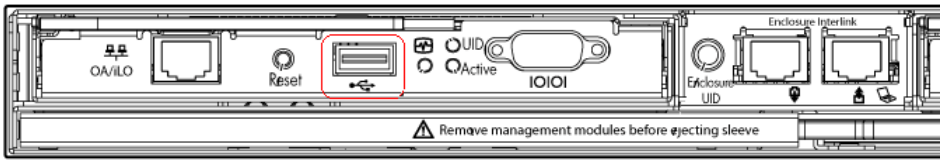
4.8.1 Upgrade Blade Server Firmware

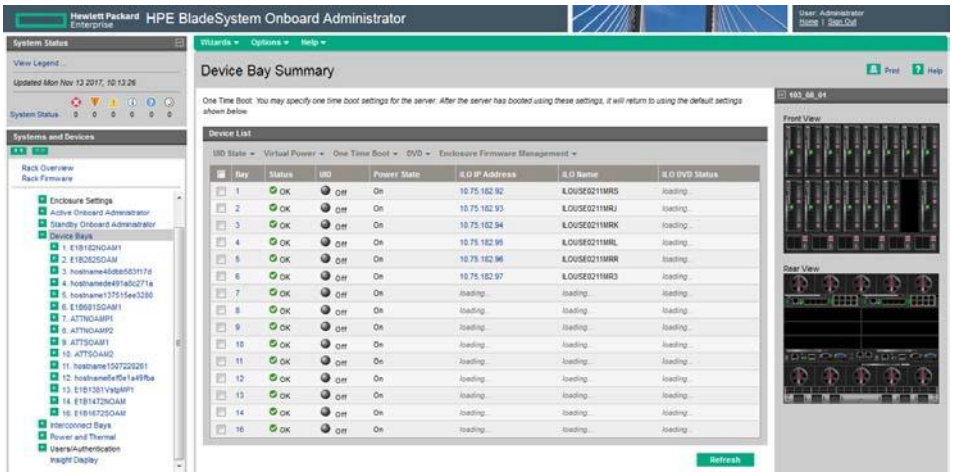
Software Centric Customers: If Oracle Consulting Services or any other Oracle Partner is providing services to a customer that includes installation and/or upgrade, then, as long as the terms of the scope of those services include that Oracle Consulting Services is employed as an agent of the customer (including update of Firmware on customer provided services), Oracle consulting services can install FW they obtain from the customer who is licensed for support from HP.

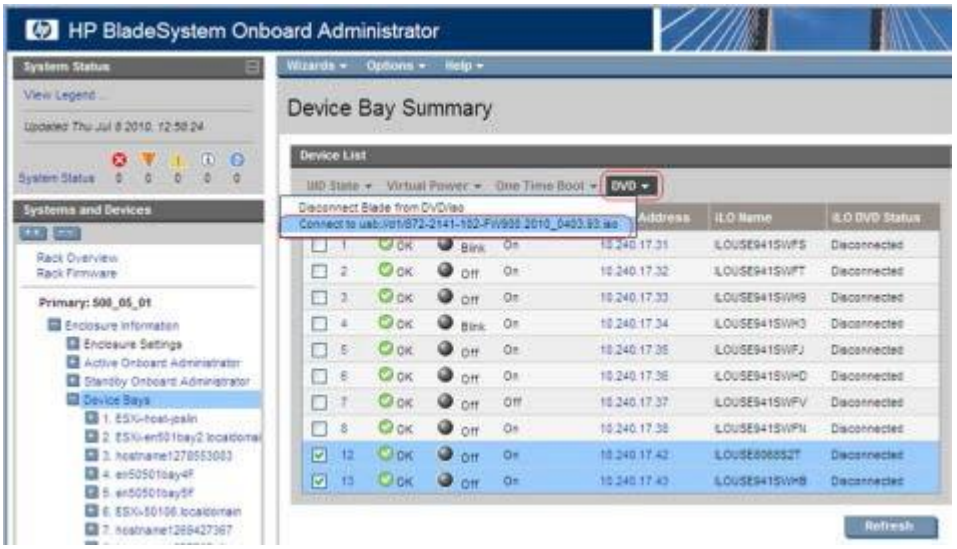
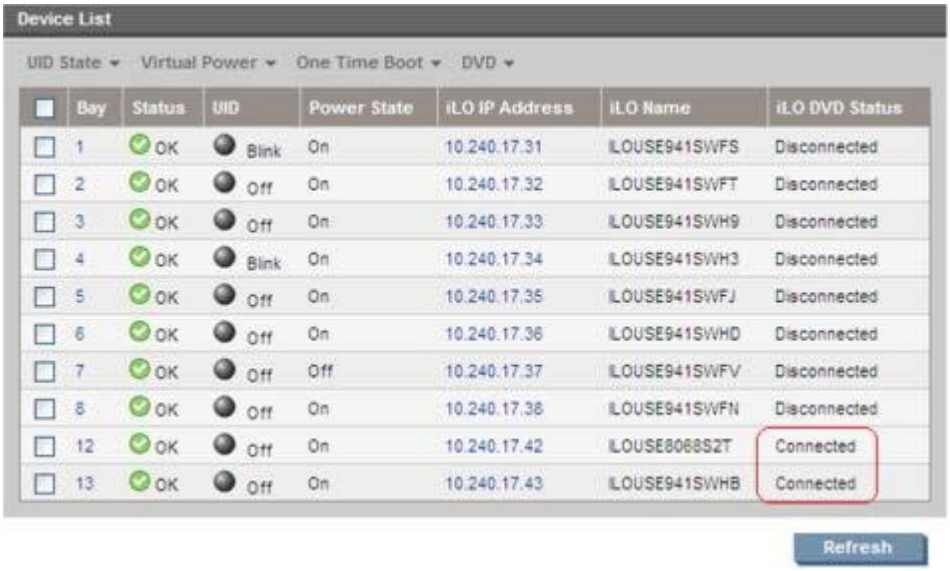
Note: This procedure uses a custom SPP version that cannot be obtained from the customer and, therefore, cannot be used for a Software Centric Customer. Software Centric Customers must ensure their firmware versions match those detailed in the *HP Solutions Firmware Upgrade Pack, Software Centric Release Notes* document.

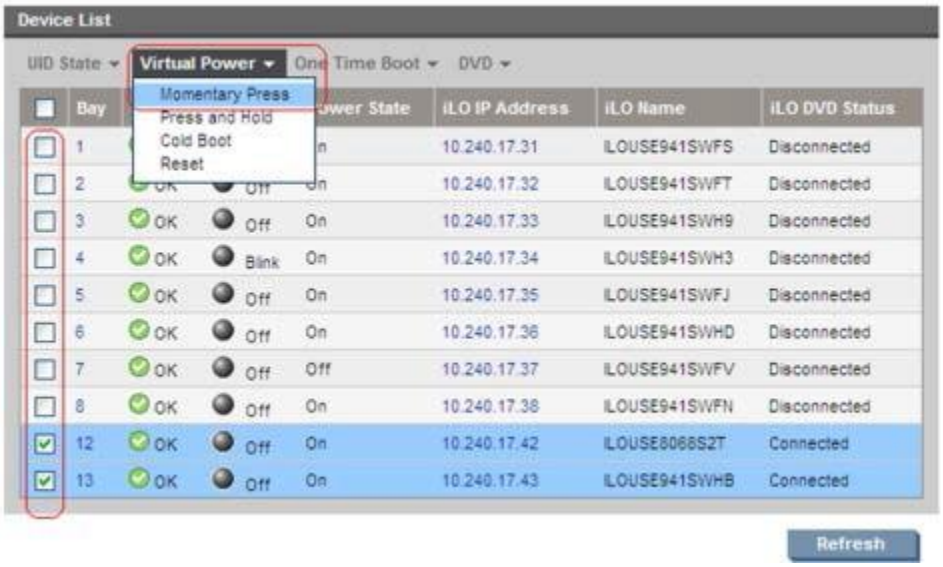
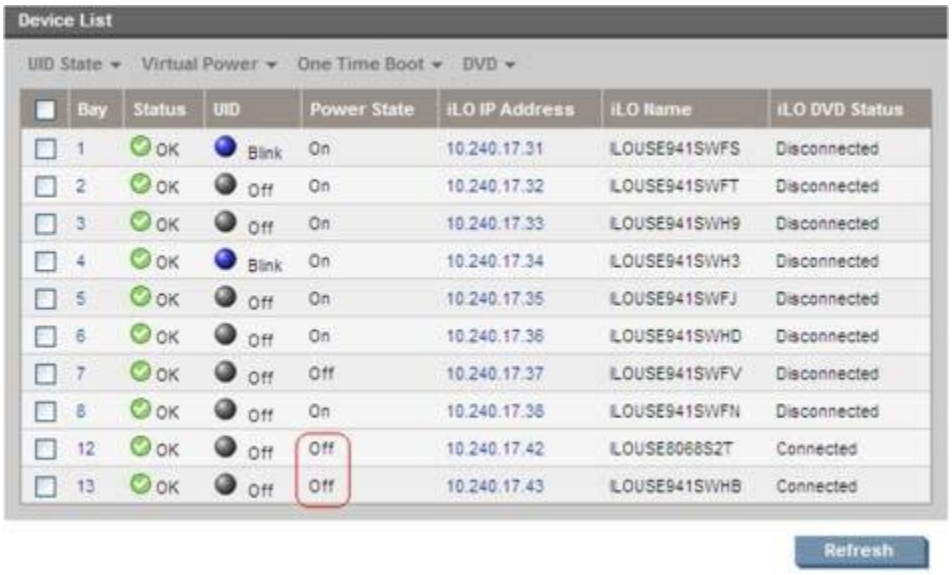
The HP Support Pack for ProLiant installer automatically detects the firmware components available on the target server and only upgrades those components with firmware older than what is on the current ISO.

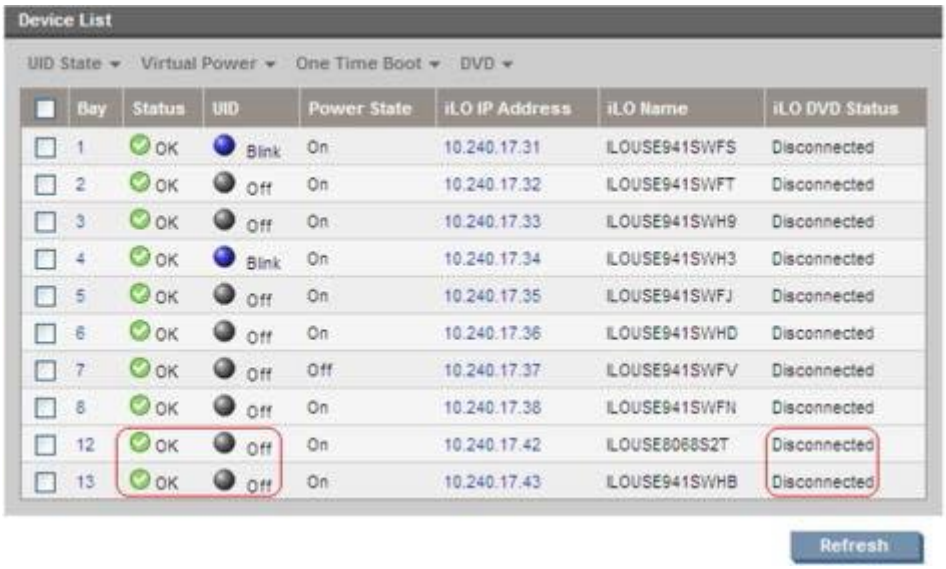
Procedure 11. Upgrade Blade Server Firmware

Step #	Procedure	Description
This procedure upgrades the firmware on the Blade servers. ***Needed Material***: • HP Service Pack for ProLiant (SPP) firmware ISO image • HP MISC firmware ISO image (for errata updates if applicable) • Release Notes of the HP Solutions Firmware Upgrade Pack, version 2.x.x [2] • USB Flash Drive (4GB or larger and formatted as FAT32) Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Local Workstation**: Copy image	Copy the HP Support Pack for ProLiant (SPP) ISO image to the USB flash drive.
2. ☐	Insert USB flash drive	Insert the USB flash drive with the HP Support Pack for ProLiant ISO into the USB port of the active OA module. 

Step #	Procedure	Description
3. ☐	**Active OA GUI**: Login	Navigate to the IP address of the active OA, using Appendix I. Login as an administrative user.
4. ☐	**OA Web GUI**: Access the device summary page	On the left pane, expand the Device Bays node to display the Device Bay Summary window. Select the individual blade servers to upgrade by clicking and enabling the corresponding checkbox next to the bay number of the blade servers. ***Note***: A maximum of 8 blade servers can be upgraded concurrently at one time. If the c7000 enclosure has more than 8 blade servers, they need to be upgraded in multiple sessions. 

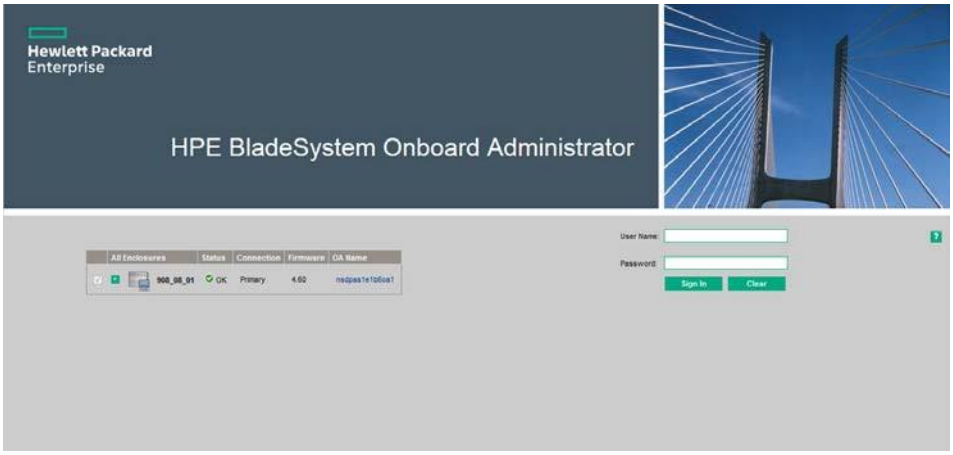
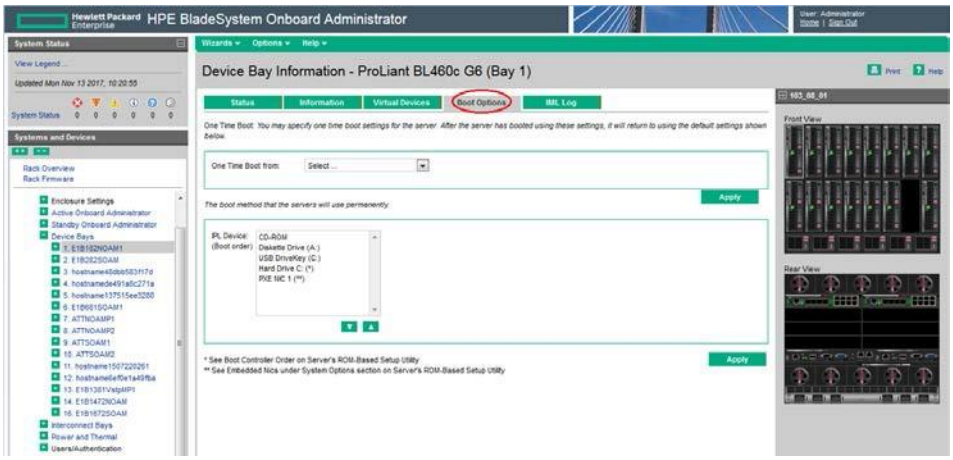
Step #	Procedure	Description
5.	**OA Web GUI**: Connect to USB drive	Connect the selected blade servers to the ISO on the USB Drive by clicking **Connect to USB** from the DVD menu.  The ISO media Device List table changes to indicate an iLO DVD Status as **Connected** for each selected blade.  | Bay	Status	UID	Power State	iLO IP Address	iLO Name	iLO DVD Status
---	---	---	---	---	---	---
1	OK	Blink	On	10.240.17.31	ILOUSE941SWFS	Disconnected
2	OK	Off	On	10.240.17.32	ILOUSE941SWFT	Disconnected
3	OK	Off	On	10.240.17.33	ILOUSE941SWH9	Disconnected
4	OK	Blink	On	10.240.17.34	ILOUSE941SWH3	Disconnected
5	OK	Off	On	10.240.17.35	ILOUSE941SWFJ	Disconnected
6	OK	Off	On	10.240.17.36	ILOUSE941SWHD	Disconnected
7	OK	Off	Off	10.240.17.37	ILOUSE941SWFV	Disconnected
8	OK	Off	On	10.240.17.38	ILOUSE941SWFN	Disconnected
12	OK	Off	On	10.240.17.42	ILOUSE8068S2T	Connected
13	OK	Off	On	10.240.17.43	ILOUSE941SWHB	Connected	 ***Note***: You may need to click **Refresh** to see the changed status of all blade servers.

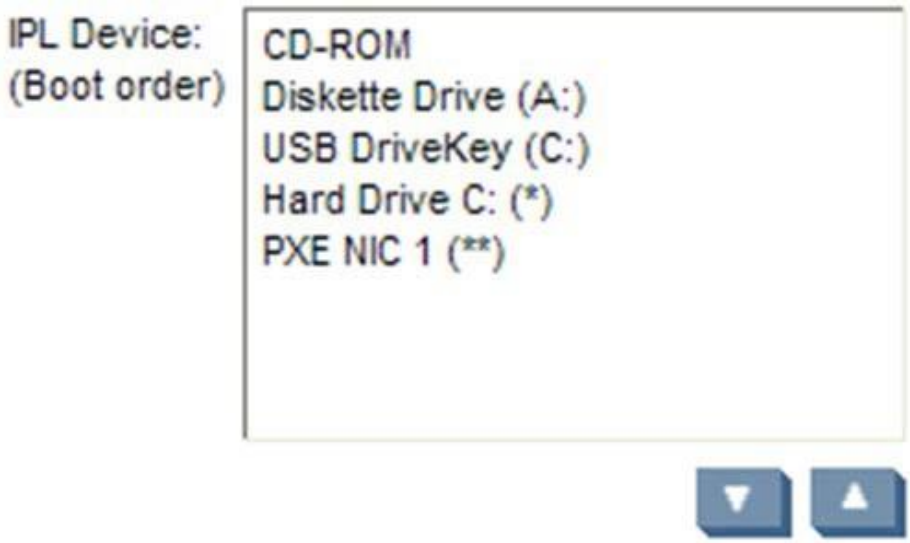
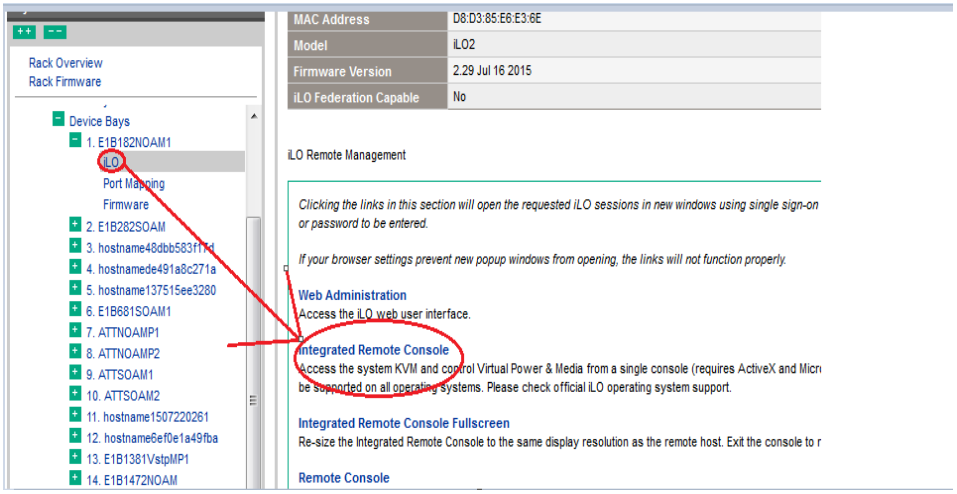
Step #	Procedure	Description
6. ☐	**OA Web GUI**: Power down blade servers	If needed, reselect the **UID** checkbox for each blade to be upgraded and select **Momentary Press** under the Virtual Power menu.  When asked, click **OK** to confirm the action. The power down sequence can take several minutes to complete. When it completes, the Device List table indicates the Power State of each selected blade server as **Off**.  ***Note***: You may need to click **Refresh** to see the changed status of all blade servers.
7. ☐	**OA Web GUI**: Initiate firmware upgrade	To power the blade servers back on and begin the automated firmware upgrade process, repeat step 6. This time being sure the Power State indicates **On** for each selected blade server.

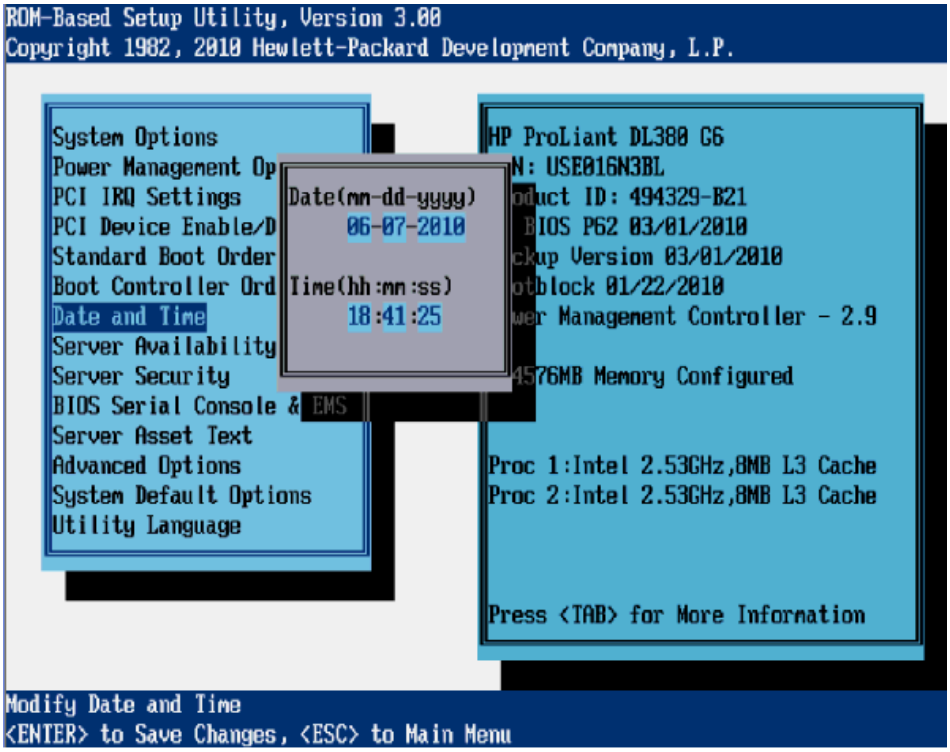
Step #	Procedure	Description
8. ☐	**OA Web GUI**: Monitor firmware upgrade	Each blade server boots into an automated firmware upgrade process that lasts approximately 30 minutes. During this time, all feedback is provided through the UID lights. The UID light on a server blinks when firmware is actively being applied. The UID lights do not blink until the server fully boots and the firmware upgrades have started to be applied. If no upgrades are needed, the UID lights do not blink, but the server still reboots and the iLO DVD is disconnected after completion.  Upon a successful firmware upgrade, the Device List table lists each blade server with a Status of **OK**, UID of **Off**, and the iLO DVD Status as **Disconnected**. At this time, the blade servers automatically reboot. ***Note***: Make sure all blade servers have disconnected before continuing. If any blade servers are still connected after their UIDs have stopped blinking and Status is **OK**, disconnect them manually by selecting **Disconnect Blade** from DVD/ISO from the DVD menu. If the UID light is solid, a failure has occurred during the firmware upgrade. Use the iLO's integrated remote console or a KVM connection to view the error. If necessary, repeat steps 1 through 8 for the remaining blades in the enclosure to be upgraded. Proceed to the next step.
9. ☐	Remove USB flash drive	The USB flash drive may now safely be removed from the active OA module.
10. ☐	Update Firmware Errata	Check the Release Notes of the HP Solutions Firmware Upgrade Pack, version 2.x.x [2] to see if there are any firmware errata items that apply to the server being upgraded. If there are firmware errata items that apply to the server being upgraded, there is a directory matching the errata's ID in the ***/errata*** directory of the HP MISC firmware ISO image. The errata directories contain the errata firmware and a README file detailing the installation steps.

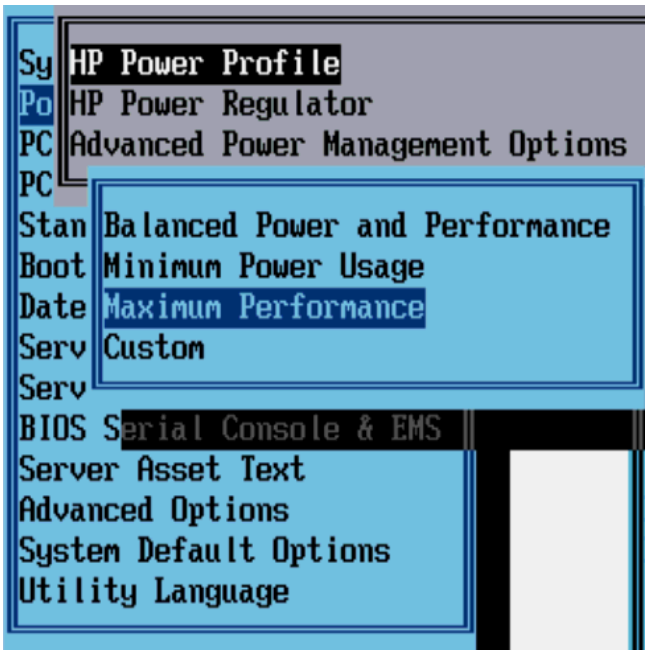
4.8.2 Confirm/Upgrade Blade Server BIOS Settings

Procedure 10. Confirm/Upgrade Blade Server BIOS Settings

Step #	Procedure	Description
This procedure updates the BIOS boot order on blade servers. All servers should have SNMP disabled. Refer to Appendix B. For instructions on BIOS configuration for Gen9 blade or RMS, refer to Procedure 31. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Active OA GUI**: Login	Navigate to the IP address of the active OA, using Appendix I. Login as an administrative user. 
2. ☐	**Active OA GUI**: Navigate to device bay settings	Navigate to **Enclosure Information > Device Bays > <Blade1>**. Click the Boot Options tabs. 

Step #	Procedure	Description
3. ☐	**Active OA GUI**: Verify/Update boot device order	Verify the boot order is as follows. If it is not, use the up and down arros to adjust the order to match the figure. Click **Apply**. 
4. ☐	**OA**: Access the blade iLO	Navigate to **Enclosure Information > Device Bays > <Blade1> > iLO**. Click **Integrated Remote Console**.  This starts the iLO interface for that blade. If this is the first time the iLO is being accessed, you are askeed to install an addon to your web browser. Follow the on screen instructions to do so.
5. ☐	**OA**: Restart the blade server and access the BIOS	Click **Continue** if a certificate security warning displays. Log into the blade server using the **admusr** username. Reboot the server using the **reboot** command and after the server is powered on, as soon as you see **F9=Setup** in the lower left corner of the screen. Press **F9** to access the BIOS setup screen.

Step #	Procedure	Description
6.	**OA**: Update BIOS settings	1. Select **Date and Time** and press **Enter**. 2. Set the current **date** and set the **time** to current UTC time. Press **Enter**.  3. Press **Esc** to go back to the main menu. Select **Power Management Options** and press **Enter**. 4. Select **HP Power Profile** and press **Enter**.

Step #	Procedure	Description
		5. Select **Maximum Performance** and press **Enter**.  6. Press **Esc** twice to return to the BIOS setup screen. Press **F10** to confirm exiting the utility. The blade server reboots.
7. ☐	Select **Server Availability**	1. Change **Automatic Power-On** to **Restore Last Power State**. 2. Change **Power-On Delay** to **No Delay**. 3. Press **ESC** to navigate to the main menu.
8. ☐	Repeat	Repeat procedure for remaining blade serves.

4.9 Install TVOE on Rack Mount Servers

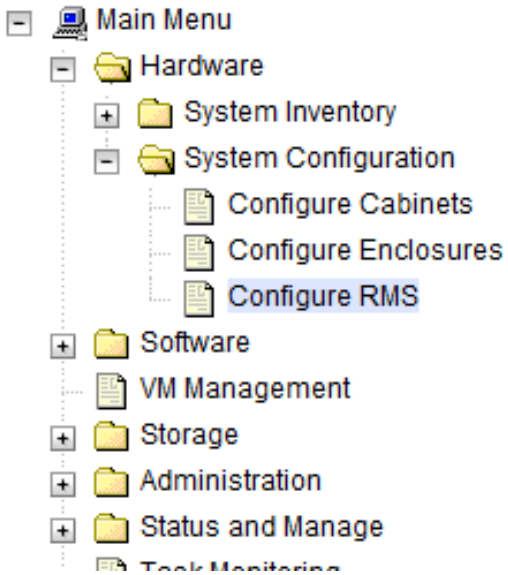
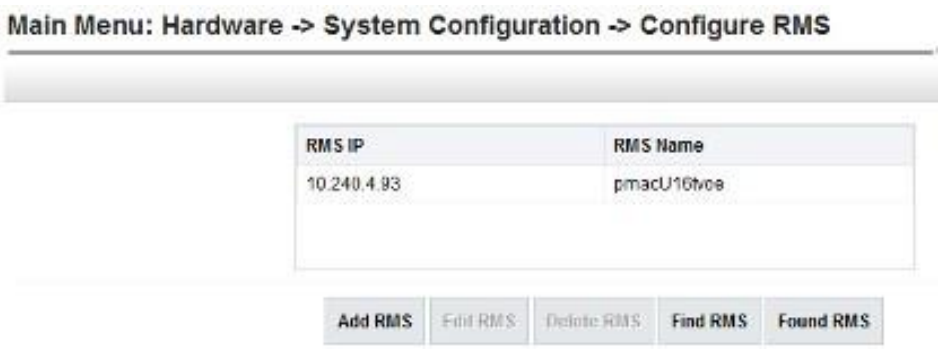
This procedure is specific to RMS servers that are manage by PMAC and do not yet have a TVOE environment configured. It requires the RMS server be on the PMAC control network (that is, it is able to receive a DHCP IP address from PMAC on the 192.168.1.0 network).

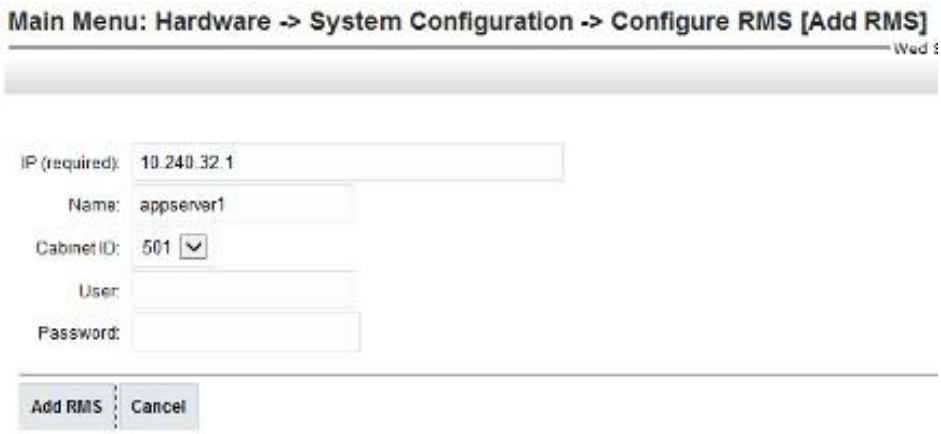
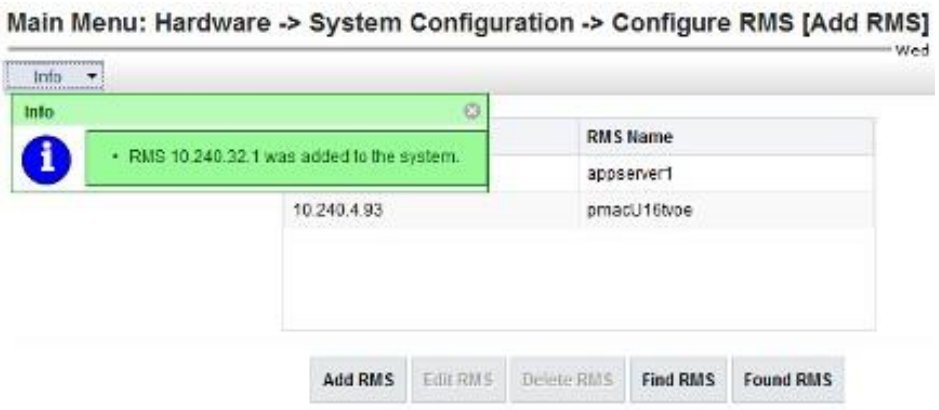
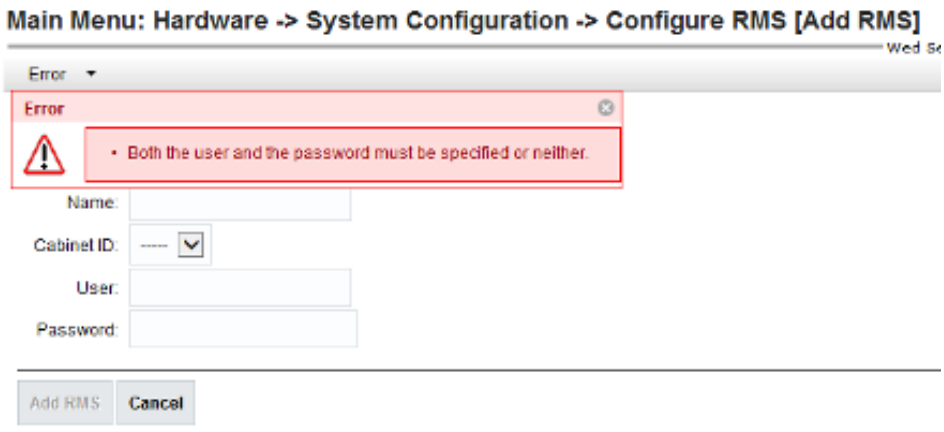
This is an IPM activity for a server that will be a virtual host.

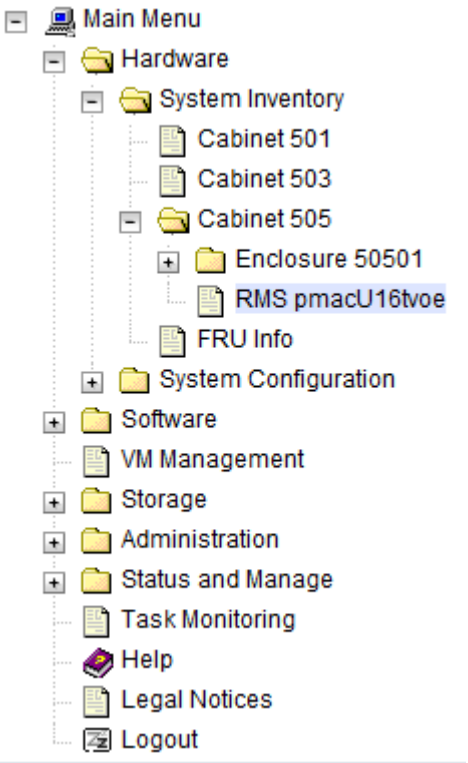
4.9.1 Add Rack Mount Server to PMAC System Inventory

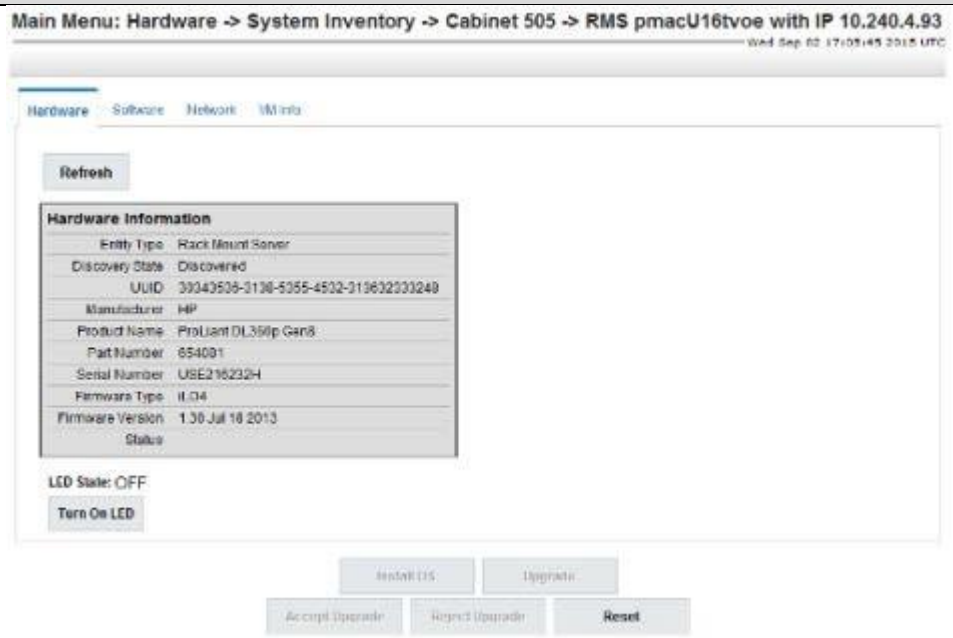
Procedure 10. Add Rack Mount Server to PMAC System Inventory

Step #	Procedure	Description
This procedure adds a rack mount server to the PMAC system inventory. ***Prerequisite***: Complete Procedure 9. ***Note***: You cannot edit the RMS iLO IP address. To change this address, delete and then add the RMS with the correct address. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as pmacadmin user.
2. ☐	**PMAC GUI**: Configure cabinet (optional)	If this is a RMS installation only or a cabinet has not been previously configured, perform steps 2. through 5. of Procedure 17 Add Cabinet and Enclosure to the PMAC System Inventory to add one or more cabinets.

Step #	Procedure	Description
3. ☐	**PMAC GUI**: Configure RMS	Navigate to **Hardware > System Configuration > Configure RMS**. 
4. ☐	**PMAC GUI**: Add RMS	Click **Add RMS**. 

Step #	Procedure	Description
5. ☐	**PMAC GUI**: Enter information	Enter the IP address of the rack mount server management port (iLO). All other fields are optional. Click **Add RMS**.  ***Note***: If the initial credentials provided by Oracle have been changed, enter valid credentials (not to be confused with OS or application credentials) for the rack mount server management port.
6. ☐	**PMAC GUI**: Check for errors	If no error is reported to the user, the following displays:  Or, an error message displays: 

Step #	Procedure	Description
7. ☐	**PMAC GUI**: Verify RMS discovered	Navigate to **Hardware > System Inventory > Cabinet xxx > RMS yyy** where **xxx** is the cabinet ID selected when adding RMS (or unspecified) and **yyy** is the name of the RMS.  Periodically refresh the hardware information using the double arrow to the right of the Hardware Information title until the **Discovery State** changes from **Undiscovered** to **Discovered**. If **Status** displays an error, contact My Oracle Support (MOS) for assistance.

Step #	Procedure	Description
		

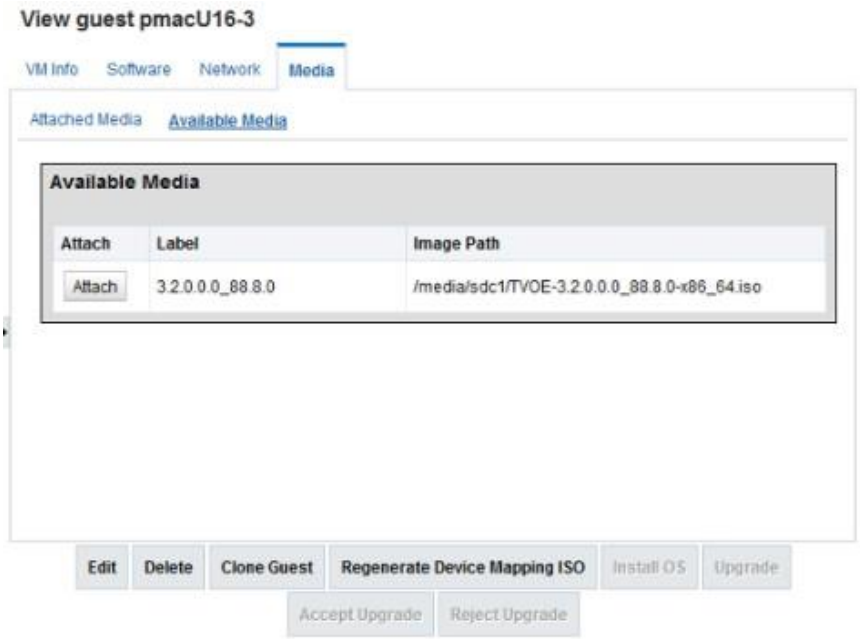
4.9.2 Add ISO Images to the PMAC Image Repository

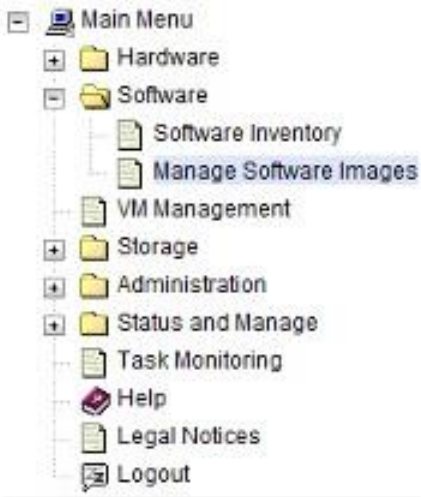
If the Rack Mount Server (RMS) or blade server is to be configured as a TVOE hosting application guest, then execute this procedure using the applicable TVOE ISO as the image to add.

Procedure 11. Add ISO Images to the PMAC Image Repository

Step #	Procedure	Decription
This procedure adds ISO images to the PMAC system inventory. ***Note***: You cannot edit the RMS iLO IP address. To change this address, delete and then add the RMS with the correct address. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		

1. □	Make image available to PMAC	There are two ways to make an image available to PMAC:
		• Attach the USB device containing the ISO image to a USB port of the management server.
		• Use sftp to transfer the iso image to the PMAC server in the /var/TKLC/smac/image/isoimages/home/smacftpusr/ directory as pmacftpusr user:
		  • cd into the directory where your ISO image is located (not on the PMAC server)
		  • Using sftp, connect to the PMAC management server as the pmacftpusr user. If using IPv6, shell escapes around the IPv6 address may be required.
		  `> sftp pmacftpusr@<pmac_management_network_ip>`
		  `> put <image>.iso`
		  • After the image transfer is 100% complete, close the connection
		  `> quit`
		Refer to the documentation provided by application for the pmacftpusr password.

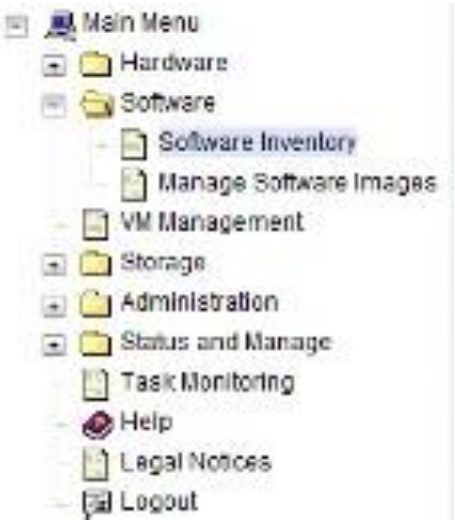
Step #	Procedure	Decription
2. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as pmacadmin user.
3. ☐	**PMAC GUI**: Attach software image to the PMAC guest	If in step 1. the ISO image was transferred directly to the PMAC guest using sftp, skip the rest of this step and continue with step 4. If the image is on a USB device, continue with this step. In the PMAC GUI, navigate to **VM Management**. In the VM Entities list, select the PMAC guest. On the resulting View VM Guest screen, select the Media tab. Under the Media tab, find the ISO image in the Available Media list, and click its **Attach** button. After a pause, the image displays in the Attached Media list. 

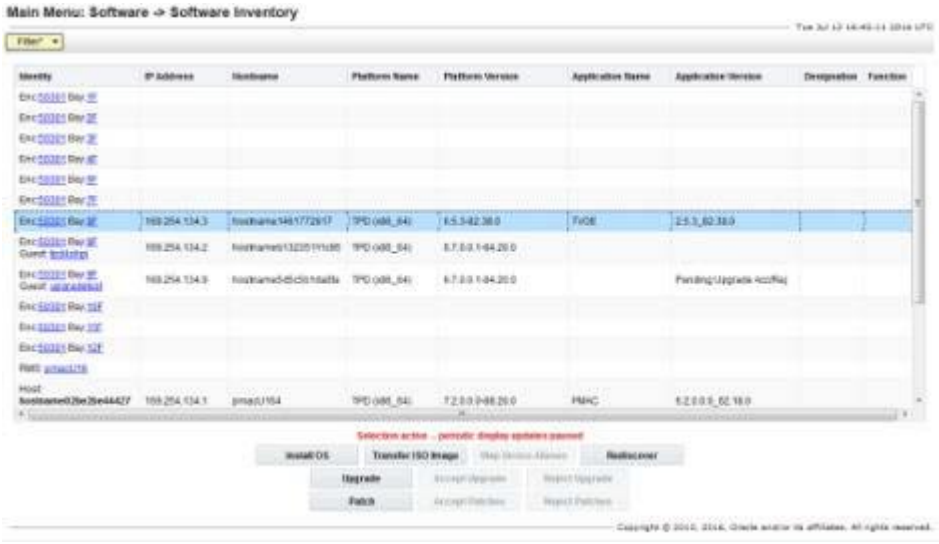
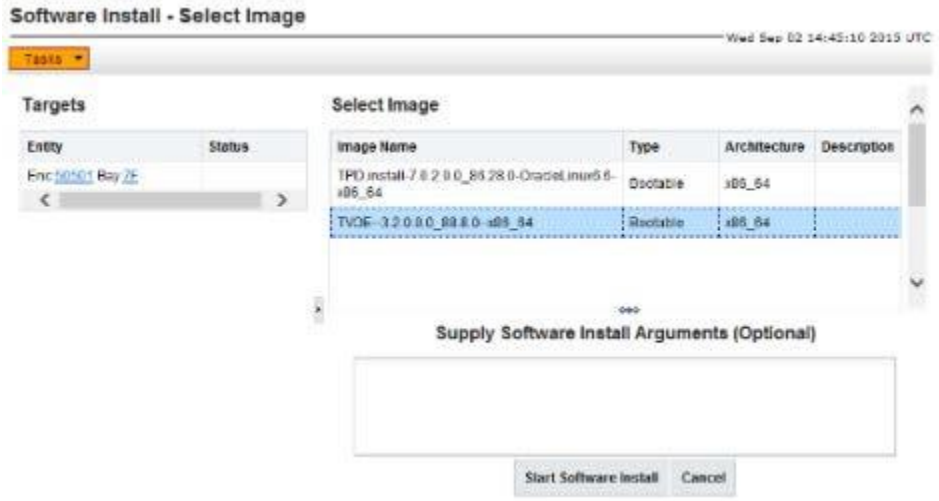
Step #	Procedure	Decription
4. ☐	**PMAC GUI**: Manage software image	Navigate to **Software** > **Manage Software Images**. 
5. ☐	**PMAC GUI**: Add image	Click **Add Image**.
6. ☐	**PMAC GUI**: Select image	Select an image to add: • If in step 1. the image was transferred to PMAC using sftp, it displays in the list as a /var/TKLC/... local file. • If the image was supplied on a USB drive, it displays as a virtual device (device://…). These devices are assigned in numerical order as USB images become available on the management server. The first virtual device is reserved for internal use by TVOE and PMAC; therefore, the iso image of interest is normally present on the second device, device://dev/sr1. If one or more USB-based images is already present on the management server before you started this procedure, select a correspondingly higher device number. Enter an image description and click **Add New Image**.

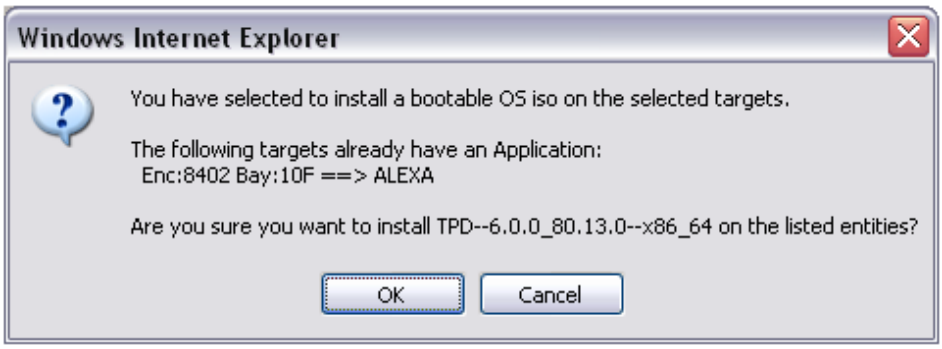
Step #	Procedure	Decription
		 The screen displays with a new background task entry in the table. When the task completes, the text changes to green and its Progress column indicates 100%. Make sure the correct image name displays in the Status column.
7. ☐	**PMAC GUI**: Detach the image from the PMAC guest	If the image was supplied on USB, return to the PMAC guest's Media tab used in step 3. , locate the image in the Attached Media list, and click its **Detach** button. After a pause, the image is removed from the Attached Media list. This releases the virtual device for future use. Remove the USB device from the management server. ***Note***: If there are additional ISO images to be provisioned on the PMAC, repeat the procedure with the appropriate ISO image data.

4.9.3 IPM Servers Using PMAC Application

Procedure 18. IPM Servers Using PMAC Application

Step #	Procedure	Description
This procedure installs TPD or TVOE using an image from the PMAC image repository. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as pmacadmin user.
2. ☐	**PMAC GUI**: Manage software inventory	Navigate to **Software** > **Software Inventory**. 

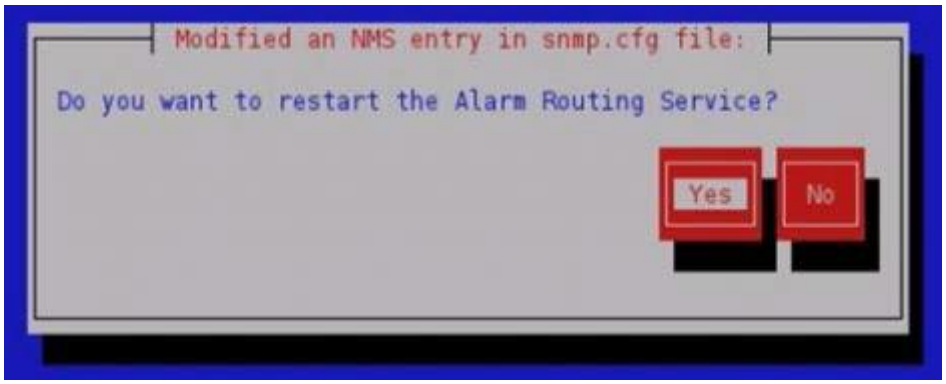
Step #	Procedure	Description
3. ☐	**PMAC GUI**: Select servers	Select the servers you want to IPM. If you want to install the same OS on more than one server, you may select multiple servers by selecting multiple rows. Selected rows are highlighted in green.  Click **Install OS**.
4. ☐	**PMAC GUI**: Select image	The left side of the screen displays the servers to be affected by the OS installation. From the list of available bootable images on the right side of the screen, select the OS image to install on the selected servers. 
5. ☐	**PMAC GUI**: Supply install arguments (optional)	Enter Installation arguments by entering them into the textbox displayed under the list of bootable images. These arguments are appended to the kernel line during the IPM process. If no install arguments are needed for the OS, leave the install arguments textbox empty. ***Note***: The valid arguments for a TPD IPM are listed in *TPD Initial Product Manufacture Software Installation Procedure*.

Step #	Procedure	Description
6. ☐	**PMAC GUI**: Start installation	Click **Start Install**.
7. ☐	**PMAC GUI**: Confirm OS installation	Click **OK** to proceed with the installation. 
8. ☐	**PMAC GUI**: Monitor install OS	Navigate to **Task Monitoring** to monitor the progress of the Install OS background task. A separate task displays for each server affected. When the task completes, the text changes to green and its Progress column indicates 100%. Make sure the correct image name displays in the Status column. Repeat this procedure for additional RMSs with appropriate data.

4.9.4 Add SNMP Trap Destination on TPD-Based Application

Procedure 18. Add SNMP Trap Destination on TPD-Based Application

Step #	Procedure
This procedure configures an SNMP trap destination to a server running on TVOE, based on TPD. All alarm information is sent to the NMS located at the destination. ***Note***: Refer to section 3.3 SNMP Configuration. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Login as platcfg user on the server.

Step #	Procedure
2. ☐	Navigate to **Network Configuration > SNMP Configuration >NMS Configuration**.
3. ☐	Click **Edit**.
4. ☐	Click **Add a New NMS Server** and enter data about the SNMP trap destination. Click **OK**. Refer to section 3.3 SNMP Configuration for SNMP trap destination recommendations.
5. ☐	Click **Exit** and then **Yes** to restart the Alarm Routing Service.  Exit platcfg by clicking **Exit** on each menu until platcfg has been exited.

4.10 Install TVOE on Blade Servers

Install the TVOE hypervisor platform on blade servers. Perform section 4.9.2 To add the TVOE ISO image to the PMAC Image Repository and then section 4.9.3 IPM Servers Using PMAC Application to install TVOE on a blade server.

Appendix A. Initial Product Manufacture of RMS and Blade Server

Appendix A.1 Set Server's CMOS Clock

The date and time in the server's CMOS clock must be set accurately before running the IPM procedure. There are a number of different ways to set the server's CMOS clock.

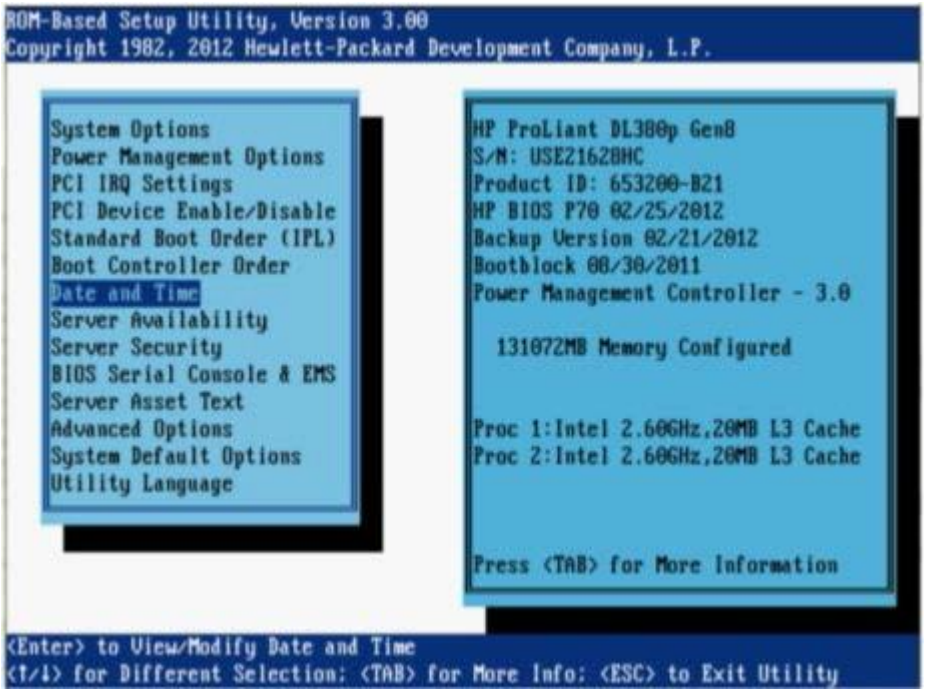
Note: The IPM installation process managed by PMAC for blade servers automatically sets the server's CMOS clock, so there is no need to set the server CMOS clock when using PMAC.

Appendix A.2 Configure BIOS Settings

Follow these steps to configure HP DL380 server BIOS settings for supported models of Gen8 and Gen9 servers.

Procedure 10. Configure HP DL380 RMS Server BIOS Settings

Step #	Procedure	Description
This procedure configures HP CL380 server BIOS settings for supported models of Gen8 and Gen8 servers. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		

Step #	Procedure	Description
1.	Access BIOS setting	Reboot the server and after the server is powered on, press **F9** when asked to access the ROM-Based Setup Utility.  **Figure 3. HP CIOS Setup**
2.	Select **Date and Time**	1. Set the server date and time to **UTC** (Coordinated Universal Time). 2. Press **ESC** to navigate to the main menu.
3.	Select **Server Availability**	3. Change **Automatic Power-On** to **Restore Last Power State**. 4. Change **Power-On Delay** to **No Delay**. 5. Press **ESC** to navigate to the main menu.
4.	Select **System Options**	1. Select **Processor Options**. 2. Change **Intel Virtualization Technology** to **Enabled**. 3. Press **ESC** to return to System Options. 4. Select **Serial Port Options**. 5. Change **Embedded Serial Port** to **COM2**. 6. Change **Virtual Serial Port** to **COM1**. 7. Press **ESC** to navigate to the main menu.
5.	Save and Exit	Press **F10** to save and exit from the ROM-Based Setup Utility.

Procedure 10. Configure HP Gen9 RMS and Blade Server BIOS Settings

Step #	Procedure
The HP Gen9 systems can have UEFI boot enabled. Since TPD is configured to use the Legacy BIOS option, both blade and rack mount Gen9 servers should have their BIOS settings checked before IPM. Rack mount servers should also have the iLO serial port configured at this time. Directions for both settings are provided in this procedure. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	If this is a rack mount server, connect via a VGA monitor and USB keyboard. If a blade server is being configured, use the iLO Integrated Remote Console.
2. ☐	Reboot/reset the server.
3. ☐	Press **F9** to access the **System Utilities** menu when **<F9 System Utilities>** displays in the lower left corner of the screen.
4. ☐	Select the **System Configuration** menu.
5. ☐	Select the **BIOS/Platform Configuration (RBSU)** menu.
6. ☐	Select the **Boot Options** menu.
7. ☐	If the Boot Mode is not **Legacy BIOS** mode, press **Enter** to open the **BIOS** mode menu; otherwise, skip to step 9.
8. ☐	Select **Legacy BIOS Mode**.
9. ☐	Press **Esc** once to back out to the **BIOS/Platform Configuration (RBSU)** menu. If a blade server is being configured, skip to step 17. ; otherwise, continue with next step.
10. ☐	Select the **System Options** menu and select the **Serial Port Options** menu.
11. ☐	Change **Embedded Serial Port** to **COM2**.
12. ☐	Change **Virtual Serial Port** to **COM1**.
13. ☐	Press <Esc> twice to back out to the **BIOS/Platform Configuration (RBSU)** menu.
14. ☐	Select the **Server Availability** menu.

Step #	Procedure
15. ☐	Set **Automatic Power-On** to **Restore Last Power State**.
16. ☐	Set **Power-On Delay** to **No Delay** and press **Esc** once to back out to the **BIOS/Platform Configuration (RBSU)** menu.
17. ☐	Select the **Power Management** menu.
18. ☐	Set **HP Power Profile** to **Maximum Performance**. Press **Esc** once to back out to the **BIOS/Platform Configuration (RBSU)** menu.
19. ☐	Press **F10** to save the updated settings, then **y** to confirm the settings change.
20. ☐	Press **Esc** twice to back out to the **System Utilities** menu.
21. ☐	Select **Reboot the System** and press **Enter** to confirm.

Appendix A.3 OS IPM Installation for HP Rack Mount Servers

Insert the IPM installation media into the system. Installation begins by resetting (or power cycling) the system so the BIOS can find and boot from the IPM installation media. The reboot steps are different for the different rack mount servers.

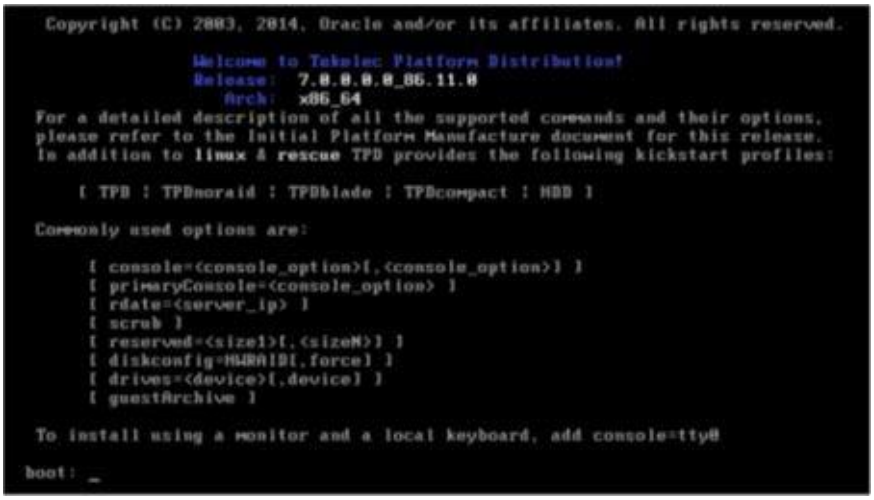
Note: You can either configure an IP address on the iLO/ILOM and access the console using the iLO/ILOM, or use the VGA monitor and keyboard. You can also use the remote media function of the iLO/ILOM to access to the installation media.

Procedure 10. Install OS IPM for HP Rack Mount Servers

Step #	Procedure	Description
This procedure prepares the server for IPM procedures. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Insert media	Insert the OS IPM media (CD/DVD or USB) into the CD/DVD tray/USB slot of the application server.
2. ☐	Power cycle the server	Press and hold the power button until the button turns amber, then release. Wait 5 seconds and press the power button. Release it again to power on the system.
3. ☐	Select boot method	For some servers, you must select a boot method so that the server does not boot directly to the hard drive. Press **F11** when asked to bring up the boot menu and select the appropriate boot method.

Appendix A.4 IPM Command Line Procedures

Procedure 10. Install OS IPM for HP Rack Mount Servers

Step #	Procedure	Description
This procedure installs the OS IPM. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Perform media check (optional)	If media has not been previously verified, perform a media check now. Refer to Appendix A.6.
2. ☐	Enter TPD command	Figure 4 shows a sample output screen indicating the initial boot from the install media was successful. The information in this screen output is representative of TPD 7.0.0.0.0.  **Figure 4. Boot from Media Screen, TPD 7.0.0.0.0** ***Note***: Based on the deployment type, either TPD or TVOE can be installed. The command to start the installation is dependent upon several factors, including the type of system, knowledge of whether an application has previously been installed or a prior IPM install failed, and what application will be installed. ***Note***: Text case is important and the command must be typed exactly. IPM the server by entering the TPD command at the boot prompt. An example command to enter is: `TPDnoraid console=tty0 diskconfig=HWRAID,force` After entering the command to start the installation, the Linux kernel loads as shown in Figure 5.

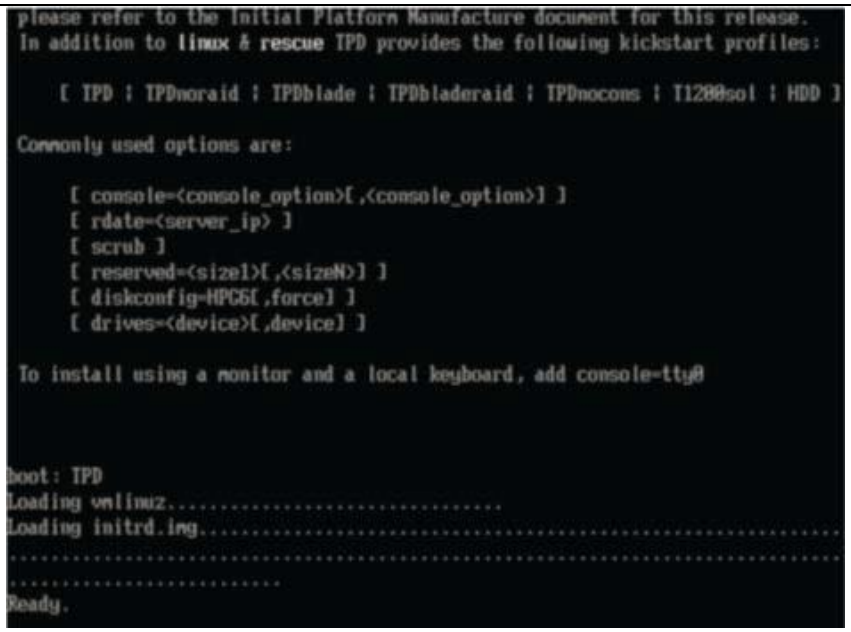


Figure 5. Kernel Loading Output

After a few seconds, additional messages begin scrolling by on the screen as the Linux kernel boots, and then the drive formatting and file system creation steps begin:

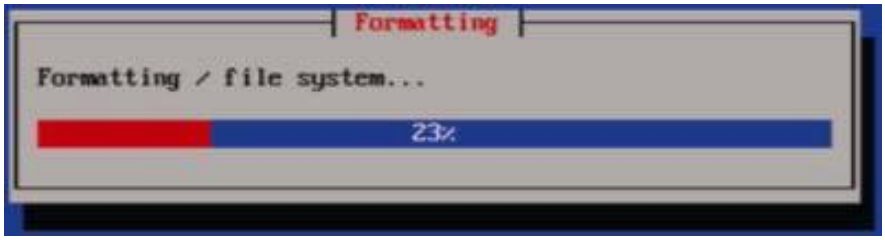


Figure 6. File System Creation Screen

Once the drive formatting and file system creation steps are complete, a screen similar to Figure 7 displays indicating the package installation step is about to begin.

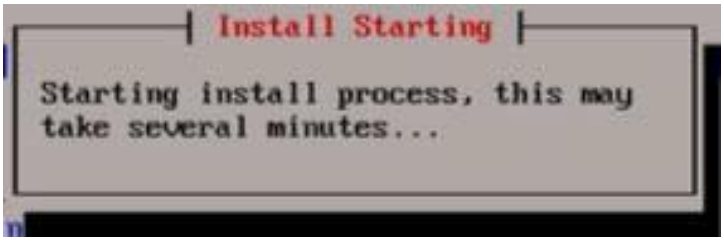
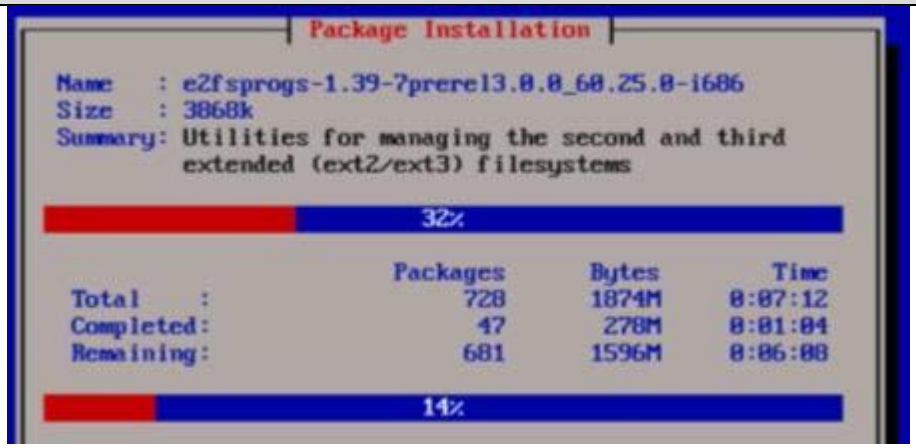
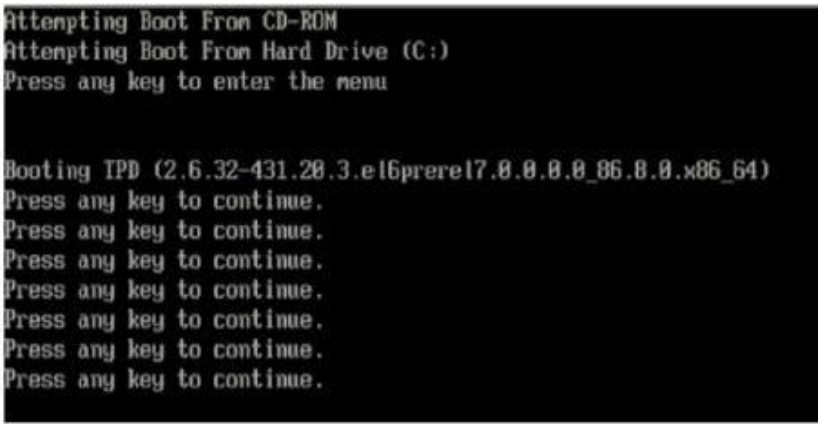


Figure 7. Package Installation Screen

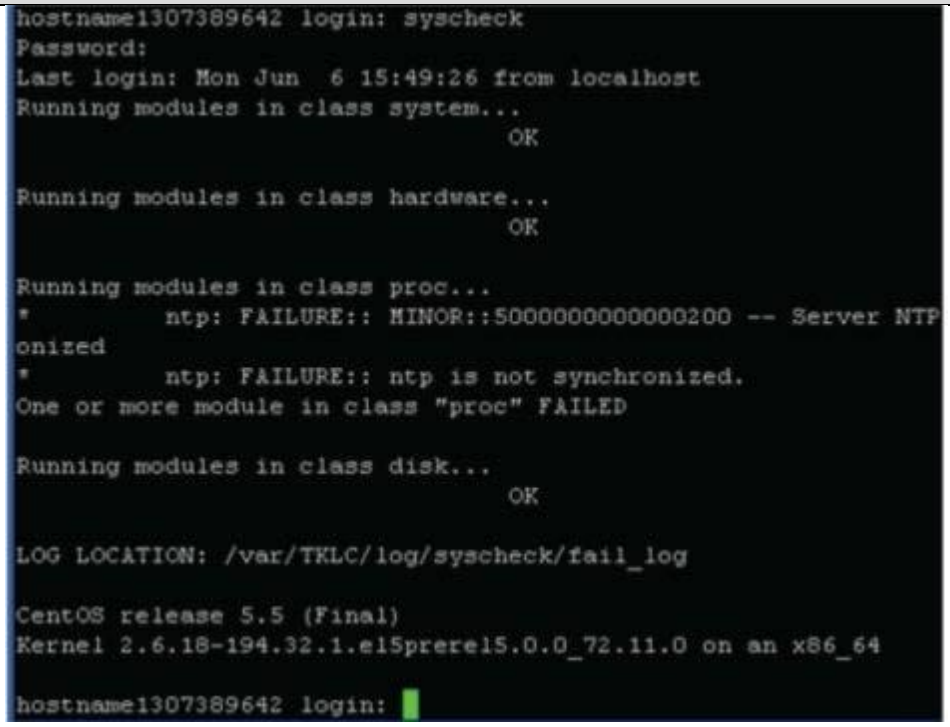
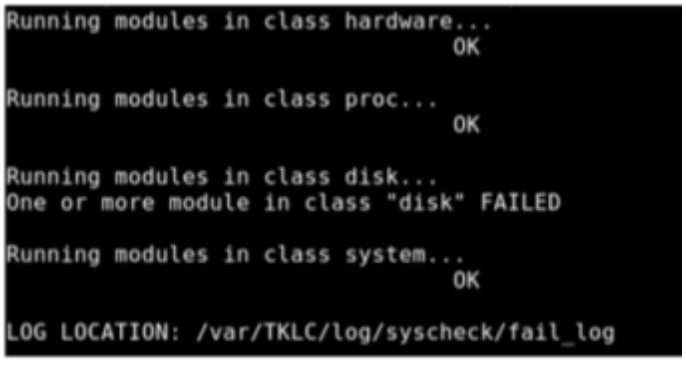
Once Figure 7 displays, it may take several minutes before anything changes. After a few minutes, a screen similar to Figure 8 displays showing the status of the package installation step. For each package, there is a status bar at the top indicating how much of the package has been installed, with a cumulative status bar at the bottom indicating how many packages remain. In the middle, you the text statistics indicate the total number of packages, the number of packages installed, the number remaining, and current and projected time estimates.

Step #	Procedure	Description
		 **Figure 8. Installation Statistics Screen**
3.	Reboot the system	Once all the packages have been successfully installed, a screen similar to Figure 9 displays, letting you know the installation process is complete. Remove the installation media (DVD or USB key) and press **Enter** to reboot the system. ***Note***: It is possible the system will reboot several times during the IPM process. No user input is required if this occurs. **Figure 9. Installation Complete Screen** After a few minutes, the server boot sequence starts and eventually displays that it is booting the new IPM load.  **Figure 10. Boot Loader Output** A successful IPM platform installation process results in a user login prompt.

Appendix A.5 Post Installation Processing

Procedure 10. Post Installation Health Check

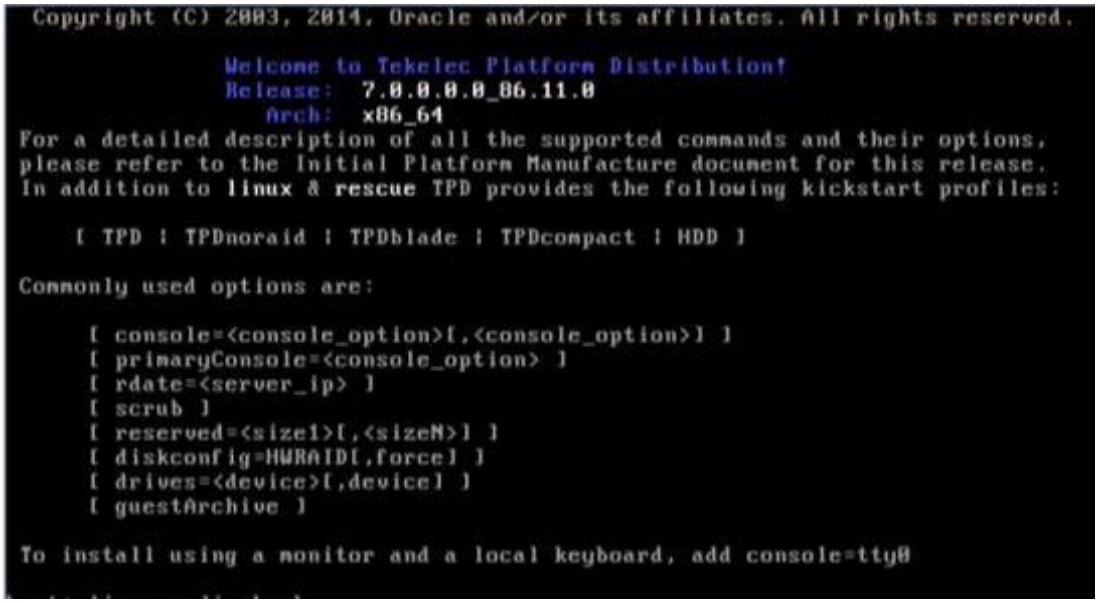
Step #	Procedure	Description
This procedure runs a system health check after installing the OS. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Login	Login as **syscheck** user and the system health check runs automatically. This checks the health of the server and prints an **OK** if the tests passed, or, a descriptive error of the problem if anything failed. The Figure 11 shows a successful run of syscheck where all tests pass indicating the server is healthy. **Figure 11. Successful Syscheck Output** Since an NTP server is not normally configured at this point, syscheck may fail due to the NTP test as shown in Figure 12. The error is acceptable and can be ignored.

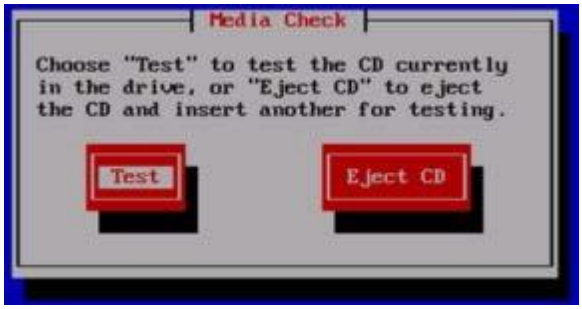
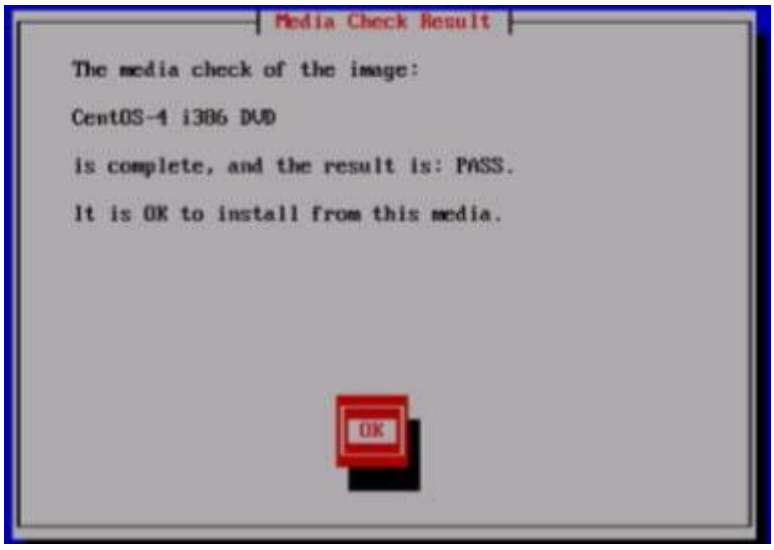
Step #	Procedure	Description
		 **Figure 12. Syscheck Output with NTP Error** Figure 13 indicates a disk failure in one of the syscheck tests. If the server is using software disk mirroring (RAID1), the syscheck disk test fails until the disks have synchronized. The amount of time required to synchronize the disks varies with disk speed and capacity. Continue executing the system check every 5 minutes (by logging in as syscheck to run syscheck again) until the health check executes successfully as shown in Figure 11. If the disk failure persists for more than two (2) hours, or if system check returns any other error message besides a disk failure or the NTP error shown in Figure 12, do not continue. Contact My Oracle Support (MOS) and report the error condition.  **Figure 13. Syscheck Disk Failure Output**
2.	Verify IPM	Verify that the IPM completed successfully by logging in as admusr and running the **verifyIPM** command. No output is expected. Contact My Oracle Support (MOS) if any output is printed by the **verifyIPM** command. `$ sudo /usr/TKLC/plat/bin/verifyIPM`

Appendix A.6 Media Check

Media check only works on CDs/DVDs. Validate USB media when it is created since the validation steps depend on how it was created.

Procedure 10. Post Installation Health Check

Step #	Procedure
This procedure verifies and validates media. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.	
1. ☐	Refer to Appendix A.3 to automatically boot from the DVD or USB IPM media.
2. ☐	The screen output shown in Figure 14 indicates the initial boot from DVD is successful. Enter the command linux mediacheck and press **Enter**.  **Figure 14. Media Check Command**

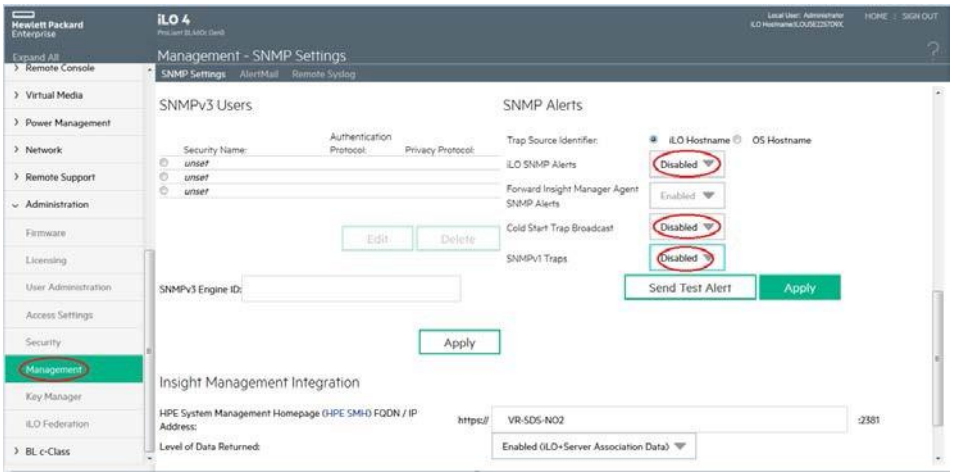
Step #	Procedure
3.	Select **OK**. **Figure 15. Media Test Screen**
4.	Select **Test** to begin testing the currently installed media.  **Figure 16. Media Check**
5.	If the media check is successful, Figure 17 displays. Select **OK**.  **Figure 17. Media Check Result**

Step #	Procedure
6.	To test additional media, remove original media, insert new media, select **Test**. If no additional media needs to be checked and the media check passed, remove the current media, insert the original media (first disk or USB pen), and select **Continue** to continue with the installation. **Figure 18. Media Check Continuation**

Appendix B. Change SNMP Configuration Settings for iLO

Perform this procedure for every iLO4 device on the network. For instance, for every HP ProLiant Blade and rack mount server.

Procedure 10. Access a Remote Server Console

Step #	Procedure	Description
This procedure changes the default SNMP settings for the HP ProLiant iLO device. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Workstation**: Open browser and login	Open a browser and connect to the iLO 4 device using **https://**. Log into the GUI using an Administrator account name and password.
2. ☐	**iLO 4 Web UI**: Disable SNMP alerts	1. Navigate to **Administration > Management**. 2. Select **Disabled** for each SNMP alert and click **Apply**.  3. Verify the setting changes by navigating away from the Management screen and returning to it to verify the SNMP settings are the same. 4. Repeat this procedure for all remaining iLO 4 devices on the network.

Appendix C. Access a Server Console Remotely Using iLO

Procedure 10. Access a Remote Server Console Using iLO

Step #	Procedure	Description
This procedure accesses a server console remotely. ***Needed Material***: <iLO_admin_user> is the privileged username for HP iLO access. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Access the iLO/ILOM GUI	Using a laptop or desktop computer connected to the customer network, navigate with Internet Explorer to the IP address of the iLO/ILOM of the Management Server. Click **Continue to this website (not recommended)** if prompted. Log into the iLO as the <iLO_admin_user>.
2. ☐	Open the remote console window	Click the Remote Console tab and select **Remote Console** to open the remote console in a new window. If prompted, click **Continue** on the Security Warning screen.

3.
☐
	Log into the console	In the Remote Console window, log into the console as the **admusr**.
		`Login as: admusr`
		`Password:`
		`Last login: Fri Oct 6 17:52:28 2017`
		`[admusr@tvo ~]$`

Appendix D. Install NetBackup Client on TVOE Server (Optional)

This optional procedure includes all information necessary to install the NetBackup software on the TVOE host. This must be done after the Aggregate Switches are properly configured. This procedure assumes all necessary NetBackup network configuration has been completed from 4.1 Configure and IPM the Management Server.

Note: Once the NetBackup Client is installed on TVOE, the NetBackup Master should be configured to back up the following files from the TVOE host:

```
/var/TKLC/bkp/*.iso
```

Procedure 18. Set Up and Install NetBackup Client

Step #	Procedure	Description
If NetBackup is configured on this system, this procedure sets up and installs the NetBackup Client on a TVOE host. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**TVOE Server**: Login	Login as the **admusr** user.

2.
☐
	TVOE Server: Open firewall ports	Open firewall ports for NetBackup using the following commands:
		`$ sudo ln -s /usr/TKLC/plat/share/netbackup/60netbackup.ipt /usr/TKLC/plat/etc/iptables`
		`$ sudo /usr/TKLC/plat/bin/iptablesAdm reconfig`

3.
☐
	TVOE Server: Enable platcfg	Enable platcfg to show the NetBackup Menu Items by executing the following commands:
		`$ sudo platcfgadm --show NBConfig`
		`$ sudo platcfgadm --show NBInit`
		`$ sudo platcfgadm --show NBDeInit`
		`$ sudo platcfgadm --show NBInstall`
		`$ sudo platcfgadm --show NBVerifyEnv`
		`$ sudo platcfgadm --show NBVerify`

Step #	Procedure	Description

4. ☐	**Server**: Create LV and filesystem	Use the vgguests volume group to create an LV and filesystem for the NetBackup client software.
		1. Create a storageMgr configuration file that defines the LV to be created.
		`$ sudo echo "lv --mountpoint=/usr/openv --size=2G --name=netbackup_lv --vg=$VG`
		`> /tmp/nb.lvm`
		This example uses the $VG as the volume group. Replace $VG with the desired volume group as specified by the application group.
		2. c) Server: Create the LV and filesystem by using storageMgr.
		`$ sudo /usr/TKlC/plat/sbin/storageMgr /tmp/nb.lvm`
		This creates the LV, formats it with a filesystem, and mounts it under **/usr/openv/**.
		Example output:
		`Called with options: /tmp/nb.lvm`
		`VG vgguests already exists.`
		`Creating lv netbackup lv.`
		`Volume netbackup_lv will be created.`
		`Success: Volume netbackup_lv was created.`
		`Creating filesystem, this may take a while.`
		`Updating fstab for lv netbackup_lv.`
		`Configuring existing lv netbackup_lv.`

5. ☐	**Application Server**: Install/Upgrade NetBackup	Perform Appendix J.1 Application NetBackup Client Install/Upgrade Procedures.

Appendix E. Uninstall NetBackup Client on TVOE Server (Optional)

In this procedure, target server refers to the TPD or TVOE server where the NetBackup client is installed. In the case of TPD, this is the application server. In the case of TVOE, this is the base server hosting the application virtual machines.

Prerequisites:

- The TPD NetBackup RPM is installed on the server.
- The contents of the NetBackup client configuration file are known if one exists. Depending on the version of NetBackup, a configuration file may not exist.
- The firewall rules implementation is known. Depending on the application, the implementation of firewall rules vary. Do not proceed without understanding the appropriate steps to remove the rules for your application. Reference the documentation for your specific application. The steps presented in this procedure are for a TVOE server and may not apply to a TPD application server.
- The server health checks return no issues.

Procedure 18. Uninstall Symantec NetBackup Client

Step #	Procedure	Description
This procedure uninstalls a successfully installed Symantec NetBackup client from a server with an OS based on TPD or TVOE. ***Note***: If you are attempting to uninstall a failed Symantec NetBackup client installation or upgrade, do not use this procedure. This procedure should only be used when the initial Symantec NetBackup client installation, or subsequent upgrade, is successful. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Back up application	Back up your application as described in your application documentation. Take care not to use NetBackup since the NetBackup client is being removed from the server.

2. ☐	**Target Server**: Login	SSH into the server and login as **admusr**.
		`login as: admusr`
		`Password: <admusr_password>`
		`Last login: Fri Aug 28 12:09:06 2015 from 10.75.8.61`
		`[admusr@<target_server> ~]$`

3. ☐	**Target Server**: Determine the NetBackup client version	Determine the NetBackup client version by inspecting the version file:
		`[admusr@<target_server> ~]$ sudo /bin/cat /usr/openv/netbackup/bin/version`
		`NetBackup-RedHat2.6.18 7.6.0.1`
		`[admusr@<target_server> ~]$`

<table>
<tr><th>Step #</th><th>Procedure</th><th>Description</th></tr>
<tr><td>4.
</td><td>Target Server: Determine packages installed and services configured</td><td>
Determine the NetBackup client packages installed and services configured on the server by inspecting the client profile configuration file. For some versions of NetBackup, a configuration file is not used and does not exist. If your installation does not use a client profile file, refer to Table 5 for your specific release.

Table 5. Installed Packages and Services for NetBackup Client 7.0, 7.1, 7.5, and 7.7
<table>
<tr><th>NetBackup Client Version</th><th>Packages (RPMs)</th><th>Services</th></tr>
<tr><td>NB 7.0</td><td>VRTS pbx</td><td>RC: netbackup</td></tr>
<tr><td>NB 7.1</td><td>SYMCpdddea
SYMCnbjre
SYMCnbjava
SYMCnbclt
VRTS pbx</td><td>RC: netbackup</td></tr>
<tr><td>NB 7.5 and NB 7.7</td><td>SYMCpdddea
SYMCnbjre
SYMCnbjava
SYMCnbclt
VRTS pbx</td><td>RC: netbackup
RC: vxpbx_exchanged</td></tr>
</table>
Note: The client profile configuration file includes the client version in the name. For example, NB7601.conf where 7601 represents the client version number with the periods removed. In this example, version 7.6.0.1 is used.

Inspect the client profile configuration file.
<pre>[admusr@<target_server> ~]$ sudo /bin/cat /usr/TKLC/plat/etc/netbackup/profiles/NB7601.conf
VERSION=7.6.0.1
RPMS="SYMCpddea,SYMCnbjre,SYMCnbjava,SYMCnbclt,VRTSpbx"
RC_SERVICES="netbackup,vxpbx_exchanged"</pre>
</td></tr>
<tr><td>5.
</td><td>Target Server: Stop all NetBackup processes</td><td>
Stop the Symantec NetBackup client services identified in step 4. This example stops the services for NetBackup version 7.6.0.1.
<pre>[admusr@<target_server> ~]$ sudo service netbackup stop
stopping the NetBackup Deduplication Multi-Threaded Agent
stopping the NetBackup Discovery Framework
stopping the NetBackup client daemon
stopping the NetBackup network daemon
[admusr@<target_server> ~]$ sudo service vxpbx_exchanged stop
Stopped Symantec Private Brach Exchange</pre>
</td></tr>
</table>

Step #	Procedure	Description
6. ☐	**Target Server**: Verify the processes stopped	Verify all NetBackup processes are stopped. No output is expected. `[admusr@<target_server> ~]$ sudo /usr/openv/netbackup/bin/bpps`
7. ☐	**Target Server**: Ensure directory is not already in use	Ensure the directory to which the NetBackup LV is mounted is not already in use. This is a precautionary step. `[admusr@<target_server> ~]$ cd ~`

8. ☐	**Target Server**: Delete services	Delete the NetBackup services identified in the client profile from step 4. In this example, the NetBackup client services are netbackup and vxpbx_exchanged.
		`[admusr@<target_server> ~]$ sudo /usr/TKLC/plat/bin/service_conf del netbackup`
		`[admusr@<target_server> ~]$ sudo /usr/TKLC/plat/bin/service_conf del vxpbx_exchanged`

9. ☐	**Target Server**: Reconfigure services	Reconfigure the server services after the deletion: `[admusr@<target_server> ~]$ sudo /usr/TKLC/plat/bin/service_conf reconfig`

10. ☐	**Target Server**: xxx	Uninstall the NetBackup client packages identified in the client profile from step 4. In this example, the NetBackup client packages are SYMCnbclt, SYMCnbjava, SYMCnbjre, SYMCpddea, and VRTSpbx.
		Note: Warnings can be ignored.
		`[admusr@<target_server> ~]$ sudo rpm -ev SYMCnbclt SYMCnbjava SYMCnbjre SYMCpddea VRTSpbx`
		`warning: erase unlink of /opt/VRTSpbx/lib/libvxicui18n.so.6 failed: No such file or directory`
		`warning: erase unlink of /opt/VRTSpbx/bin/vxpbxcfg failed: No such file or directory`
		`Starting SYMCpddea postremove script.`
		`Removing link /opt/pdag`
		`Removing link /opt/pdshared`
		`Removing /opt/pdde directory.`
		`Removing link /usr/openv/lib/ost-plugins/libstspipd.so`
		`Removing link /usr/openv/lib/ost-plugins/libstspipdMT.so`
		`Removing PDDE installation directory.`
		`SYMCpddea postremove script done!`

11. ☐	**Target Server**: Verify removal of client RPMs	Verify the removal of the NetBackup client RPMs. In this example the NetBackup client RPMs are: SYMCnbclt, SYMCnbjava, SYMCnbjre, SYMCpddea, and VRTSpbx. No output is expected. `[admusr@<target_server> ~]$ sudo rpm -qa | egrep "SYMCnbclt|SYMCnbjava|SYMCnbjre|SYMCpddea|VRTSpbx"`

Step #	Procedure	Description

12. ☐	**Target Server**: Clean up directory	Clean up the **/etc/rc.d/init.d** directory.
		List any NetBackup client service files that may not have been removed by the uninstall of the client RPMs. In this example, the client services are netbackup and vxpbx_exchanged.
		`[admusr@<target_server> ~]$ sudo ls -l /etc/rc.d/init.d/netbackup /etc/rc.d/init.d/vxpbx_exchanged`
		`ls: cannot access /etc/rc.d/init.d/vxpbx_exchanged: No such file or directory`
		`-r-x------ 1 root root 22776 Sep 6 16:04 /etc/rc.d/init.d/netbackup`
		The output of this example shows the netbackup service file was not removed. Delete the service file:
		`[admusr@<target_server> ~]$ sudo rm -f /etc/rc.d/init.d/netbackup`

13. ☐	**Target Server**: Identify volume and volume group	Identify the NetBackup logical volume (LV) and volume group (VG). The LV and VG are referenced in later steps.
		`[admusr@<target_server> ~]$ sudo lvs`
		`LV VG Attr LSize Pool Origin Data% Meta% Move Log Cpy%Sync Convert`
		`netbackup_lv vgroot -wi-ao---- 5.00g`
		`plat_root vgroot -wi-ao---- 1.00g`
		`plat_tmp vgroot -wi-ao---- 1.00g`
		`plat_usr vgroot -wi-ao---- 4.00g`
		`plat_var vgroot -wi-ao---- 1.00g`
		`plat_var_tklc vgroot -wi-ao---- 4.00g`
		The output shows the NetBackup LV is named **netbackup_lv** and the VG is **vgroot**.

14. ☐	**Target Server**: Identify processes using volume	Verify no processes are using the LV identified in the previous step. Use the VG and LV values identified in the previous step. No output is expected. `[admusr@<target_server> ~]$ sudo /sbin/fuser -m /dev/vgroot/netbackup_lv`
15. ☐	**Target Server**: Unmount device	Unmount **/usr/openv** device from the NetBackup LV: `[admusr@<target_server> ~]$ sudo /bin/umount -l /usr/openv`
16. ☐	**Target Server**: Remove LV entry	Remove the NetBackup LV entry from **/etc/fstab** file. `[admusr@<target_server> ~]$ sudo /bin/sed -i.bak '/netbackup_lv/d' /etc/fstab`
17. ☐	**Target Server**: Check in file	Check the **/etc/fstab** file into the RCS. `[admusr@<target_server> ~]$ sudo /usr/TKLC/plat/bin/rcscheck /etc/fstab`

Step #	Procedure	Description

18. ☐	**Target Server**: Verify removal of file	Verify the removal of the entry from the **/etc/fstab** file.
		Compare the **/etc/fstab** file to the **/etc/fstab.bak** backup file.
		`[admusr@<target_server> ~]$ sudo /usr/bin/diff /etc/fstab.bak /etc/fstab`
		`19d18`
		`< /dev/vgroot/netbackup_lv /usr/openv ext4 defaults 1 2`

19. ☐	**Target Server**: Remove backup file	Remove the **/etc/fstab.bak** file. `[admusr@<target_server> ~]$ sudo rm -f /etc/fstab.bak`
20. ☐	**Target Server**: Remove volume	Remove the NetBackup LV identified in step 13. Take care to use the correct volume group. `[admusr@<target_server> ~]$ sudo /sbin/lvremove -f /dev/vgroot/netbackup_lv`
21. ☐	**Target Server**: Remove client package entries	Execute the command in this step to remove the NetBackup client package entries from the **pkgKeep.conf** file. The NetBackup client packages were identified in step 4. If **pkgKeep.conf** only contains these packages, the pkgKeep.conf file can be removed. In this example, the NetBackup client packages are SYMCnbclt, SYMCnbjava, SYMCnbjre, SYMCpddea, and VRTSpbx. `[admusr@<target_server> ~]$ sudo /bin/sed -i.bak '/SYMCnbclt|SYMCnbjava|SYMCnbjre|SYMCpddea|VRTSpbx/d' /usr/TKLC/plat/etc/upgrade/pkgKeep.conf`

22. ☐	**Target Server**: Verify removal of packages	Verify the removal of the NetBackup client package entries from the **pkgKeep.conf** file by comparing the pkgKeep.conf to the **pkgKeep.conf.bak** backup file.
		`[admusr@<target_server> ~]$ sudo /usr/bin/diff /usr/TKLC/plat/etc/upgrade/pkgKeep.conf.bak /usr/TKLC/plat/etc/upgrade/pkgKeep.conf`
		`1,5d0`
		`< SYMCnbclt`
		`< SYMCnbjava`
		`< SYMCnbjre`
		`< SYMCpddea`
		`< VRTSpbx`

23. ☐	**Target Server**: Remove backup file	Remove the pkgKeep.conf.bak file. `[admusr@<target_server> ~]$ sudo rm -f /usr/TKLC/plat/etc/upgrade/pkgKeep.conf.bak`

Step #	Procedure	Description
24. ☐	**Target Server**: Remove configuration file	Remove the client profile configuration file, if one exists. The existence of this file is determined in step 4. ***Note***: The client profile configuration file includes the client version in the name. For example, NB7601.conf where 7601 represents the client version number with the periods removed. In this example, version 7.6.0.1 is used. `[admusr@<target_server> ~]$ sudo rm -f /usr/TKLC/plat/etc/netbackup/profiles/NB7601.conf`
25. ☐	**Target Server**: Remove script file	Remove the NetBackup client script file. For some versions of NetBackup, a script file is not used and does not exist. Proceed to the next step if this is the case. ***Note***: The client profile configuration file includes the client version in the name. For example, NB7601.conf where 7601 represents the client version number with the periods removed. In this example, version 7.6.0.1 is used. `[admusr@<target_server> ~]$ sudo rm -f /usr/TKLC/plat/etc/netbackup/scripts/NB7601`

26. ☐	**Target Server**: Remove firewall rules	Remove the firewall rules related to NetBackup.
		Note: This step varies depending on how the application implemented the firewall rules. The example in this step illustrates the correct steps for a TVOE server. If you are uninstalling NetBackup on a TPD application server, refer to the documentation for your specific application.
		Remove the iptables and ip6tables firewall rules related to NetBackup on a TVOE server:
		`[admusr@<target_server> ~]$ sudo /usr/TKLC/plat/bin/iptablesAdm delete --type=domain --domain=60netbackup --protocol=ipv4`
		`[admusr@<target_server> ~]$ sudo /sbin/service iptables restart`
		`iptables: Setting chains to policy ACCEPT: filter [ OK ]`
		`iptables: Flushing firewall rules: [ OK ]`
		`iptables: Applying firewall rules: [ OK ]`
		`[admusr@<target_server> ~]$ sudo /usr/TKLC/plat/bin/iptablesAdm delete --type=domain --domain=60netbackup --protocol=ipv6`
		`[admusr@<target_server> ~]$ sudo /sbin/service ip6tables restart`
		`ip6tables: Setting chains to policy ACCEPT: filter [ OK ]`
		`ip6tables: Flushing firewall rules: [ OK ]`
		`ip6tables: Applying firewall rules: [ OK ]`

Step #	Procedure	Description

27. ☐	**Target Server**: Remove firewall configuration files	Remove firewall configuration files related to NetBackup.
		Note: This step varies depending on how the application implemented the firewall rules. The example in this step illustrates the correct steps for a TVOE server. If you are uninstalling NetBackup on a TPD application server, refer to the documentation for your specific application.
		Remove firewall configuration files related to NetBackup on a TVOE server:
		`[admusr@<target_server> ~]$ sudo rm -f /usr/TKLC/plat/etc/iptables/60netbackup.ipt`
		`[admusr@<target_server> ~]$ sudo rm -f /usr/TKLC/plat/etc/ip6tables/60netbackup.ipt`

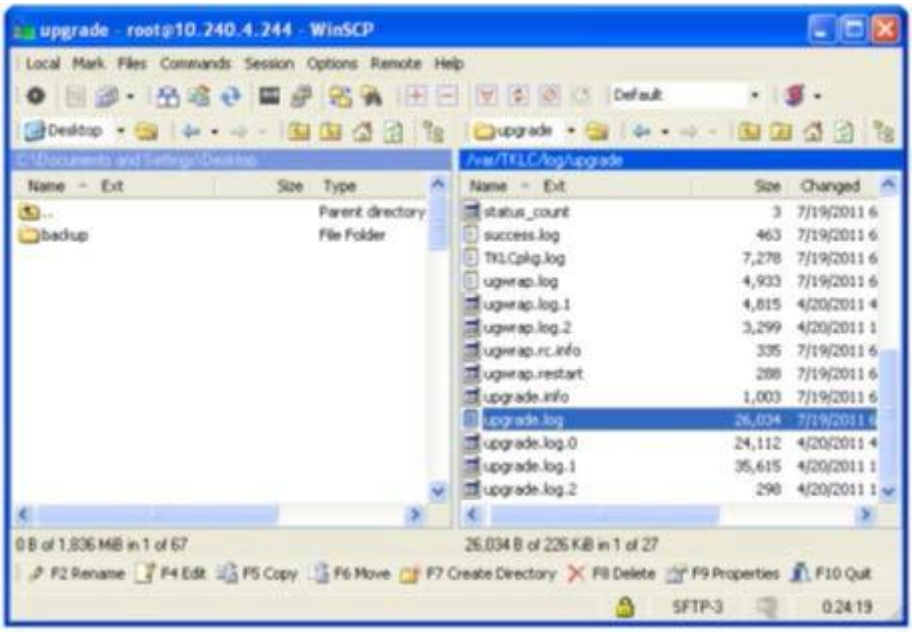
28. ☐	**Target Server**: Update hosts file	Update the /etc/hosts file to remove the NetBackup server host using the platcfg utility. ***Note***: If the NetBackup entry in the **/etc/hosts** file is an alias and you do not want to delete the host, select **Delete Alias** instead of **Delete Host**. The rest of the steps remain the same. 1. As admusr, execute the **sudo su - platcfg** command to launch the platcfg utility. 2. Select **Network Configuration**. 3. Select **Modify Hosts File**. 4. Select **Edit**. 5. Select **Delete Host**. 6. Select the host entry for NetBackup. 7. Select **Yes** to confirm deletion. 8. Exit out of the platcfg utility.

29. ☐	**Target Server**: Verify server health	No unexpected alarms should display and no missing package files should exist.
		`[admusr@<target_server> ~]$ sudo /usr/TKLC/plat/bin/alarmMgr -alarmStatus`
		`[admusr@<target_server> ~]$ sudo rpm -Va`

Appendix F. Using WinSCP

Procedure 10. Copy a File from the Management Server to the PC Desktop

Step #	Procedure	Description
This procedure demonstrates how to copy a file from the management server to your PC desktop. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Download the WinSCP application	`http:winscp.net/eng/download.php`
2. ☐	Connect to the management server	After starting this application, navigate to Session and enter: **<management_server_IP>** into the **Host name** field, **root** into the **User name** field, and **<root_password>** into the **Password** field. Click **Login**.

Step #	Procedure	Description
3. ☐	Copy the target file from the management server	On the left is your own desktop filesystem. Navigate within it to Desktop directory. On the right side is the management server file system. Within it, navigate into the location of the file you would like to copy to your desktop. Highlight the file in the management server file system by pressing the insert key, and then press **F5** to copy the file. 
4. ☐	Close the WinSCP application	Press **F10** and click **OK** to confirm terminating the session.

Appendix G. Upgrade Cisco 4948 PROM

Procedure 11. Upgrade Cisco 4948 PROM

Step #	Procedure	Description
This procedure upgrades the Cisco 4948 PROM. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		

1. ☐	**Virtual PMAC/ Management Server**: Verify the PROM image is on the system	If the appropriate image does not exist, copy the image to the server.
		Determine if the PROM image for the 4948/4948E/4948E-F is on the system.
		For a PMAC system:
		`$ ls /var/TKLC/smac/image/<PROM_image_file>`
		For a NON-PMAC system:
		`$ ls /var/lib/tftpboot/<PROM_image_file>`
		If the file exists, skip the remainder of this step and continue with the next step. If the file does not exist, copy the file from the firmware media and ensure the file is specified by the Release Notes of the HP Solutions Firmware Upgrade Pack, version 2.x.x [2].

2. ☐	**Virtual PMAC/ Management Server**: Attach to switch console	If upgrading the firmware on switch1A, connect serially to the switch by issuing the following command as admusr on the server: `$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg` `switch1A_console` `Enter platcfg@pmac5000101's password: <platcfg_password>` `[Enter `^Ec?' for help]` Press **Enter**. If the switch is not already in enable mode (**switch#** prompt), then issue the **enable** command; otherwise, continue with the next step. `Switch> enable` If upgrading the firmware on switch1B, connect serially to switch1B by issuing the following command as admusr on the PMAC server: `$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg` `switch1B_console` `Enter platcfg@pmac5000101's password: <platcfg_password>` `[Enter `^Ec?' for help]` Press **Enter**. If the switch is not already in enable mode (**switch#** prompt), then issue the **enable** command; otherwise, continue with the next step. `Switch> enable`

Step #	Procedure	Description

3. ☐	**Virtual PMAC/ Management Server (Switch Console Session)**: Configure ports on the 4948/4948E/ 4948E-F switch	To ensure connectivity, ping the management server's management vlan IP <pmac_mgmt_ip_address> address from the switch.
		`Switch# conf t`
		If upgrading the firmware on switch1A, use these commands:
		`Switch(config)# vlan <switch_mgmtVLAN_id>`
		`Switch(config-vlan)# int vlan <switch_mgmtVLAN_id>`
		`Switch(config-if)# ip address <switch1A_mgmtVLAN_ip_address> <netmask>`
		`Switch(config-if)# no shut`
		`Switch(config-if)# int gi1/40`
		If upgrading the firmware on switch1B, use these commands:
		`Switch(config)# vlan <switch_mgmtVLAN_id>`
		`Switch(config-vlan)# int vlan <switch_mgmtVLAN_id>`
		`Switch(config-if)# ip address <switch1B_mgmtVLAN_ip_address> <netmask>`
		`Switch(config-if)# no shut`
		`Switch(config-if)# int gi1/40`
		If the model is 4948, execute these commands:
		`Switch(config-if)# switchport trunk encap dot1q`
		`Switch(config-if)# switchport mode trunk`
		`Switch(config-if)# spanning-tree portfast trunk`
		`Switch(config-if)# end`
		`Switch# write memory`
		If the model is 4948E or 4948E-F, execute these commands:
		`Switch(config-if)# switchport mode trunk`
		`Switch(config-if)# spanning-tree portfast trunk`
		`Switch(config-if)# end`
		`Switch# write memory`
		Now issue **ping** command:
		Note: The IP address <pmac_mgmt_ip_address> is in the reference table at the beginning of the Cisco 4948 configuration procedure that referenced this procedure.
		`Switch# ping <pmac_mgmtVLAN_ip_address>`
		`Type escape sequence to abort.`
		`Sending 5, 100-byte ICMP Echos to <pmac_mgmt_ip_address>, timeout is 2 seconds:`
		`!!!!!`
		`Success rate is 100 percent (5/5), round trip min/avg/max = 1/1/4 ms`
		If ping is not successful, make sure the procedure was completed correctly by repeating all steps up to this point. If after repeating those steps, ping is still unsuccessful, then contact My Oracle Support (MOS).

Step #	Procedure	Description

4. ☐	**Virtual PMAC/ Management Server (Switch Console Session)**: Upgrade PROM	`Switch# copy tftp: bootflash:`
		`Address or name of remote host []? <pmac_mgmt_ip_address>`
		`Source filename []? <PROM_image_file>`
		`Destination filename [<PROM_image_file>]? [Enter]`
		`Accessing tftp://<pmac_mgmt ip_address>/<PROM_image_file>...`
		`Loading <PROM_image_file> from <pmac_mgmt ip_address> (via Vlan2): !!!!!! [OK-`
		`45606 bytes]`
		`45606 bytes copied in 3.240 secs (140759 bytes/sec)`
		`Switch#`

5. ☐	**Virtual PMAC/ Management Server (Switch Console Session)**: Reload switch	`Switch# reload`
		`System configuration has been modified. Save? [yes/no]: no`
		`Proceed with reload? [confirm] [Enter]`
		`=== Boot messages removed ===`
		Type **Control-C** when **Type control-C to prevent autobooting** message displays.

6. ☐	**Virtual PMAC/ Management Server (Switch Console Session)**: Upgrade PROM	`rommon 1 > boot bootflash:<PROM_image_file>`
		`=== PROM upgrade messages removed ===`
		`System will reset itself and reboot within few seconds....`

7. ☐	**Virtual PMAC/ Management Server (Switch Console Session)**: Verify upgrade	The switch reboots when the firmware upgrade completes. Allow it to boot. Wait for the following line to be printed:
		`Press RETURN to get started!`
		`Would you like to terminate autoinstall? [yes]: [Enter]`
		`Switch> show version | include ROM`
		`ROM: 12.2(31r)SGA1`
		`System returned to ROM by reload`
		Review the output and look for the ROM version. Verify the version is the desired new version.
		If the switch does not boot properly, or has the wrong ROM version, contact My Oracle Support (MOS).

Step #	Procedure	Description

8. ☐	**Virtual PMAC/ Management Server**: Reset switch to factory defaults	Connect serially to the switch as outlined in step 4. , and reload by performing the following commands:
		`Switch# write erase`
		`Switch# reload`
		Wait until the switch reloads, then exit from console, enter **ctrl-e + c + .** and you are returned to the server prompt.
		Note: There may be messages from the switch, if asked to confirm, press **Enter**. If asked yes or no, type **No** and press **Enter**.

Appendix H. Backup Procedures

Appendix H.1 Back Up HP (6120XG, 6125G, 6125XLG, 6127XLG) Enclosure Switch

Execute this procedure after every change to the switch configuration after completing Procedure 21, Procedure 22, and/or Procedure 23.

Prerequisites:

- Install TVOE on the Management Server (section 4.1.1)
- Deploy PMAC (section 4.2.1) must be completed
- Configure 3020 Switches (netConfig) (Procedure 20)
- Configure HP 6120XG Switch (netConfig) (Procedure 21)
- Configure HP 6125G Switch (netConfig) (Procedure 22)
- Configure HP 6127XLG Switch (netConfig) (Procedure 24)

Variable	Value
<switch_name>	Hostname of the switch

Procedure 11. Back Up the HP Enclosure Switch

Step #	Procedure
	This procedure backs up the HP enclosure switch. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

1. ☐	Ensure the directory where the backups are stored exists.
	`$ sudo /bin/ls -i -l /usr/TKLC/smac/etc/switch/backup`
	If you receive an error such as the following:
	`-bash: ls: /usr/TKLC/smac/etc/switch/backup: No such file or directory`
	Then the directory must be created by issuing the following command:
	`$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/switch/backup`
	Change the directory permissions:
	`$ sudo /bin/chmod go+x /usr/TKLC/smac/etc/switch/backup`

Step #	Procedure
2. ☐	Execute the backup command. `$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> backupConfiguration service=ssh_service filename=<switch_name>-backup`
3. ☐	Copy the files to the backup directory. `$ sudo /bin/mv -i ~admusr/<switch>-backup* /usr/TKLC/smac/etc/switch/backup`

4. ☐	Verify switch configuration was backed up by **cat <switch_name>** and inspect its contents to ensure it reflects the latest known good switch configurations.
	`$ sudo /bin/ls -i /usr/TKLC/smac/etc/switch/backup/<switch_name>-backup*`
	`$ sudo /bin/cat /usr/TKLC/smac/etc/switch/backup/<switch_name>-backup`

5. ☐	Save FW files. If a firmware upgrade, switch replacement, or an initial install (which performed a FW upgrade during initialization) was performed, back up the FW image used by performing the following command: `$ sudo /bin/mv -i ~<switch_backup_user>/<fw image> <switch backup directory>/`
6. ☐	Repeat step 2. through 5. for each HP switch to be backed up.

7. ☐	Back up the PMAC application.
	`$ sudo /usr/TKLC/smac/bin/pmacadm backup`
	`PMAC backup has been successfully initiated as task ID 7`
	Note: The backup runs as a background task. To check the status of the background task use the PMAC GUI Task Monitor screen, or issue the command `$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`. The result should eventually be **PMAC Backup successful** and the background task should indicate **COMPLETE**.
	Note: The **pmacadm backup** command uses a naming convention that includes a date/time stamp in the filename (for example, backupPmac_20111025_100251.pef). In the example provided, the backup filename indicates it was created on 10/25/2011 at 10:02:51 am server time.

Step #	Procedure

8. ☐	Verify PMAC backup was successful
	Note: If the background task shows the backup failed, then the backup did not complete successfully. STOP and contact My Oracle Support (MOS).
	The output of pmaccli getBgTasks should look similar to the example below:
	`$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`
	`2: Backup PMAC COMPLETE - PMAC Backup successful`
	`Step 2: of 2 Started: 2012-07-05 16:53:10 running: 4 sinceUpdate: 2 taskRecordNum:`
	`2 Server Identity:`
	`Physical Blade Location:`
	`Blade Enclosure:`
	`Blade Enclosure Bay:`
	`Guest VM Location:`
	`Host IP:`
	`Guest Name:`
	`TPD IP:`
	`Rack Mount Server:`
	`IP:`
	`Name:`
	::

9. ☐	Save the PMAC backup The PMAC backup must be moved to a remote server. Transfer (sftp, scp, rsync, or preferred utility), the PMAC backup to an appropriate remote server. The PMAC backup files are saved in the following directory: **/var/TKLC/smac/backup**.

Appendix H.2 Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig)

***Prerequisites* for RMS system aggregation switch**:

- Step 2 of 4.1.1 Install TVOE on the Management Server to install the IPM DL380 server.
- Configure TVOE Network (section 4.1.4)
- Configure Aggregation Switches (section 4.3.1)

***Prerequisites* for Cisco 3020 enclosure switch**:

- Install TVOE on the Management Server (section 4.1.1)
- Configure TVOE Network (section 4.1.4)
- Deploy PMAC (section 4.2.1) must be completed
- Configure 3020 Switches (netConfig) (Procedure 20)

Variable	Value
<switch_backup_user> (also needed in switch configuration procedure)	admusr
<switch_backup_user_password> (also needed in switch configuration procedure)	admusr
<switch_name>	Hostname of the switch
<switch_backup_directory>	Non-PMAC System: /usr/TKLC/plat/etc/switch/backup
	PMAC System: /usr/TKLC/smac/etc/switch/backup

Procedure 10. Back Up the Cisco Switch

Step #	Procedure
	This procedure backs up the Cisco aggregation and enclosure switches. Refer to Appendix Q for the workaround on cipher mismatch issue with Cisco switches. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

1. ☐	Verify switch is at least initialized correctly and connectivity to the switch by verifying hostname
	`$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> getHostname`
	`Hostname: switch1A`
	Note: The value beside **Hostname** should be the same as the <switch_name> variable.

Step #	Procedure

2. ☐	Run the **netConfig --repo showService name=ssh_service** command and look for ssh service.
	`$ sudo /usr/TKLC/plat/bin/netConfig --repo showService name=ssh_service`
	`Service Name: ssh_service`
	`Type: ssh`
	`Host: 10.250.62.85`
	`Options:`
	`password: C20F7D639AE7E7`
	`user: admusr`
	In the ssh_service parameters, the value for **user:** is the value for the variable <switch_backup_user>.

3. ☐	Verify existence of the backup directory.
	`$ sudo /bin/ls -i <switch_backup_directory>`
	If the output contains:
	`ls: cannot access <switch_backup_directory>: No such file or directory`
	Create the directory with:
	`$ sudo /bin/mkdir -p <switch_backup_directory>`
	Change directory permissions:
	`$ sudo /bin/chmod go+x <switch backup directory>`

4. ☐	Execute the backup command. `$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> backupConfiguration service=ssh_service filename=<switch_name>-backup`

5. ☐	Verify switch configuration was backed up by **cat <switch_name>** and inspect its contents to ensure it reflects the latest known good switch configurations. Copy the files to the backup directory.
	`$ sudo /bin/ls -i ~<switch_backup_user>/<switch_name>-backup*`
	`$ sudo /bin/cat ~<switch_backup_user>/<switch_name>-backup*`
	`$ sudo /bin/chmod 644 <switch_name>-backup*`
	`$ sudo /bin/mv -i ~admusr/<switch name>-backup* <switch_backup_directory>/`
	Note: The cat command may leave garbled text on the next terminal prompt. Disregard this text.
	Example:
	`[admusr@pmac ~]$ PuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPuTTYPu`

Step #	Procedure

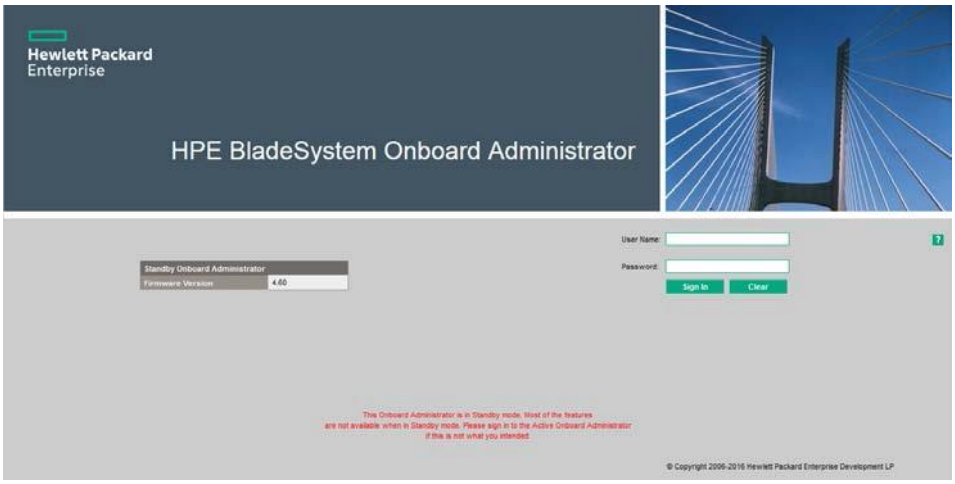
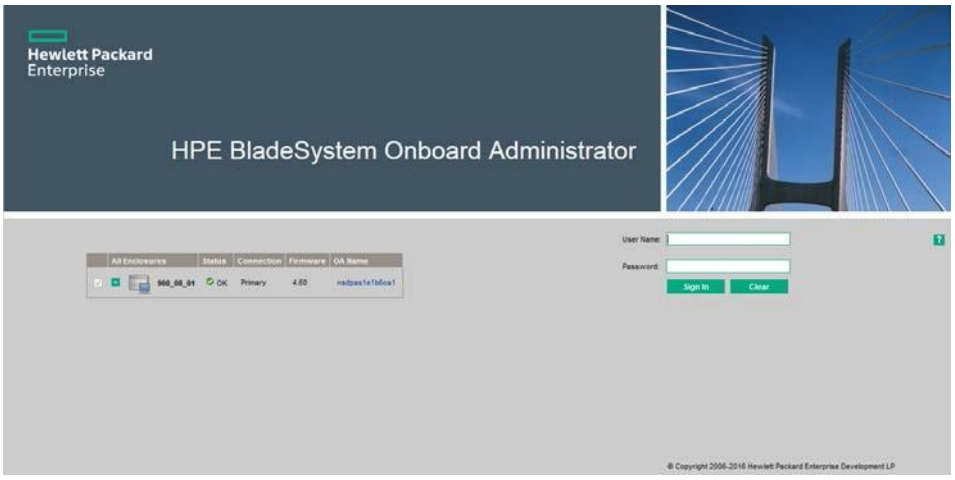
6. ☐	Back up the PMAC application.
	`$ sudo /usr/TKLC/smac/bin/pmacadm backup`
	`PMAC backup has been successfully initiated as task ID 7`
	Note: The backup runs as a background task. To check the status of the background task use the PMAC GUI Task Monitor screen, or issue the command `$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`. The result should eventually be **PMAC Backup successful** and the background task should indicate **COMPLETE**.
	Note: The **pmacadm backup** command uses a naming convention that includes a date/time stamp in the filename (for example, backupPmac_20111025_100251.pef). In the example provided, the backup filename indicates it was created on 10/25/2011 at 10:02:51 am server time.

7. ☐	Verify PMAC backup was successful
	Note: If the background task shows the backup failed, then the backup did not complete successfully. STOP and contact My Oracle Support (MOS).
	The output of pmaccli getBgTasks should look similar to the example below:
	`$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks`
	`2: Backup PMAC COMPLETE - PMAC Backup successful`
	`Step 2: of 2 Started: 2012-07-05 16:53:10 running: 4 sinceUpdate: 2 taskRecordNum:`
	`2 Server Identity:`
	`Physical Blade Location:`
	`Blade Enclosure:`
	`Blade Enclosure Bay:`
	`Guest VM Location:`
	`Host IP:`
	`Guest Name:`
	`TPD IP:`
	`Rack Mount Server:`
	`IP:`
	`Name:`
	`::`

8. ☐	Save the PMAC backup The PMAC backup must be moved to a remote server. Transfer (sftp, scp, rsync, or preferred utility), the PMAC backup to an appropriate remote server. The PMAC backup files are saved in the following directory: **/var/TKLC/smac/backup**.
9. ☐	Repeat steps steps 1. and 4. through 8. for each switch to be backed up.

Appendix I. Determine which Onboard Administrator is Active

Procedure 11. Determine which Onboard Administrator is Active

Step #	Procedure	Description
This procedure determines which onboard administrator is active in an enclosure with two OAs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**OA GUI**: Determine which OA is active	Open a web browser and navigate to the IP address of one of the administrators. If you see the following page, you have navigated to a GUI of the Standby Onboard Administrator as indicated by the red warning. In such case, navigate to the other Onboard Administrator IP address.  If you navigate the GUI of active Onboard Administrator GUI, the enclosure overview table is available in the left part of the login page as shown below. 

Appendix J. NetBackup Procedures (Optional)

Appendix J.1 Application NetBackup Client Install/Upgrade Procedures

The NetBackup is a utility used to manage backups and recover remote systems. The NetBackup suite supports disaster recovery at the customer site.

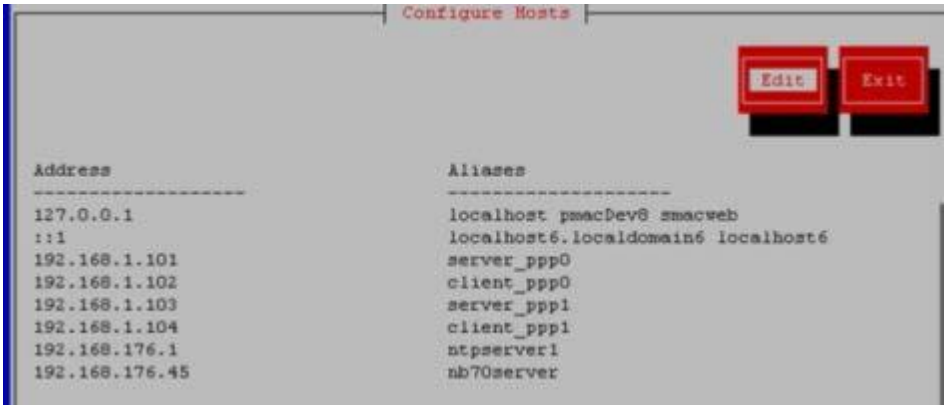
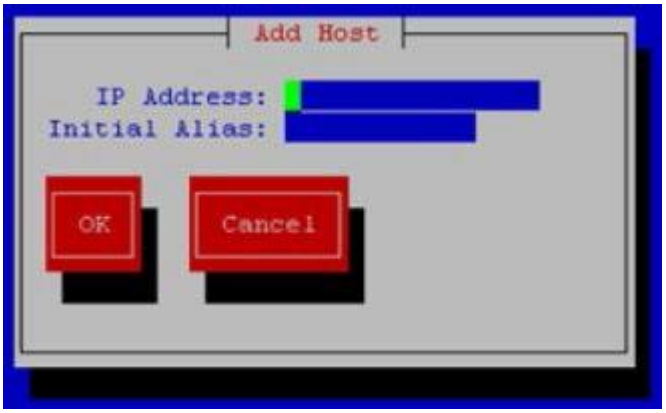
Notes

- Platform 7.0.0 only supports NetBackup 7.1 and 7.5 clients, while Platform 7.0.1 only supports NetBackup 7.1, 7.5, and 7.6 clients. Platform 7.4 supports NetBackup 7.7. If the NetBackup client being installed is not supported, contact My Oracle Support (MOS) for guidance on creating a configuration file that allows for installing unknown NetBackup clients. Use Appendix J.4 Create NetBackup Client Configuration File once the contents of the configuration file are known.
- Failure to install the NetBackup client properly (that is, by neglecting to execute this procedure) may result in the NetBackup client being deleted during an Oracle software upgrade.

Procedure 10. Install/Upgrade NetBackup Client Software on an Application Server

Step #	Procedure	Description
This procedure installs and configures the NetBackup client software on an application server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	Select and perform NetBackup client installation	There are two different ways to install NetBackup Client. Perform one of the following methods. • If a customer has a way of transferring and installing the NetBackup client without the aid of TPD tools, then use Appendix J.2 NetBackup Client Install/Upgrade with nbAutoInstall. This is not common and if the answer to the previous question is not known then do not use Appendix J.2. • If you do not use Appendix J.2, use Appendix J.3 NetBackup Client Install/Upgrade with platcfg.

2. ☐	**Application Console**: Modify host file	Use platform configuration utility (platcfg) to modify hosts file with the NetBackup server alias.
		Note: If the NetBackup client has successfully been installed, then you can find the NetBackup server's hostname in the **/usr/openv/netbackup/bp.conf** file. It is identified by the **SERVER** configuration parameter as shown in the following output:
		1. List NetBackup servers hostname:
		`$ sudo cat /usr/openv/netbackup/bp.conf`
		`SERVER = nb70server`
		`CLIENT_NAME = pmacDev8`
		Note: In the case of nbAutoInstall, the NetBackup client may not yet be installed. For this situation, the **/usr/openv/netbackup/bp.conf** command cannot be used to find the NetBackup server alias.
		Use platform configuration utility (platcfg) to update application hosts file with NetBackup Server alias.
		`$ sudo su – platcfg`

Step #	Procedure	Description
		2. Navigate to **Network Configuration > Modify Hosts File**.  3. Select **Edit** to display the Host Action Menu. 4. Select **Add Host** and enter the appropriate data.  5. Select **OK** to confirm the host alias add and exit the Patfrom Cofiguration Utility.

Step #	Procedure	Description

3. ☐	**Application Console**: Create path	Create a link for the NetBackup client scripts to a path on the application server where the NetBackup expects to find them.
		Note: Link notify scripts from appropriate path on application server for given application.
		`$ sudo mkdir -p /usr/openv/netbackup/bin/`
		`$ sudo ln -s <path>/bpstart_notify /usr/openv/netbackup/bin/bpstart_notify`
		`$ sudo ln -s <path>/bpend_notify /usr/openv/netbackup/bin/bpend_notify`

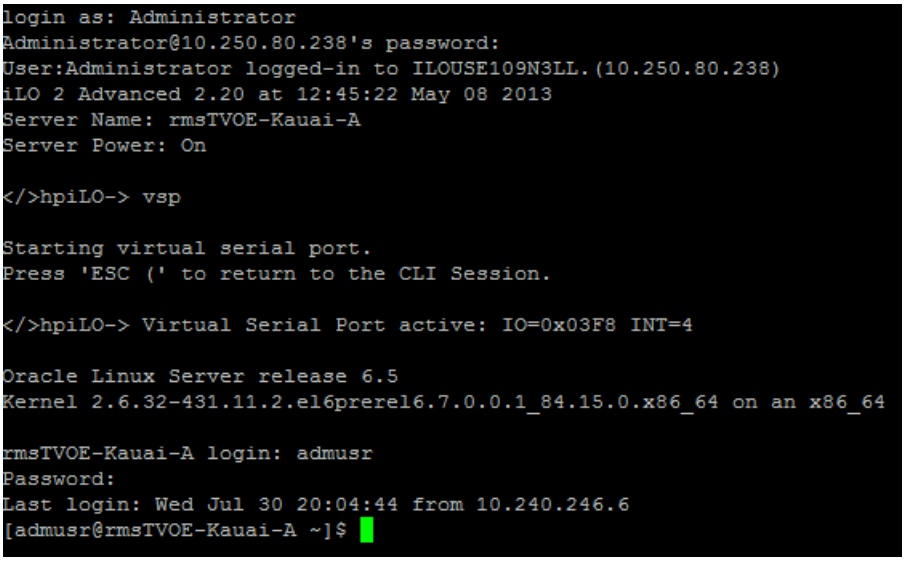
Appendix J.2 NetBackup Client Install/Upgrade with nbAutoInstall

Procedure 10. Install/Upgrade NetBackup Client with nbAutoInstall

Step #	Procedure
	This procedure enables TPD to detect when a NetBackup client is installed and completes TPD tasks needed for NetBackup client operation. ***Notes***: • The NetBackup client installation (pushing the client and performing the installation) is the responsibility of the customer and is not covered in this procedure. If the customer does not have a way to push and install the NetBackup client, use Appendix J.3. • Execute this procedure before the customer does the NetBackup client installation. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.
1. ☐	Enable nbAutoInstall by executing: `$ sudo /usr/TKLC/plat/bin/nbAutoInstall --enable` The server now periodically checks to see if a new version of NetBackup client has been installed and performs necessary TPD configuration accordingly. At any time, the customer may now push and install a new version of NetBackup client.

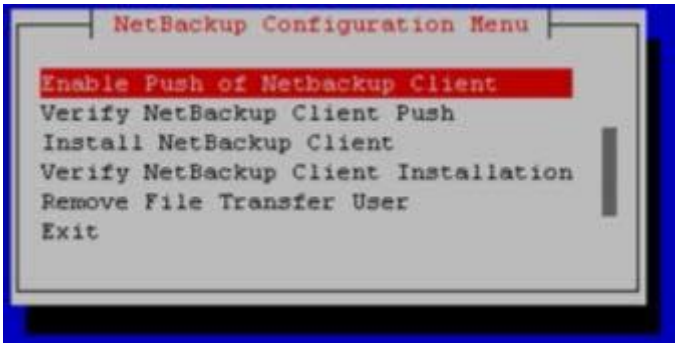
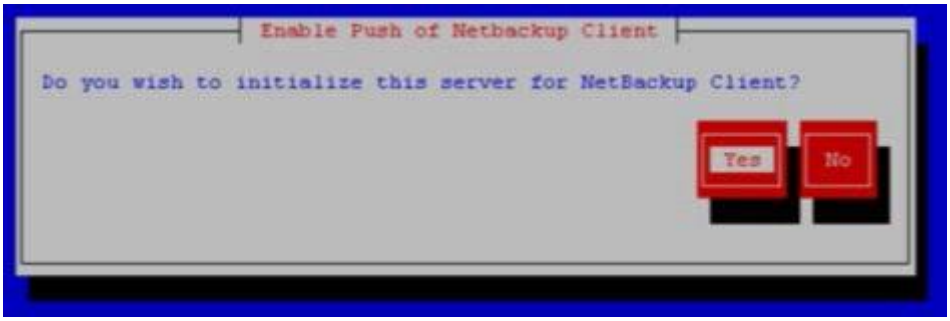
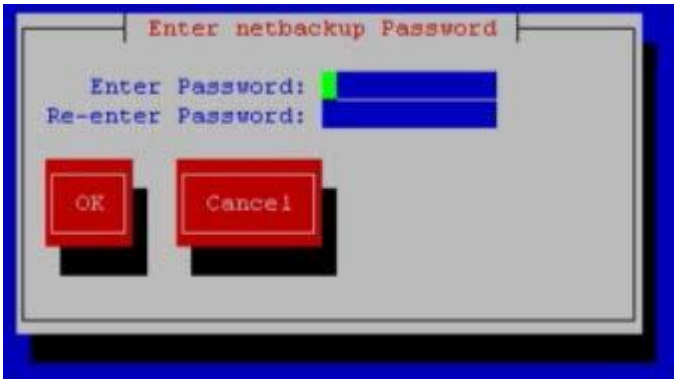
Appendix J.3 NetBackup Client Install/Upgrade with platcfg

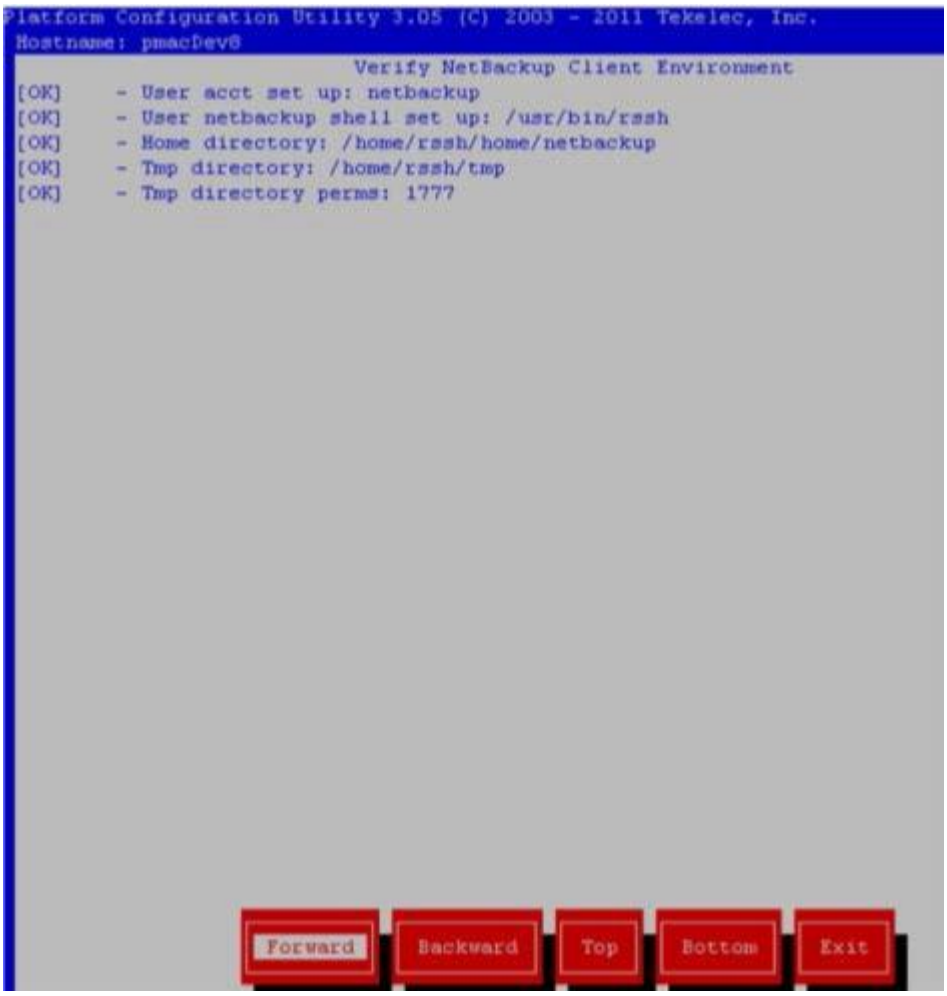
Procedure 11. Install/Upgrade NetBackup Client with platcfg

Step #	Procedure	Description
This procedure pushes and installs NetBackup client using platcfg. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**Application Server iLO**: Login and open integrated remote console	1. Log into the using a web browser and the password provided by the application. `http://<management_server_iLO_IP>` 2. Click the Remote Console tab and open the Integrate Remote Console on the server.  3. Click **Yes** if the security alert displays.

Step #	Procedure	Description

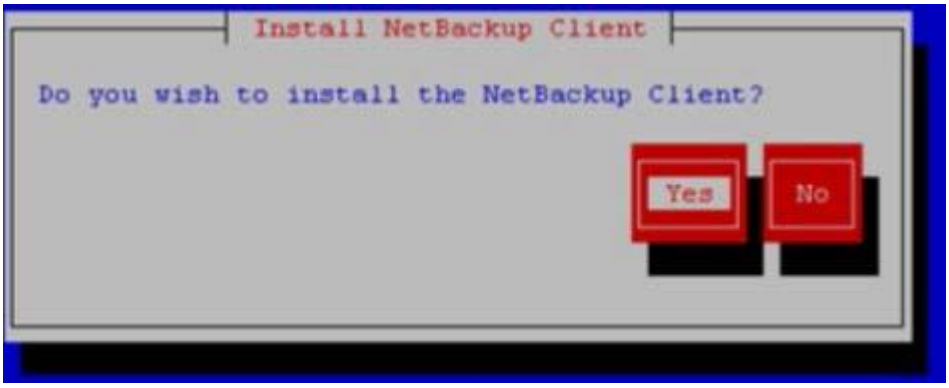
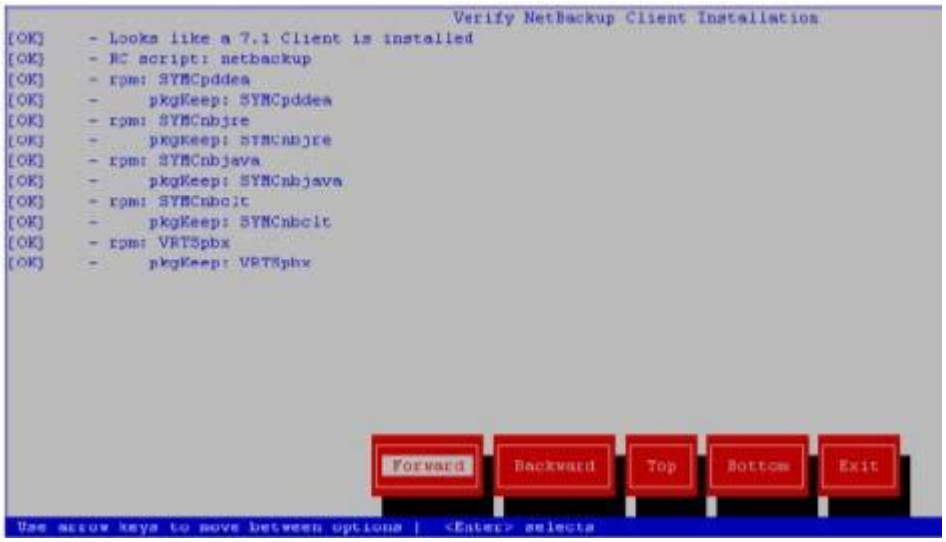
2. ☐	**TVOE Application Server ILO**: Login	If the application is a guest on a TVOE host, login with application **admusr** credentials. If the application is not a guest on a TVOE host, continue to step 3.
		
		Note: On a TVOE host, if you open the virsh console, for example, `$ sudo /usr/bin/virsh console X` or from the virsh utility `virsh # console X` command and you get garbage characters or the output is not correct, then there is likely a stuck **virsh console** command already being run on the TVOE host. Exit out of the virsh console, run `ps -ef |grep virsh`, and then kill the existing process "`kill -9 <PID>`. Then execute the `virsh console X` command. Your console session should now run as expected.
		
		Log into the application console using virsh and wait until you see the login prompt:
		
		`$ virsh`
		`$ virsh list --all`
		`Id Name State`
		`----------`
		`13 myTPD running`
		`20 applicationGuestName running`
		`$ virsh console applicationGuestName`
		`[Output Removed]`
		`Starting ntdMgr: [ OK ]`
		`Starting atd: [ OK ]`
		`'TPD Up' notification(s) already sent: [ OK ]`
		`upstart: Starting tpdProvd...`
		`upstart: tpdProvd started.`
		`CentOS release 6.2 (Final)`
		`Kernel 2.6.32-220.17.1.el6prerel6.0.0_80.14.0.x86_64 on an x86_64`
		`applicationGuestName login:`

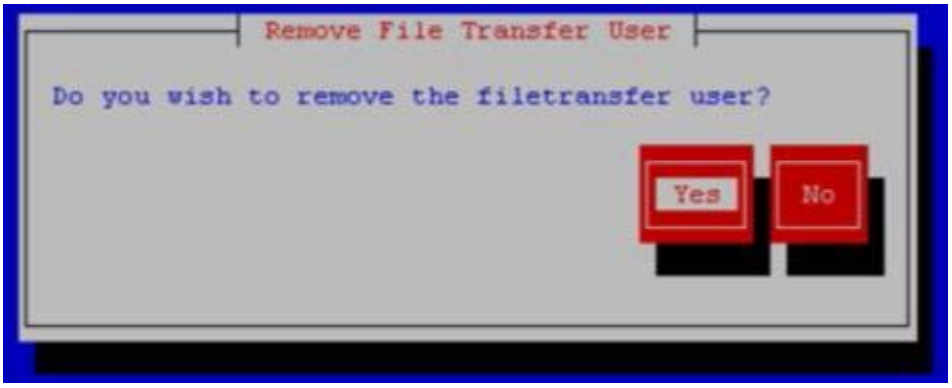
Step #	Procedure	Description
3.	**Application Console**: Configure NetBackup	1. Configure the NetBackup client on the application server. `$ sudo su – platcfg` 2. Navigate to NetBackup Configuration > Enable Push of NetBackup Client.  3. Select **Yes** to initialize the server and enable the NetBackup client software push.  4. Enter NetBackup password and select **OK**.  If the version of NetBackup is 7.6.0.0 or greater, follow the instructions provided by the OSDC download for the version of NetBackup that is being pushed.

Step #	Procedure	Description
4.	**Application Console**: Verify software push is enabled	Verify the NetBackup client software push is enabled. 1. Navigate to NetBackup Configuration > Verify NetBackup Client Push. 2. Verify list entries indicate **OK** for NetBackup client software environment.  3. Select **Exit** to return to the NetBackup Configuration menu.

Step #	Procedure	Description

5. ☐	**NetBackup Server**: Push software	Push appropriate NetBackup client software to application server.
		Notes
		• The NetBackup server is not an application asset. Access to the NetBackup server and location path of the NetBackup client software is under the control of the customer. These steps are required on the NetBackup server to push the NetBackup client software to the application server. It is assumed the NetBackup server is executing in a Linux environment.
		• The backup server is supported by the customer and the backup utility software provider. If this step, executed at the backup utility server, fails to execute successfully, STOP and contact My Oracle Support (MOS) for the backup and restore utility software provider being used at this site.
		• The NetBackup user on the client is a new user who is required to change the password immediately. Change the initial password during the client's NetBackup configuration patcfg session.
		1. Log into the NetBackup server using the password provided by the customer.
		`$ sudo cd /usr/openv/netbackup/client/Linux/6.5`
		2. Execute the sftp_to_client NetBackup utility using the application IP address and application NetBackup user:
		`# ./sftp_to_client 10.240.17.106 netbackup`
		`Connecting to 10.240.17.106...`
		`Password:`
		`You are required to change your password immediately (root enforced)`
		`Changing password for netbackup.`
		`(current) UNIX password:`
		`New password:`
		`Retype new password:`
		`sftp completed successfully.`
		The root user on 10.240.17.106 must now execute the command **sh /tmp/bp.26783/client_config [-L]**. The optional argument, **-L**,is used to avoid modification of the client's current bp.conf file.

Step #	Procedure	Description
6. ☐	**Application Console**: Install software	Install NetBackup client software on application server. 1. Navigate to **NetBackup Configuration > Install NetBackup Client**.  2. Select **Yes** to install the NetBackup client software. 3. Select **Exit** to return to the NetBackup Configuration menu.
7. ☐	**Application Console**: Verify installation	Verify NetBackup client software installation on the application server. 1. Navigate to NetBackup Configuration > Verify NetBackup Client Installation. 2. Verify list entries indicate **OK** for NetBackup client software installation.  3. Select **Exit** to return to the NetBackup Configuration menu.

Step #	Procedure	Description
8.	**Application Console**: Verify transfer	Disable NetBackup client software transfer to the application server. 1. Navigate to **NetBackup Configuration > Remove File Transfer User**.  2. Select **Yes** to remove the NetBackup file transfer user from the application server.

9.	**Application Console**: Verify server has been added to file	Verify the server has been added to the **/user/openv/netbackup/bp.conf** file.
		`$ sudo cat /usr/openv/netbackup/bp.conf`
		`CLIENT_NAME = 10.240.34.10`
		`SERVER = NB71server`

10.	**Application Server iLO**: Exit	Exit platform configuration utility (platcfg)

Appendix J.4 Create NetBackup Client Configuration File

Procedure 18. Create NetBackup Client Configuration File

Step #	Procedure	Description
This procedure copies a NetBackup client configuration file into the appropriate location on the TPD based application server. The configuration file allows you to install previously unsupported versions of the NetBackup client by providing necessary information to the TPD. The contents of the configuration file are provided by My Oracle Support (MOS). Contact My Oracle Support (MOS) if you are attempting to install an unsupported version of the NetBackup client. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		

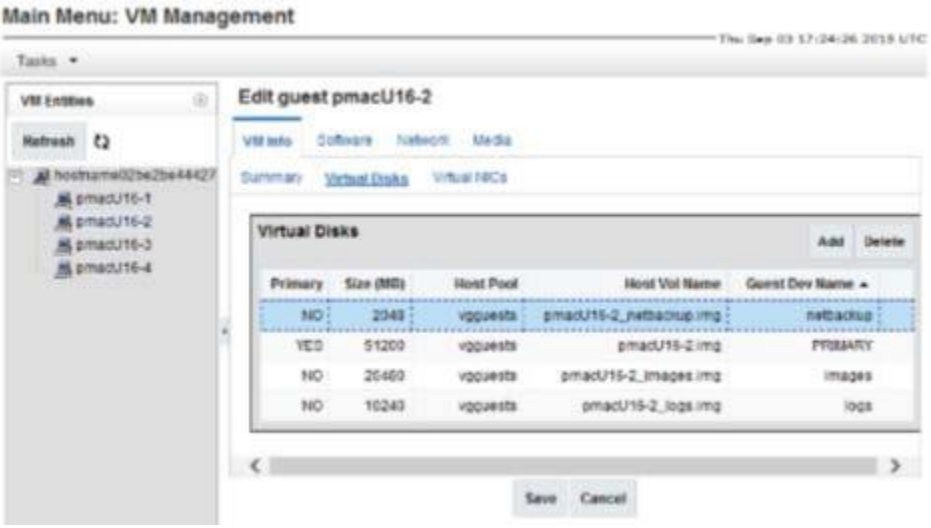
1.
☐
	Server:
	Create NetBackup client config file
		Create the NetBackup client configuration file on the server using the contents that were previously determined. The configuration file is placed in the **/usr/TKLC/plat/etc/netbackup/profiles** directory and follows this naming convention:
		
		`NB$ver.conf`
		
		Where **$ver** is the client version number with the periods removed. For the 7.5 client, the value of **$ver** would be 75 and the full path to the file would be:
		
		`/usr/TKLC/plat/etc/netbackup/profiles/NB75.conf`
		Note: The config files must start with **NB** and must have a suffix of **.conf**.
		
		The server is now capable of installing the corresponding NetBackup Client.

2.
☐
	Server:
	Create NetBackup client config file script
		Create the NetBackup client configuration script file on the server using the contents that were previously determined. The configuration script file is placed in the **/usr/TKLC/plat/etc/netbackup/scripts** directory. The name of the NetBackup client configuration script file is determined from the contents of the NetBackup client configuration file. As an example for the NetBackup 7.5 client the following is applicable:
		
		NetBackup client configuration:
		
		`/usr/TKLC/plat/etc/netbackup/profiles/NB75.conf`
		
		NetBackup client configuration script:
		
		`/usr/TKLC/plat/etc/netbackup/scripts/NB75`

Appendix J.5 Configure PMAC Application Guest NetBackup Virtual Disk

Procedure 18. Configure PMAC Application Guest NetBackup Virtual Disk

Step #	Procedure	Description
This procedure configures the PMAC application guest NetBackup virtual disk. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as pmacadmin user. Navigate to **VM Management**.
2. ☐	**PMAC GUI**: Determine configuration	Select the PMAC application guest from the **VM Entities** list. If the NetBackup device exists for the PMAC application guest, then return to the procedure that invoked this procedure; otherwise, continue with this procedure.

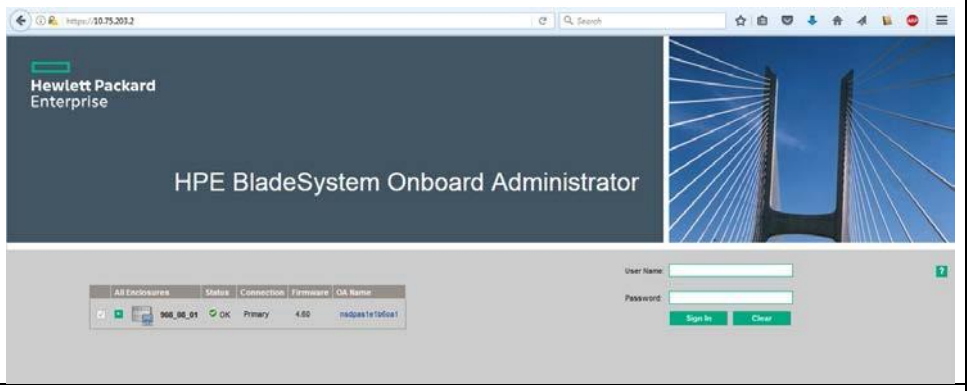
Step #	Procedure	Description
3. ☐	**PMAC GUI**: Add virtual disk	Edit the PMAC application guest to add the **NetBackup** virtual disk. 1. Click **Edit** and enter the following data for the new NetBackup virtual disk. • Size (MB): 2048 • Host Pool: vgguests • Host Vol Name: <pmacGuestName>_netbackup.img • Guest Dev Name: netbackup ***Note***: The **Guest Dev Name** must be set to **netbackup** for the PMAC application to mount the appropriate host device. The **<pmacGuestName>** variable should be set to the PMAC guest's name to create a unique volume name on the TVOE host of the PMAC.  2. Click **Save**. A confirmation screen displays with the message: Changes to the PMAC guest: <pmacGuestName> will not take effect until after the next power cycle. Do you wish to continue? 3. Click **OK**. 4. Navigate to the **Background Task Monitoring**. Confirm the guest edit task has completed successfully.

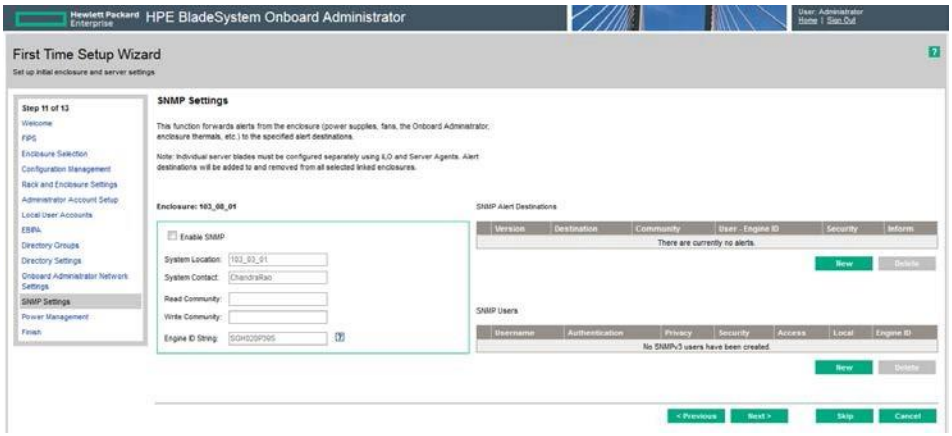
Step #	Procedure	Description

4. ☐	**TVOE Management Server iLO**: Shut down guest	Shut down the PMAC application guest.
		Note: To configure the PMAC application with the new NetBackup virtual disk, the PMAC application guest needs to be shut down and restarted. Refer to *PMAC Incremental Upgrade*, Release 5.7 and 6.0, E54387, Appendix O, **Shutdown PMAC 5.5 or Later Guest**.
		Using virsh utility on TVOE host of PMAC guest, start the PMAC guest. Query the list of guests until the PMAC guest is **running**.
		`$ sudo /usr/bin/virsh`
		`virsh # list --all`
		`Id Name State`
		`----------`
		`20 pmacU14-1 shut off`
		`virsh # start pmacU14-1`
		`Domain pmacU14-1 started`
		`virsh # list --all`
		`Id Name State`
		`----------`
		`20 pmacU14-1 running`

Appendix K. Disable SNMP on the OA

Procedure 10. Disable SNMP on the OA

Step #	Procedure	Description
This procedure disables SNMP on the OA. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**OA GUI**: Login	Open you web browser and navigate to the OA Bay 1 IP address assigned in Procedure 11. `http://<OA_IP>` Login as an administrative user. The original password is on a paper card attached to each OA. 
2. ☐	**OA GUI**: SNMP Settings	Use either the **First Time Setup Wizard SNMP Settings** menu or the **Enclosure Information > Enclosure Settings > SNMP Settings** menu.

Step #	Procedure	Description
3. ☐	**OA GUI**: SNMP Settings	Unmark the **Enable SNMP** checkbox. 

Appendix L. Downgrade Firmware on a 6125 Switch

Procedure 10. Downgrade Firmware on a 6125 Switch

Step #	Procedure	Description
This procedure downgrades firmware on 6125G enclosure switches when they are found to contain firmware newer than the qualified baseline. See HP Solutions Firmware Upgrade Pack, version 2.x.x [2] (the latest is recommended if an upgrade is to be performed; otherwise, version 2.2.8 is the minimum) for the target firmware version. ***Prerequisite***: This procedure assumes the netConfig repository data fill is complete including copying the target firmware to the netConfig server (PMAC). Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		

1. ☐	**Active OA**: Login	SSH into the active OA and login as the administrative user.
		`login as: <oa_user>`
		`<oa user>@<oa ip>'s password: <oa password>`

2. ☐	**Active OA**: Access serial console	Gain serial console access to the switch by executing the following command.
		Note: Multiple **Enter** keystrokes are required to gain the switch console prompt.
		`> connect interconnect <io_bay> [Enter] [Enter] [Enter]`
		`Username: <switch_user> [Enter]`
		`Password: <switch password> [Enter] [Enter]`

Step #	Procedure	Description

3. ☐	**Switch**: Determine firmware	Execute the **display version** command to determine if a downgrade of the firmware needs to be performed.
		`> display version`
		`HP Comware Platform Software`
		`Comware Software, Version 5.20.99, Release 2105`
		`Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.`
		`HP 6125G Blade Switch uptime is 0 week, 2 days, 23 hours, 49 minutes`
		`Slot 1 (M):`
		`Uptime is 0 weeks,2 days,23 hours,49 minutes`
		`HP 6125G Blade Switch with 1 Processor`
		`1024M bytes SDRAM`
		`256M bytes Nand Flash Memory`
		`Hardware Version is Ver.B`
		`CPLD Version is 003`
		`BootWare Version is 1.07`
		`[SubSlot 0] Back Panel`
		`[SubSlot 1] Front Panel`
		If the firmware is found to be newer than the target firmware, then proceed with the rest of this procedure; otherwise, gracefully exit the switch and PMAC.

4. ☐	**Virtual PMAC**: Login	SSH into the PMAC and login as **admusr**.
		`login as: admusr`
		`Password: <admusr_password>`
		`Last login: Fri Aug 28 12:09:06 2015 from 10.75.8.61`
		`[admusr@<pmac> ~]$`

5. ☐	**Virtual PMAC**: Copy firmware	Copy the firmware file to the switch.
		`$ sudo /usr/bin/scp 6125-cmw520-r2105.bin <switch_user>@<switch_ip>:/6125-cmw520-r2105.bin`
		`<switch_user>@<switch_ip>'s password: <switch_platform_password>`
		`100% 16MB 766.3KB/s 00:21`

6. ☐	**Virtual PMAC**: Exit	Gracefully exit from the PMAC SSH session. `$ logout`

7. ☐	**Active OA**: Login	If not already connected, ssh into the active OA and login as the administrative user.
		`login as: <oa_user>`
		`<oa_user>@<oa_ip>'s password: <oa_password>`

Step #	Procedure	Description

8. ☐	**Active OA**: Access serial console	If not already connected, gain serial console access to the switch by executing the following command.
		Note: Multiple **Enter** keystrokes are required to gain the switch console prompt.
		`> connect interconnect <io_bay> [Enter] [Enter] [Enter]`
		`Username: <switch_user> [Enter]`
		`Password: <switch_password> [Enter] [Enter]`

9. ☐	**Switch**: Reboot switch	Reboot the switch and enter into the extended boot menu by pressing **Ctrl+B** when prompted.
		Note: During this process, you may be prompted for additional input. Only respond with the input noted in this step; otherwise, let the system time out and continue automatically.
		`> reboot`
		`Start to check configuration with next startup configuration file, please wait.....DONE!N`
		`This command will reboot the device. Current configuration will be lost, save current configuration? [Y/N]: N`
		`This command will reboot the device. Continue? [Y/N]: Y`
		`#May 15 15:03:44:478 2015 HP6125G_IOBAY5 DEVM/1/REBOOT:`
		`Reboot device by command.`
		`%May 15 15:03:44:570 2015 HP6125G_IOBAY5 DEVM/5/SYSTEM_REBOOT: System is rebooting now.`
		`System is starting...`
		`Press Ctrl+D to access BASIC BOOT MENU`
		`Press Ctrl+T to start memory test`
		`Booting Normal Extend BootWare`
		`The Extend BootWare is self-decompressing.....Done!`
		`[ OUTPUT REMOVED ]`
		`BootWare Validating...`
		`Backup Extend BootWare is newer than Normal Extend BootWare,Update? [Y/N]`
		`Press Ctrl+B to enter extended boot menu...`
		`BootWare password: Not required. Please press Enter to continue.`
		`[ OUTPUT REMOVED ]`

Step #	Procedure	Description
10. 	**Switch**: Access File Control menu	Select **4** to access the file control from the extend-bootware menu. ==========<EXTEND-BOOTWARE MENU>========== |<1> Boot System | |<2> Enter Serial SubMenu | |<3> Enter Ethernet SubMenu | |<4> File Control | |<5> Restore to Factory Default Configuration | |<6> Skip Current System Configuration | |<7> BootWare Operation Menu | |<8> Clear Super Password | |<9> Storage Device Operation | |<0> Reboot | ========== Ctrl+Z: Access EXTEND-ASSISTANT MENU Ctrl+C: Display Copyright Ctrl+F: Format File System Enter your choice(0-9): 4

Step #	Procedure	Description

11.	**Switch**: Identify target firmware	Select **1** from the file control menu to list all files and identify the target firmware from the list.
		`======================<File CONTROL>=======================`
		`|Note:the operating device is flash |`
		`|<1> Display All File(s) |`
		`|<2> Set Application File type |`
		`|<3> Delete File |`
		`|<0> Exit To Main Menu |`
		`============================================================`
		`Enter your choice(0-3): 1`
		`Display all file(s) in flash:`
		`'M' = MAIN 'B' = BACKUP 'S' = SECURE 'N/A' = NOT ASSIGNED`
		`============================================================`
		`|NO. Size(B) Time Type Name |`
		`|1 1584 Aug/27/2015 18:41:08 N/A private-data.txt |`
		`|2 151 Aug/27/2015 18:41:08 N/A system.xml |`
		`|3 3626 Aug/27/2015 18:41:09 M config.cfg |`
		`|4 16493888 Aug/20/2015 11:14:44 M+B 6125-cmw520-r2106.bin |`
		`|5 4 Apr/26/2000 07:00:52 N/A snmpboots |`
		`|6 16913408 Aug/20/2015 10:56:42 N/A 6125-cmw520-r2112.bin |`
		`|7 735 Apr/26/2000 12:04:14 N/A hostkey_v3 |`
		`|8 591 Apr/26/2000 12:04:15 N/A serverkey_v3 |`
		`|9 16166 Sep/05/2013 10:17:21 N/A test |`
		`|10 16053376 Jun/05/2012 10:14:37 N/A ~/6125-cmw520-r2103.bin |`
		`|11 16479296 Apr/26/2000 10:31:54 N/A ~/6125-cmw520-r2105.bin |`
		`|12 16493888 Apr/26/2000 10:59:10 N/A ~/6125-cmw520-r2106.bin |`
		`|13 16479296 Nov/05/2013 23:24:06 N/A ~/2105.bin |`
		`|14 5361 Jun/25/2013 14:22:05 N/A ~/config.cfg |`
		`|15 16493888 Nov/05/2013 23:20:13 N/A ~/2106.bin |`
		`|16 1048519 Aug/27/2015 23:30:55 N/A logfile/logfile.log |`
		`|17 735 Apr/26/2000 12:05:10 N/A hostkey |`
		`|18 591 Apr/26/2000 12:05:11 N/A serverkey |`
		`============================================================`
		`[ OUTPUT REMOVED ]`

12.	**Switch**: Set application file type	Select **2** from the file control menu to set the application file type.
		`======================<File CONTROL>=======================`
		`|Note:the operating device is flash |`
		`|<1> Display All File(s) |`
		`|<2> Set Application File type |`
		`|<3> Delete File |`
		`|<0> Exit To Main Menu |`
		`============================================================`
		`Enter your choice(0-3): 2`

Step #	Procedure	Description
13.	**Switch**: Select file	Select the firmware file identified in step 11. and enter the corresponding line number. 'M' = MAIN 'B' = BACKUP 'S' = SECURE 'N/A' = NOT ASSIGNED ========== |NO. Size(B) Time Type Name | |1 16493888 Aug/20/2015 11:14:44 M+B 6125-cmw520-r2106.bin | |2 16913408 Aug/20/2015 10:56:42 N/A 6125-cmw520-r2112.bin | |3 16053376 Jun/05/2012 10:14:37 N/A ~/6125-cmw520-r2103.bin | |4 16479296 Apr/26/2000 10:31:54 N/A ~/6125-cmw520-r2105.bin | |5 16493888 Apr/26/2000 10:59:10 N/A ~/6125-cmw520-r2106.bin | |6 16479296 Nov/05/2013 23:24:06 N/A ~/2105.bin | |7 16493888 Nov/05/2013 23:20:13 N/A ~/2106.bin | |0 Exit | ========== Enter file No: <4>
14.	**Switch**: Modify file attribute	Select **1** from the file attributes menu to modify the file attribute to **+Main**. Modify the file attribute: ========== |<1> +Main | |<2> -Main | |<3> +Backup | |<4> -Backup | |<0> Exit | ========== Enter your choice(0-4): 1 This operation may take several minutes. Please wait.... Set the file attribute success!

Step #	Procedure	Description

15.	**Switch**: Verify change	Select **1** from the file control menu to verify the file attribute modification by listing the files and inspecting the **type** attribute for the target firmware. The type attribute on this line should display **M**:
		`======================<File CONTROL>=========================`
		`|Note:the operating device is flash |`
		`|<1> Display All File(s) |`
		`|<2> Set Application File type |`
		`|<3> Delete File |`
		`|<0> Exit To Main Menu |`
		`============================================================`
		`Enter your choice(0-3): 1`
		`Display all file(s) in flash:`
		`'M' = MAIN 'B' = BACKUP 'S' = SECURE 'N/A' = NOT ASSIGNED`
		`|NO. Size(B) Time Type Name |`
		`|1 1584 Aug/27/2015 18:41:08 N/A private-data.txt |`
		`|2 151 Aug/27/2015 18:41:08 N/A system.xml |`
		`|3 3626 Aug/27/2015 18:41:09 M config.cfg |`
		`|4 16493888 Aug/20/2015 11:14:44 B 6125-cmw520-r2106.bin |`
		`|5 4 Apr/26/2000 07:00:52 N/A snmpboots |`
		`|6 16913408 Aug/20/2015 10:56:42 N/A 6125-cmw520-r2112.bin |`
		`|7 735 Apr/26/2000 12:04:14 N/A hostkey_v3 |`
		`|8 591 Apr/26/2000 12:04:15 N/A serverkey_v3 |`
		`|9 16166 Sep/05/2013 10:17:21 N/A test |`
		`|10 16053376 Jun/05/2012 10:14:37 N/A ~/6125-cmw520-r2103.bin |`
		`|11 16479296 Apr/26/2000 10:31:54 M ~/6125-cmw520-r2105.bin |`
		`|12 16493888 Apr/26/2000 10:59:10 N/A ~/6125-cmw520-r2106.bin |`
		`|13 16479296 Nov/05/2013 23:24:06 N/A ~/2105.bin |`
		`|14 5361 Jun/25/2013 14:22:05 N/A ~/config.cfg |`
		`|15 16493888 Nov/05/2013 23:20:13 N/A ~/2106.bin |`
		`|16 1048519 Aug/27/2015 23:30:55 N/A logfile/logfile.log |`
		`|17 735 Apr/26/2000 12:05:10 N/A hostkey |`
		`|18 591 Apr/26/2000 12:05:11 N/A serverkey |`
		`============================================================`

16.	**Switch**: Exit	Select **0** from the file control menu to Exit to the main menu.
		`======================<File CONTROL>=========================`
		`|Note:the operating device is flash |`
		`|<1> Display All File(s) |`
		`|<2> Set Application File type |`
		`|<3> Delete File |`
		`|<0> Exit To Main Menu |`
		`============================================================`
		`Enter your choice(0-3): 0`

Step #	Procedure	Description

17.	**Switch**: Boot the system	Select **1** from the extend-bootware menu to Boot the system.
		Note: Do NOT select reboot by choosing **0**!
		Note: During this process, you may be asked for additional input. Only respond with the input noted in this step; otherwise, let the system time out and continue automatically.
		`==================<EXTEND-BOOTWARE MENU>==================`
		`|<1> Boot System |`
		`|<2> Enter Serial SubMenu |`
		`|<3> Enter Ethernet SubMenu |`
		`|<4> File Control |`
		`|<5> Restore to Factory Default Configuration |`
		`|<6> Skip Current System Configuration |`
		`|<7> BootWare Operation Menu |`
		`|<8> Clear Super Password |`
		`|<9> Storage Device Operation |`
		`|<0> Reboot |`
		`==========`
		`Ctrl+Z: Access EXTEND-ASSISTANT MENU`
		`Ctrl+C: Display Copyright`
		`Ctrl+F: Format File System`
		`Enter your choice(0-9): 1`
		`Starting to get the main application file--flash:/~/6125-cmw520-r2105.bin!.....`
		`The main application file is self-decompressing.....`
		`[ OUTPUT REMOVED ]`
		`.....Done!`
		`System application is starting...`
		`User interface aux0 is available.`
		`Press ENTER to get started.`
		`Login authentication`
		`Username:`

Step #	Procedure	Description

18. ☐	**Switch**: Login	Log back into the switch and verify the firmware version by executing the **display version** command.
		Note: You may have to press **Enter** multiple times after authenticating to land on the switch prompt.
		`Username: username [Enter]`
		`Password: password [Enter] [Enter]`
		`#Aug 28 09:29:09:694 2015 HP6125g_sanity SHELL/4/LOGIN: Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1:plat login from Console`
		`%Aug 28 09:29:09:819 2015 HP6125g_sanity SHELL/5/SHELL_LOGIN: plat logged in from aux0.`
		`> display version`
		`HP Comware Platform Software`
		`Comware Software, Version 5.20.99, Release 2105`
		`Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.`
		`HP 6125G Blade Switch uptime is 0 week, 0 day, 0 hour, 9 minutes`
		`[ OUTPUT REMOVED ]`

19. ☐	**Switch**: Disconnect from the switch	Gracefully disconnect from the switch serial console by pressing **Ctrl +** _ (Control + Shift + Underscore).
		`> '<Ctrl>_' (Control + Shift + Underscore)`
		`----------`
		`Command: D)isconnect, C)hange settings, send B)reak, E)xit command mode X)modem`
		`send > D`
		`----------`
		`D [Enter]`

20. ☐	**Active OA**: Logout	Log out of the OA. `> logout`

Appendix M. Configure Speed and Duplex for 6125XLG LAG Ports (netConfig)

Procedure 10. Configure Speed and Duplex for 6125XLG LAG Ports (netConfig)

Step #	Procedure	Description
This utility procedure is only for use with 1 GE LAG ports from HP 6125XLG enclosure switches to Cisco 4948/E/-F product aggregation switches or the cutomer network. Configuring speed and duplex on the LAG ports turns off auto-negotiation for the individual links, and must be performed on both switches for all participating LAG links. This procedure addresses a known weakness with auto-negotiation on 1GE SFPs and the 6125XLG which causes 1GE links to take longer than expected to become active. ***Note***: Do not use this procedure for 6125 switches. See Appendix L for the correct procedure for that switch. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		

1. ☐	**Virtual PMAC**: List aggregation groups	List configured link aggregation groups on the 6125XLG enclosure switch. Capture the LAG ID connected to the 4948/E/E-F product aggregation switch or the customer network. In the following example, LAG ID 1 is identified as the 4x1GE LAG requiring speed and duplex configuration.
		`[admusr@exapmle~]$ sudo netConfig --device=<switch_hostname> listLinkAggregations`
		`LAG: 1`

2. ☐	**Virtual PMAC**: : List interfaces	Get the list of interfaces configured for the LAG on the 6125XLG. In the following example, LAG ID 1 is inspected and shown to include interfaces tenGE17-20.
		`[admusr@exapmle~]$ sudo netConfig --device=<switch_hostname> getLinkAggregation`
		`id=1`
		`Type: Dynamic`
		`Description: ISL_to_agg_switch`
		`Switchport: =(`
		`link-type trunk`
		`vlan all`
		`)`
		`Interfaces: =(`
		`tenGE17`
		`tenGE18`
		`tenGE19`
		`tenGE20`
		`)`

3. ☐	**Virtual PMAC**: : Set speed and duplex	Inspect the switch LAG port configurations and verify speed and duplex are set on the LAG interfaces, as shown in this example:
		`[admusr@exapmle~]$ sudo netConfig --device=<switch_hostname>`
		`setSwitchportinterface=tenGE17-20 speed=1000 duplex = full`

Step #	Procedure	Description

4.	**Virtual PMAC**: : Verify speed and duplex	Inspect the switch LAG port configurations and verify speed and duplex are set on the LAG interfaces, as shown in this example:
		`[admusr@exapmle~]$ sudo netConfig --device=<switch_hostname>`
		`getSwitchportinterface=tenGE17-20`
		`Switchport: trunk`
		`Description: Ten-GigabitEthernet1/1/5 Interface`
		`Speed: 1000Mbps`
		`Duplex: full`
		`VLAN =(`
		`1(default`
		`2-4094`
		`)`
		`Default VLAN: 1`

Appendix N. RPM Installation of Switch 6127XLG for PMAC

This section provides the procedure to download the required patch and install RPMs.

1. To retrieve RPMs, do the following:
    a. Go to My Oracle Support (http://support.oracle.com/).
    b. Download the following patch:

```
Patch: 34319403 - Patch for Oracle Communications DSR 8.6.0.1.0 PMAC 6.7 netconfig 3.7.0


Platform    = Tekelec
Product     = Oracle Communications Diameter Signaling Router (DSR)
Version     = 8.6.0.1.0
```

    c. When the patch is downloaded, extract the zip file to retrieve the following files:

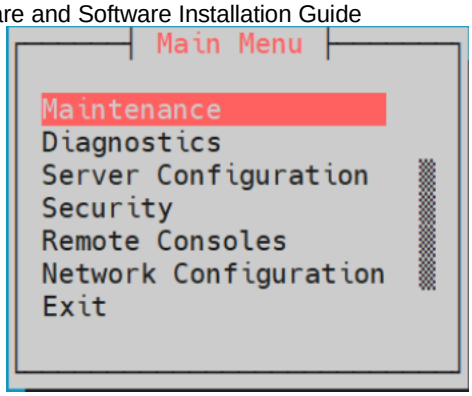
- README.txt
- TKLCnetwork-config-3.7.0-0.67694.x86_64.rpm
- TKLCnetwork-config-templates-3.7.0-0.67694.noarch.rpm
- TKLCnetwork-config-utilities-3.7.0-0.67694.noarch.rpm

Note: One of the Oracle Server patches is not subject to the same rigorous level of testing as done for Oracle Server patch sets. Operator can choose to install and test this patch in a test environment prior to full production implementation.

2. To install the RPMs, do the following:
    a. Copy the retrieved rpm files to the following PMAC path: `/var/TKLC/upgrade/patch/`
    b. In the PMAC Linux terminal, run the following command:

```
sudo su – platcfg
```

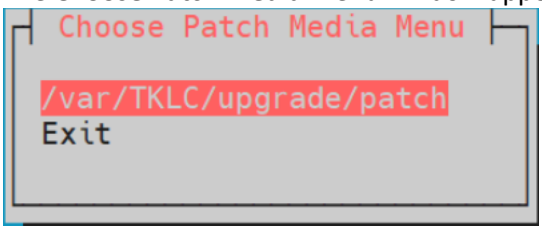
The **Main Menu** window appears.



c. Select **Maintenance**, and then **Patching.**

d. Click **Initiate Patch**.

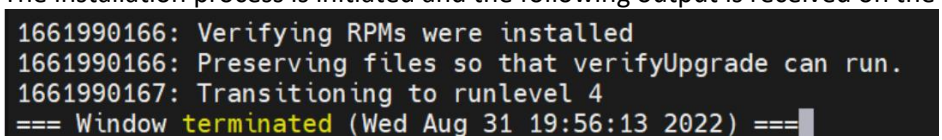
The **Choose Patch Media** Menu window appears.



e. Select `/var/TKLC/upgrade/patch`.

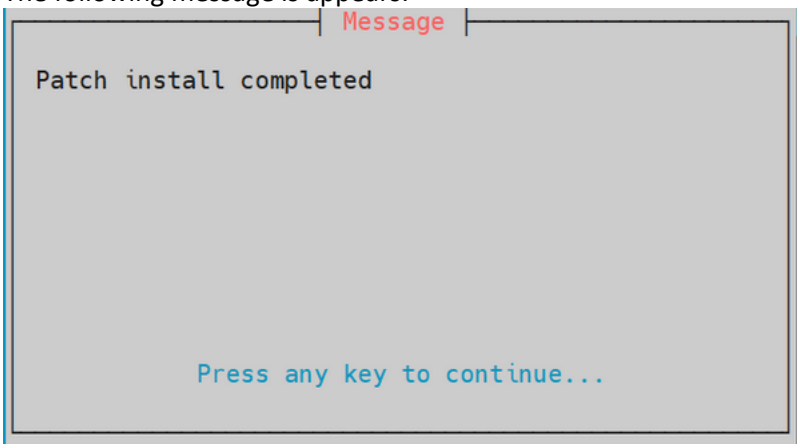
f. Select **NO** in the next two windows.

The installation process is initiated and the following output is received on the terminal.



g. To close the terminal, enter **q**. This task might exit from vim.

The following message is appears:



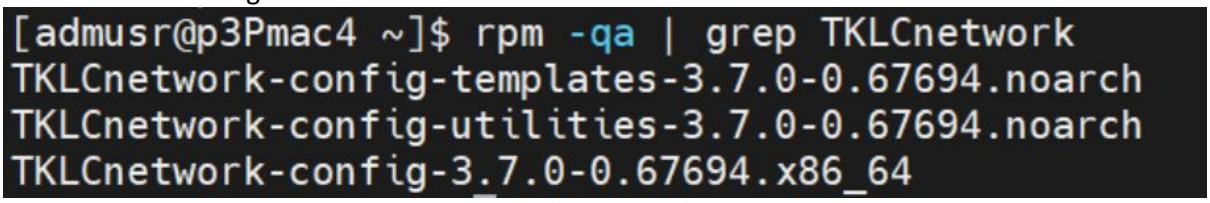
h. Press any key to continue, and then select **exit** until it returns to the command line.

When it is complete, the support to the switch 6127XLG is enabled.

3. To verify the installation, run the following command:

```
rpm -qa | grep TKLCnetwork
```

The following aforementioned RPMs are listed.



Netconfig 6127XLG support

Netconfig is a PMAC tool that can be used to configure network devices. This section describes how to add support to a new switch model and usage of the new support.

Initialization and Configuration of Switch 6127XLG

Netconfig is initialized through an init netconfig file.

- To initialize, run the following command:
  `sudo netConfig --file=/usr/TKLC/smac/etc/switch/xml/6127XLG_<device_name>_init.xml`
- To configure, run the following command:
  `sudo netConfig --file=/usr/TKLC/smac/etc/switch/xml/6127XLG_<device_name>_configure.xml`

Note: The init and configure xml files are composed to contain all the corresponding configurations required for DSR traffic.

6127XLG Templates

The templates are located at `/usr/TKLC/plat/etc/TKLCnetwork-config-templates/templates/init/Enclosure/`. In this case the device must be changed for the device network hostname.

Example for 6127XLG_<device_name>_init.xml:

```
<!-- TKLCnetwork-config-templates-3.5.0 -->
<configure apiVersion="1.1">
<procedure mode="init" access="oob">
        <!-- 6127XLG Initialization Template File -->
        <name>6127XLG Switch Initialization File</name>
        <device>6127</device>
</procedure>
</configure>
```

Example for 6127XLG_<device_name>_configure.xml:

```
<!-- TKLCnetwork-config-templates-2.0.9 -->
<configure>
<procedure>
        <!-- 6127XLG Layer 2 Template File -->
<!-- Begin 6127XLG -->
        <!-- Hostname must not exceed 20 characters -->
        <device> name_6127XLG_xyz </device>

        <!-- GENERAL SWITCH SECTION -->

        <!-- set the clock -->
        <task>
        <command>setClock</command>
        <!-- 'name' option has been removed, timezone is UTC with offset -->
        <option name="offsetHour">0</option>
        </task>

        <!-- This enables and configures NTP parameters -->
        <task>
        <command>addNTP</command>
        <option name="server">10.31.128.254</option>
        </task>
        <!-- This only configures the SNMP community info, other SNMP "commands"
are needed -->
        <task>
```

```
        <command>addSNMP</command>
        <option name="community">tklcuser</option>
        </task>

        <!-- This configures the SNMP server to send informs/traps to -->
        <task>
        <command>addSNMPNotify</command>
        <!-- If host is specified, then auth aka community name must be specified
-->
        <option name="host">10.155.225.10</option>
        <option name="auth">tklcuser</option>
        <!-- Not required options -->
        <option name="version">2c</option>
        <!-- Enables all of the Platform 6 supported SNMP traps -->
        <option name="trap">Plat6</option>
        </task>

        <!-- This configures STP on the device -->
        <task>
        <command>enableSTP</command>
        <option name="type">rstp</option>
        <option name="vlanSTP">1 to 4094</option>
        <!-- This must be a multiple of 4096 -->
        <option name="priority">53248</option>
        </task>
<!--
        <task>
        <command>addRemoteLogging</command>
        <option name="server">$logging_server_ip</option>
        </task>
-->
        <!-- CREATE VLANS SECTION -->
        <!-- Control vlan creation -->
        <task>
        <command>addVlan</command>
        <option name="name">control</option>
        <option name="id">1</option>
        </task>

        <!-- Platform management vlan creation -->
        <task>
        <command>addVlan</command>
        <option name="name">management</option>
        <option name="id">3030</option>
        </task>

        <!-- APPNET1 vlan creation -->
        <task>
        <command>addVlan</command>
        <option name="name">IMI</option>
        <option name="id">4</option>
        </task>

        <!-- APPNET2 vlan creation -->
        <task>
        <command>addVlan</command>
        <option name="name">XSI-1</option>
        <option name="id">3031</option>
        </task>
        <!-- APPNET3 vlan creation -->
        <task>
        <command>addVlan</command>
        <option name="name">XSI-2</option>
```

```
        <option name="id">3032</option>
        </task>

        <!-- CREATE SWITCHPORTS & LAG SECTION -->

        <!-- ISL to mate switch -->
        <task>
        <command>addLinkAggregation</command>
        <option name="id">1</option>
        <option name="description">ISL_to_agg_switch</option>
        <!-- Default LAG Mode: Active.  Uncomment the below line to use a static
LAG -->
        <!-- <option name="mode">static</option> -->
        </task>

        <task>
        <command>setLinkAggregation</command>
        <option name="id">1</option>
        <option name="description">ISL_to_agg_switch</option>
        <option name="interface">GE19-22</option>
        <!-- User can define access or trunk for access option -->
        <option name="access">trunk</option>
        <option name="vlanMembership">1 to 4094</option>
        </task>

        <task>
        <command>addSTP</command>
        <option name="interface">LAG1</option>
        <option name="edgeport">yes</option>
        </task>

        <!-- The following command DISABLES BPDUs on the uplink port -->
        <!-- If the customer does not allow BPDUs (STP) on their network -->
        <!-- and there are no TKLC aggregation switches in this deployment -->
        <!-- then uncomment the following command and there are no -->
        <!--aggregation switches in this deployment, otherwise -->
        <!-- leave as it is! -->

        <!--
         <task>
         <command>addSTP</command>
         <option name="interface">LAG1</option>
         <option name="bpduFilter">on</option>
         </task>
        -->



        <!-- CREATE SWITCHPORTS SECTION -->
        <!-- Ethernet Management Interface -->
        <task>
        <command>setSwitchport</command>
        <option name="interface">management</option>
        <option name="linkstate">up</option>
        </task>

        <!-- Connection to enclosure blades -->
        <task>
        <command>setSwitchport</command>
        <option name="interface">GE1-16</option>
        <option name="description">bayX.ethY</option>
        <!-- User can define access or trunk for type option -->
        <option name="type">trunk</option>
        <!-- Multiple VLANs can be entered by stringing the VLANs in the
```

```
vlanMembership option Ex. 1 to 5 or 1 2 3 4 5 -->
        <option name="vlanMembership">1 to 4094</option>
        <!-- Uncomment the next line for a Tagged Control Vlan Deployment -->
        <!-- <option name="vlanDefault">$control_vlan_id</option> -->
        <option name="linkstate">up</option>
        </task>

        <task>
        <command>addSTP</command>
        <option name="interface">GE1-16</option>
        <option name="edgeport">yes</option>
        </task>

        <!-- Unused Ports -->

        <task>
        <command>setSwitchport</command>
        <option name="interface">GE17-18</option>
        <option name="description">unused</option>
        <!-- User can define access or trunk for type option -->
        <option name="type">access</option>
        <option name="vlanMembership">1 to 4094</option>
        <option name="linkstate">down</option>
        </task>
        <task>
        <command>setSwitchport</command>
        <option name="interface">tenGE1-2</option>
        <option name="description">unused_shutdown</option>
        <!-- User can define access or trunk for type option -->
        <option name="type">access</option>
        <option name="linkstate">down</option>
        </task>

        <task>
        <command>setSwitchport</command>
        <option name="interface">tenGE17</option>
        <option name="description">unused_shutdown</option>
        <!-- User can define access or trunk for type option -->
        <option name="type">access</option>
        <option name="linkstate">down</option>
        </task>

        <!-- CREATE LINK STATE TRACKING SECTION -->

        <task>
        <command>enableLinkStateTracking</command>
        <option name="id">1</option>
        <option name="interface">LAG1</option>
        </task>

        <task>
        <command>addLinkStateTracking</command>
        <option name="id">1</option>
        <option name="interface">GE1-16</option>
        </task>

        <!-- Uncomment the following section if the management interface is IPv6
-->
        <!-- IPV6 ROUTING -->
        <!-- $ip6_remote_network_id_with_prefix should look like this
IPv6address/prefix  -->
        <!-- If the nexthop is a link-local address (FE80::XYZ) specify a link-
local interface with the network option as seen below: -->
```

```
        <!-- address/prefix%mgmt -->
        <!-- <task>
        <command>addRoute</command>
        <option name="network">$ip6_remote_network_id_with_prefix</option>
        <option name="nexthop">$ip6_next_hop_gateway</option>
        </task> -->
        <!-- End 6125G -->
</procedure>
</configure>
```

Note: The **6127XLG_<device_name>_configure.xml** configuration files are composed according to the topology used. The templates are located at **/usr/TKLC/plat/etc/TKLCnetwork-config-templates/templates/config**

Run the following command to view this topology.

```
sudo ls /usr/TKLC/plat/etc/TKLCnetwork-config-templates/templates/config
Generic  Topo1  Topo2  Topo3  Topo4  Topo5  Topo6  Topo7  Topo8
```

Note: While configuring the network devices, update the proper values as required.

Appendix O. Operational Dependencies on Platform Account Passwords

This appendix describes the operational dependencies on platform account passwords to provide guidance in cases when the customer insists on modifying a default password. Note that changing passwords should be attempted only on systems that are fully configured and stable. Modifying passwords during system installation is strongly discouraged.

Procedure 10. Operational Dependencies on Platform Account Passwords

Step #	Procedure	Description
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**PMAC CLI**: Login	Login to PMAC as **admusr**
2. ☐	Backup of PMAC database	Execute steps 6. through 8. in Procedure 9 Configure PMAC Application.
3. ☐	Restore passwords	Execute the steps 4 through 9 (inclusive), in Procedure 1 of the *PMAC Disaster Recovery*, latest release.

Appendix O.1 PMAC Credentials for Communication with Other System Components

This section covers the credentials that can be changed using the PMAC updateCredentials utility and the Platform dependencies users must be aware of to keep PMAC fully functional. Only the credentials that PMAC considers to be user accessible are listed here.

- oaUSer

  PMAC uses these credentials to communicate with OAs for all enclosures it monitors. Therefore, all active OAs must be updated to have the new credentials and then the updateCredentials should be

used to match the credentials PMAC uses. Lastly, all enclosures already provisioned in the PMAC must be rediscovered.

- To update the credentials on the OA's, log into the active OA GUI. On the left hand side of the OA GUI, navigate to **Users/Authentication > Local Users > pmacadmin**. After supplying the new password, click on **Update User**.
- To update the credentials on the PMAC, execute the following on the UI:

```
$ sudo/usr/TKLC/smac/bin/updateCredentials --type=oaUser
```

- To rediscover an enclosure already provisioned in the PMAC inventory, log into the PMAC GUI and navigate to **Hardware** > **System Inventory** > **Cabinet XXX** > **Enclosure XXXXX** and click **Rediscover Enclosure**.

- tpdPlatCfg
  - To update the tpdPlatcfg credentials on the PMAC, log into the PMAC server shell with the rootcredentials and execute:

```
$ passwd
```

  - The Storage Configuration functionality on the PMAC uses the TPD platcfg credentials when communicating with its TVOE host. If the tpdPlatcfg credentials are changed on the PMAC TPD OS, it must also be changed on the PMAC application using this command.
  - To update the credentials on the PMAC, execute the following in the UI:

$sudo/usr/TKLC/smac/bin/updateCredentials--type=tpdPlatCfg

- tvoeUser

  TVOE administrator passwords need to be changed for all TVOE hosts PMAC is expected to communicate with and then the updateCredentials should be used to match the credentials PMAC uses. Note each time a new TVOE is installed its default password has to be updated to match.

  - To update the credentials, log into the TVOE UI with the admusr credentials and execute:

```
$ passwd
```

  - To update the credentials on the PMAC, execute the following on the UI:

```
$ sudo /usr/TKLC/smac/bin/updateCredentials --type=tvoeUser
```

- backupPassword

  PMAC backup images are encrypted. The passphrase to encrypt the backup files may be changed. This only changes the encryption for future backups; prior backups cannot be restored without changing to the original pass phrase as shown below. A restore task that fails with a "Failed to decrypt backup file" reason is an indication of this condition.

  - To update the passphrase on a PMAC, exceute the following in the UI:

```
$ sudo /usr/TKLC/smac/bin/updateCredentials --type=backupPassword
```

- remoteBackupUser

  If pmacop credentials are changed on a redundant PMAC, the updateCredentials should be used to match credentials the primary PMAC uses.

  - To update the credentials on a redundant PMAC, log into the redundant PMAC UI with the pmacop credentials and execute:

```
$ passwd
```

  - To update the credentials on the primary PMAC, execute the following in primary PMAC UI:

```
$ sudo /usr/TKLC/smac/bin/updateCredentials --type=remoteBackupUser
```

- oobUser

These credentials are used to communicate with the iLO of RMS, when no other credentials have been specified when the RMS was provisioned in PMAC. So the user has the option to modify this default password, or the RMS can be edited/added in the GUI with its specific credentials.

- To update the credentials on an RMS iLO, log into the iLO GUI and navigate to **Administration > User Administration**. Check the box next to root password and click the Edit button. After the password is changed, click **Update User**.
- To modify the default oobUser credentials on the PMAC, execute the following in the UI:

  ```
  $ sudo /usr/TKLC/smac/bin/updateCredentials --type=oobUser
  ```
- To add a RMS to PMAC system inventory with its unique iLO password, refer to 4.9.1 Add Rack Mount Server to PMAC System Inventory.
- To edit iLO password of a specific RMS already in PMAC system inventory, refer to Appendix O Edit Rack Mount Server in the PMAC System Inventory.

- tpdProvd
  - The tpdProvd credentials are used to allow tpdProvd communication between the PMAC and servers on its control network. The procedure for updating the tpdProvd password has changed as of PMAC 66.5.0. The user can now enter multiple passwords, which can be matched to one or more individual servers. The update of the password on the PMAC does not use the updateCredentials script in this case. It uses two new commands under the pmacadm cli interface: addProvdCredentials and deleteProvdCredentials.

Expected Behaviors

1. If a tpdProvd password is changed on a non-discovered provisioned server (seen in the Main Menu->Software=>Software Inventory page but no data is associated to it) on both the server side and the **PMAC side**, after a few minutes, the IPv6 address will appear in the “Address” field and the server will self discover. The server can also be fully discovered if that server is selected in the grid and the **Rediscover** button is selected.
2. If a tpdProvd password is changed on an existing discovered server but not updated on the **PMAC side**, that server will remain discovered in the Main Menu->Software->Software Inventory page until a **sentry restart** is performed. Once performed, the server will no longer show as discovered in the Software Inventory page. Once the tpdProvd password has been updated on the **PMAC**, the behavior in number 1 will occur.

Procedure

1. Update the password on a given server or group of servers (assuming all passwords are the same for the group) either using the linux passwd command on the server(s) or by some other means.
2. From a PMAC shell, use the following command to add the password(s) to the PMAC database and update the PMAC messaging interface. This command will prompt the user for the password and echo asterisks as characters are entered.

Note: --flushBAs can be set to "no" if entering multiple passwords and set to "yes" on the last password add. If --flushBAs is not set to "yes" on the last password entry, a **sentry restart** must be performed on the PMAC to flush out all the Broker Agents (server interfaces) in the PMAC messaging system and rebuild them using the new passwords.

```
/usr/bin/sudo /usr/TKLC/smac/bin/pmacadm addProvdCredentials --
flushBAs=yes
```

1. The new password can be verified using the following command (this should return a valid response with a password. If it fails, there may be a tpdProvd password mismatch issue betweent he PMAC and the server):

   ```
   /usr/bin/sudo /usr/TKLC/smac/bin/pmaccli getHostCommStr --
   ip=<ipv4 address of the server> --accessType=ro
   ```

2. If a password must be removed (and the exact spelling of the password is known), it can be deleted from the PMAC database and messaging system using the following command (again note that the user is prompted for the password):

   ```
   /usr/bin/sudo /usr/TKLC/smac/bin/pmacadm deleteProvdCredentials -
   -flushBAs=yes
   ```

Appendix O.2 GUI Account Credentials

Modification of any of the PMAC GUI accounts has no system impact.

Procedure 10. GUI account credentials

Step #	Procedure	Description
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**PMAC CLI**: Login	Login to PMAC as **admusr**
2. ☐	Select Users	Navigate to **Administration** > **Users.** Select the user from the first **Username** list and click **Set Password.**
3. ☐	Setting New Password	In Set Password window, enter the new password twice. Click **Continue.**

Appendix O.3 PMAC Linux User Account Credentials

Modification of any PMAC Linux user account has no system impact with the exception of the **pmacop** user and **admusr** credentials. If pmacop credentials are changed on a redundant PMAC, use the updateCredentials to match the credentials the primary PMAC uses. If admusr credentials are changed after configuration of the netconfig repository, then delete netconfig services and re-add using the new credentials.

- To update the pmacop credentials on a redundant PMAC, log into the redundant PMAC UI with the pmacop credentials and execute:

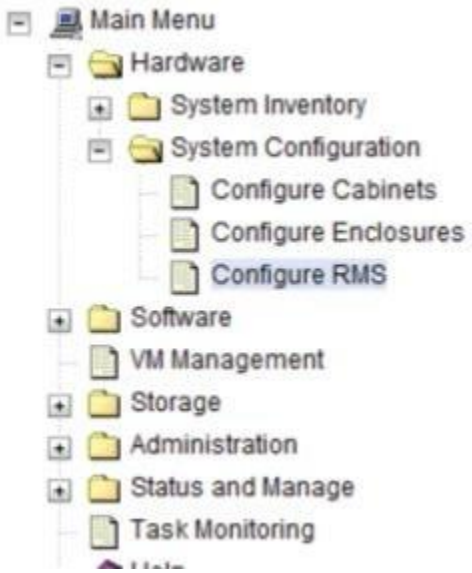
  ```
  $ passwd
  ```

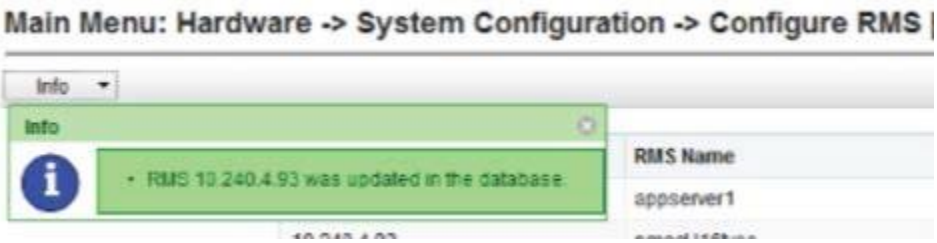
- To update the pmacop credentials the primary PMAC uses to communicate with the redundant PMAC, execute the following in primary PMAC UI:

  ```
  $ sudo /usr/TKLC/smac/bin/updateCredentials --type=pmacop
  ```

Appendix P. Edit Rack Mount Server in the PMAC System Inventory

Procedure 55. Edit Rack Mount Server in the PMAC System Inventory

Step #	Procedure	Description
This procedure edits a rack mount server in the PMAC system inventory. This option is used to modify the name, cabinet, or credentials of an already provisioned rack mount server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**PMAC GUI**: Login	Open web browser and enter: `https://<pmac_management_network_ip>` Login as pmacadmin user.
2. ☐	**PMAC GUI**: Navigate to Configure RMS	Navigate to **Hardware > System Configuration > Configure RMS**. 

Step #	Procedure	Description
3. ☐	**PMAC GUI**: Edit RMS	Select a row in the list of rack mount servers and click **Edit RMS**. Modify the field and click **Edit RMS**.
4. ☐	**PMAC GUI**: Check errors	If no errors are reported, the Info box states it is successful.  Or an error message displays:

Appendix Q. Increase the PMAC NetBackup File System Size

This appendix describes how to increase the PMAC NetBackup file system to accommodate upgrading to NetBackup 7.7 or greater. Currently, the recommended filesystem size for NetBackup 7.7 is 5GB. This filesystem is mounted to a logical volume maintained on the TVOE host.

Prerequisites:

- There is a volume defined on the TVOE host called `<pmac guest name>_netback.img` and set to 2GB.
- There is a filesystem on the PMAC guest at `/dev/<device_name>` mounted to `/usr/openv`' and sized to 2GB.
- The NetBackup filesystem on the PMAC must be type ext2/3/4.
- This procedure assumes there is an entry in the /etc/fstab file for the mounted /usr/openv filesystem.

Notes:

- The `<device_name>` used can differ from `/dev/vdd`. This can be determined by issuing the `df -h` command on the PMAC prior to starting this procedure and searching for the `/usr/openv` NetBackup filesystem. Once NetBackup has been enabled and configured on a PMAC, there should be a softlink defined, called `/dev/netbackup`, which points to the actual device. Usually this points to `/dev/vdd`. If that is available then all references to `/dev/vdd` can be replaced with `/dev/netbackup` and the user does not have to know what actual device is used for the filesystem. The procedure below assumes this to be true.
- The commands listed below require root access to execute them. `sudo` is used to elevate the user permissions to be able to execute the commands. Any command that is not prefixed with `sudo` does not require elevation to execute.
- All commands are executed from a PMAC shell or from a TVOE shell.
- Performing this procedure increases the size of the NetBackup filesystem to 5GB. You can use this procedure to increase the NetBackup volume to any size that can be accommodated by the TVOE host. 5GB is the required size for NetBackup 7.7.
- Each step in this procedure begins by identifying the target server on which the command is to be executed. In this procedure, commands are executed on either the TVOE host or the PMAC.

Procedure 10. Increase the PMAC NetBackup Files System Size

Step #	Procedure	Description
This procedure increases the PMAC NetBackup file system to accommodate upgrading to NetBackup 7.7 or greater. ***Note***: If you are attempting to uninstall a failed Symantec NetBackup client installation or upgrade, do not use this procedure. This procedure should only be used when the initial Symantec NetBackup client installation, or subsequent upgrade, is successful. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		
1. ☐	**TVOE Host**: Login	Connect to the management server's TVOE host shell and log into the PMAC shell as **admusr** using ssh.

<table>
<tr><th>Step #</th><th>Procedure</th><th>Description</th></tr>
<tr><td>2.
</td><td>TVOE Host:
Verfiy existing volume</td><td>Verify the existing TVOE NetBackup volume is set to 2GB.
1. Display the logical volume sizes.
<pre>[admusr@<tvoe_host> ~]$ /usr/bin/sudo /sbin/lvs
LV   VG   Attr   LSize
<pmac_guest>.img   vgguests   -wi-ao----   50.00g
<pmac_guest>_images.img   vgguests   -wi-ao----   20.00g
<pmac_guest>_logs.img   vgguests   -wi-ao----   10.00g
<pmac_guest>_netbackup.img   vgguests   -wi-ao----   2.00g
plat_root   vgroot   -wi-ao----   768.00m
plat_swap   vgroot   -wi-ao----   2.00g
plat_tmp   vgroot   -wi-ao----   1.00g
plat_usr   vgroot   -wi-ao----   3.00g
plat_var   vgroot   -wi-ao----   1.00g</pre>
2. Display the logical volume details.
<pre>[admusr@<tvoe_host> ~]$ /usr/bin/sudo /sbin/lvdisplay
/dev/vgguests/<pmac_guest>_netbackup.img
--- Logical volume ---
LV Path   /dev/vgguests/<pmac_guest>_netbackup.img
LV Name   <pmac_guest>_netbackup.img
VG Name   vgguests
LV UUID   CWe1Nl-ln6r-22Tv-5B0p-Xj4F-44dM-SyGUwp
LV Write Access   read/write
LV Creation host, time <tvoe_host>, 2016-11-14 10:00:54 -0500
LV Status   available
open   1
LV Size   2.00 GiB
Current LE   64
Segments   1
Allocation   inherit
Read ahead sectors   auto
- currently set to   4096
Block device   253:19</pre></td></tr>
<tr><td>3.
</td><td>PMAC:
Verify filesystem</td><td>Verify the NetBackup filesystem is set to 2GB.
<pre>[admusr@<pmac_guest> ~]$ /bin/df -h /usr/openv
Filesystem   Size Used Avail Use% Mounted on
/dev/vdd   2.0G 69M   2.3G   1%   /usr/openv</pre></td></tr>
<tr><td>4.
</td><td>TVOE Host:
Resize volume</td><td>Resize the NetBackup volume from 2GB to 5GB.
<pre>[admusr@<tvoe_host> ~]$ usr/bin/sudo /sbin/lvextend --size
5G /dev/vgguests/<pmac_guest>_netbackup.img
Size of logical volume vgguests/<pmac_guest>_netbackup.img
changed from 2.00 GiB (64 extents) to 5.00 GiB (160
extents).
Logical volume <pmac_guest>_netbackup.img successfully
resized</pre></td></tr>
</table>

<table>
<tr><th>Step #</th><th>Procedure</th><th>Description</th></tr>
<tr><td>5.
</td><td>TVOE Host:
Verify increase</td><td>Verify the size of the volume has increased to 5GB.
1. Display the logical volume sizes.
<pre>[admusr@<tvoe_host> ~]$ /usr/bin/sudo /sbin/lvs
LV   VG   Attr   LSize
<pmac_guest>.img   vgguests   -wi-ao----   50.00g
<pmac_guest>_images.img   vgguests   -wi-ao----   20.00g
<pmac_guest>_logs.img   vgguests   -wi-ao----   10.00g
<pmac_guest>_netbackup.img vgguests   -wi-ao----   5.00g
plat_root   vgroot   -wi-ao----   768.00m
plat_swap   vgroot   -wi-ao----   2.00g
plat_tmp   vgroot   -wi-ao----   1.00g
plat_usr   vgroot   -wi-ao----   3.00g
plat_var   vgroot   -wi-ao----   1.00g</pre>
2. Display the logical volume details.
<pre>[admusr@<tvoe_host> ~]$ /usr/bin/sudo /sbin/lvdisplay
/dev/vgguests/<pmac_guest>_netbackup.img
--- Logical volume ---
LV Path   /dev/vgguests/<pmac_guest>_netbackup.img
LV Name   <pmac_guest>_netbackup.img
VG Name   vgguests
LV UUID   CWe1Nl-ln6r-22Tv-5B0p-Xj4F-44dM-SyGUwp
LV Write Access   read/write
LV Creation host, time <tvoe_host>, 2016-11-14 10:00:54 -
0500 LV Status   available
open   1
LV Size   5.00 GiB
Current LE   64
Segments   1
Allocation   inherit
Read ahead sectors   auto
- currently set to   4096
Block device   253:19</pre></td></tr>
<tr><td>6.
</td><td>PMAC:
Verify filesystem</td><td>Verify the space on the PMAC NetBackup filesystem has not changed.
<pre>[admusr@<pmac_guest> ~]$ /bin/df -h /usr/openv
Filesystem   Size Used Avail Use% Mounted on
/dev/vdd   2.0G 69M   2.3G   1%   /usr/openv</pre></td></tr>
</table>

Step #	Procedure	Description

7. ☐	**TVOE Host**: Verify PMAC is aware of volume size increase	Ensure the PMAC is made aware of the volume size increase.
		1. Identify the PMAC guest using the **virrsh** command.
		`[admusr@<tvoe_host> ~]$ /usr/bin/sudo /usr/bin/virsh list --all`
		`Id  Name  State`
		`----------`
		`86  <pmac_guest>  running`
		2. Shut down the PMAC guest.
		`[admusr@<tvoe_host> ~]$ /usr/bin/sudo /usr/bin/virsh shutdown <pmac_guest>`
		`Domain <pmac_guest> is being shutdown`
		3. Wait for the PMAC shutdown to complete. If the State is **running**, repeat the command until it indicates the State is **shut off**.
		`[admusr@<tvoe_host> ~]$ /usr/bin/sudo /usr/bin/virsh list --all`
		`Id  Name  State`
		`----------`
		`86  <pmac_guest>  shut off`
		4. Once shutdown is complete, restart the PMAC.
		`[admusr@<tvoe_host> ~]$ /usr/bin/sudo /usr/bin/virsh start <pmac_guest>`
		`Domain <pmac_guest> started`
		5. Verify the PMAC has completed the restart. This can be checked by executing the command **sudo virsh console <pmac_guest>** and checking for the PMAC guest login prompt.
		Once the escape character is displayed, press **Enter** once more to reach the login prompt.
		Afterwards, press **Ctrl-]** to exit the PMAC login prompt and return to the TVOE host prompt.
		`[admusr@<tvoe_host> ~]$ /usr/bin/sudo /usr/bin/virsh console <pmac_guest>`
		`Connected to domain <tvoe_host>`
		`Escape character is ^]`

8. ☐	**PMAC**: Verify volume size	Verify the volume size increase is 5GB as seen from the PMAC.
		`[admusr@<pmac_guest> ~]$ /usr/bin/sudo admusr /sbin/fdisk -l /dev/netbackup`
		`Disk /dev/netbackup: 5368 MB, 5368709120 bytes`
		`16 heads, 63 sectors/track, 10402 cylinders`
		`Units = cylinders of 1008 * 512 = 516096 bytes`
		`Sector size (logical/physical): 512 bytes / 512 bytes`
		`I/O size (minimum/optimal): 512 bytes / 512 bytes`
		`Disk identifier: 0x00000000`

Step #	Procedure	Description

9. ☐	**PMAC**: Resize filesystem	Resize the PMAC NetBackup filesystem to 5GB.
		1. Verify the filesystem is still mounted by issuing the mount command and looking for /dev/vdd mounted on /usr/openv.
		`[admusr@<pmac_guest> ~]$ /bin/mount`
		`/dev/mapper/vgroot-plat_root on / type ext4 (rw)`
		`proc on /proc type proc (rw)`
		`sysfs on /sys type sysfs (rw)`
		`devpts on /dev/pts type devpts (rw,gid=5,mode=620)`
		`tmpfs on /dev/shm type tmpfs (rw)`
		`/dev/vda1 on /boot type ext4 (rw)`
		`/dev/mapper/vgroot-plat_tmp on /tmp type ext4 (rw)`
		`/dev/mapper/vgroot-plat_usr on /usr type ext4 (rw)`
		`/dev/mapper/vgroot-plat_var on /var type ext4 (rw)`
		`/dev/mapper/vgroot-plat_var_tklc on /var/TKLC type ext4 (rw)`
		`/dev/mapper/vgroot-smac_root on /usr/TKLC/smac type ext4 (rw)`
		`/dev/mapper/vgroot-smac_var on /var/TKLC/smac type ext4 (rw)`
		`/dev/mapper/vgroot-smac_backup on /var/TKLC/smac/backup type ext4 (rw)`
		`/dev/mapper/vgroot-smac_isoimages on /var/TKLC/smac/image/isoimages type ext4 (rw)`
		`/var/TKLC/smac/image/core on /var/TKLC/core type none (rw,bind)`
		`/dev/vdb on /var/TKLC/smac/logs type ext3 (rw)`
		`/dev/vdc on /var/TKLC/smac/image/repository type ext3 (rw)`
		`none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)`
		`sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)`
		`nfsd on /proc/fs/nfsd type nfsd (rw)`
		`/dev/vdd on /usr/openv type ext3 (rw)`
		2. Unmount the NetBackup filesystem. The **umount** command can be verified by issuing the **mount** command again. The **/usr/openv** filesystem should not be displayed as in the previous command.
		Note: There **umount** command does not generate output upon success.
		`[admusr@<pmac_guest> ~]$ /usr/bin/sudo /bin/umount /usr/openv`
		3. Execute the **e2fsck** command to make sure the NetBackup filesystem is clean.
		`[admusr@<pmac_guest> ~]$ /usr/bin/sudo /sbin/e2fsck /dev/netbackup`
		`e2fsck 1.43-WIP (20-Jun-2013)`
		`/dev/netbackup: clean, 11/327680 files, 37999/1310720 blocks`
		4. Execute the **resize2fs** command to resize the filesystem and map it to the 5GB size of the disk volume on the TVOE host. If the size attribute is not

Step #	Procedure	Description

		included in the command, the NetBackup filesystem resizes to the total free space on the TVOE host volume. This should be 5GB since there should not be any other filesystems mounted to this volume. If the **resize2fs** command returns an indication that the **e2fsck** command must be executed on the NetBackup filesystem, then re-execute that command.
		`[admusr@<pmac_guest> ~]$ /usr/bin/sudo /usr/bin/resize2fs /dev/netbackup`
		`resize2fs 1.43-WIP (20-Jun-2013)`
		`Resizing the filesystem on /dev/netbackup to 1310720 (4k) blocks.`
		`The filesystem on /dev/netbackup is now 1310720 blocks long.`
		5. Re-mount the **/usr/openv** NetBackup filesystem with the **mount -a** command.
		`[admusr@<pmac_guest> ~]$ mount -a`
		Note: This command can only be used if the existing entry to mount the filesystem is contained in the **/etc/fstab** file (which is expected).
		6. Verify the new size of the NetBackup filesystem. Issue the **mount** command to verify the filesystem is correctly mounted. Issue the **/bin/df -h /usr/openv** command to show the NetBackup filesystem using 5GB instead of 2GB.
		`[admusr@<pmac_guest> ~]$ /bin/mount`
		`/dev/mapper/vgroot-plat_root on / type ext4 (rw)`
		`proc on /proc type proc (rw)`
		`sysfs on /sys type sysfs (rw)`
		`devpts on /dev/pts type devpts (rw,gid=5,mode=620)`
		`tmpfs on /dev/shm type tmpfs (rw)`
		`/dev/vda1 on /boot type ext4 (rw)`
		`/dev/mapper/vgroot-plat_tmp on /tmp type ext4 (rw)`
		`/dev/mapper/vgroot-plat_usr on /usr type ext4 (rw)`
		`/dev/mapper/vgroot-plat_var on /var type ext4 (rw)`
		`/dev/mapper/vgroot-plat_var_tklc on /var/TKLC type ext4 (rw)`
		`/dev/mapper/vgroot-smac_root on /usr/TKLC/smac type ext4 (rw)`
		`/dev/mapper/vgroot-smac_var on /var/TKLC/smac type ext4 (rw)`
		`/dev/mapper/vgroot-smac_backup on /var/TKLC/smac/backup type ext4 (rw)`
		`/dev/mapper/vgroot-smac_isoimages on /var/TKLC/smac/image/isoimages type ext4 (rw)`
		`/var/TKLC/smac/image/core on /var/TKLC/core type none (rw,bind)`
		`/dev/vdb on /var/TKLC/smac/logs type ext3 (rw)`
		`/dev/vdc on /var/TKLC/smac/image/repository type ext3 (rw)`
		`none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)`
		`sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)`

Step #	Procedure	Description
		nfsd on /proc/fs/nfsd type nfsd (rw) /dev/vdd on /usr/openv type ext3 (rw) The second command in this sub-step shows the NetBackup filesystem using 5GB instead of 2GB. [admusr@<pmac_guest> ~]$ /bin/df -h /usr/openv Filesystem Size Used Avail Use% Mounted on /dev/vdd 5.0G 69M 4.3G 1% /usr/openv 7. Change the directory to the **/usr/openv** directory and verify any files contained on the original 2GB NetBackup filesystem are still available on the new 5GB NetBackup filesystem. [admusr@<pmac_guest> ~]$ /bin/ls -l /usr/openv java lost+found pack regid.1992-12.com.symantec_netbackup-7.6.0.1_1.swidtag share var lib msg pack.7.6.0.1 regid.1992-12.com.symantec_netbackup-7.7.1.0_1.swidtag swidtag.xml logs netbackup pdde resources tmp

Appendix R. netConfig backup Configuration/restoreConfiguration/upgradeFirmware with TPD Cipher Change

Beginning with TPD 7.7.0.0.0-88.68.0, the cipher list is restricted to allow only a limited number of ciphers for ssh access to the servers. As a result, netConfig backup and restore operations are not functional with Cisco switches (3020, 4948s) since these switches use other ciphers. Executing these commands with the restricted ciphers would fail as shown here:

```
[admusr@p5-pmac ~]$ sudo netConfig --device=3020_ip backupConfiguration service=ssh_ip filename=backup
Command failed: backupConfiguration
Error saving to SSH service
[admusr@p5-pmac ~]$
```

To avoid this issue while maintaining a focus on improved security, the Procedure 57 must be executed before and after netConfig backup and restore operations.

Procedure 55. Turn Off Cipher List Before backupConfiguation/restoreConfiguration/upgradeFirmware Command

Step #	Procedure	Description
This procedure prepares the PMAC to avoid the cipher mismatch issue with Cisco switches. This is performed before the netConfig backup or restore operations. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		

1. ☐	Turn off cipher list	From the PMAC shell enter:
		`sudo vi /etc/ssh/sshd_config`
		Add # in the beginning of the following three lines to comment them out, the result is:
		`#Ciphers aes256-ctr,aes192-ctr,aes128-ctr`
		`#MaxAuthTries 4`
		`#LoginGraceTime 1m`

2. ☐	Restart sshd	`sudo service sshd restart`

3. ☐	Run the netConfig backupConfiguation/restoreConfiguration/upgradeFirmware command	For a backup operation:
		`[admusr@pmac ~]$ sudo /usr/TKLC/plat/bin/netConfig backupConfiguration --device=<switch_name> service=<ssh_service> filename=<switch_name>-backup`
		For a restore operation:
		`[admusr@pmac ~]$ sudo /usr/TKLC/plat/bin/netConfig restoreConfiguration --device=<switch_name> service=<ssh_service> filename=<switch_name>-backup`
		For a upgrade operation:
		`[admusr@pmac ~]$ sudo /usr/TKLC/plat/bin/netConfig upgradeFirmware --device=<switch_name> service=<ssh_service> filename=<Cisco IOS>`

Procedure 18. Resume Cipher List After backupConfiguation/restoreConfiguration/upgradeFirmware Command

Step #	Procedure	Description
This procedure restores the PMAC restricted cipher list after perform the netConfig backup and restore operations. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.		

1. ☐	Resume the cipher list	From the PMAC shell enter:
		`sudo vi /etc/ssh/sshd_config`
		Uncomment the three lines:
		`Ciphers aes256-ctr,aes192-ctr,aes128-ctr`
		`MaxAuthTries 4`
		`LoginGraceTime 1m`

2. ☐	Restart sshd	`sudo service sshd restart`

Appendix S. My Oracle Support (MOS)

MOS (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at **1-800-223-1711** (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select **2** for New Service Request.
2. Select **3** for Hardware, Networking and Solaris Operating System Support.
3. Select one of the following options:
   - For technical issues such as creating a new Service Request (SR), select 1.
   - For non-technical issues such as registration or assistance with MOS, select 2.

You are connected to a live agent who can assist you with MOS registration and opening a support ticket. MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the CAS main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at **http://www.oracle.com/us/support/contact/index.html**. The emergency response provides immediate coverage, automatic escalation, and other features to ensure the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability

- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the **Oracle Help Center** site at http://docs.oracle.com.
2. Click Industries.
3. Under the **Oracle Communications** subheading, click the **Oracle Communications documentation** link. The Communications Documentation page appears. Most products covered by these documentation sets display under the headings N**etwork Session Delivery and Control Infrastructure** or **Platforms**.

   Click on your Product and then the Release Number. A list of the entire documentation set for the selected product and release displays. To download a file to your location, right-click the PDF link, select `Save target as` (or similar command based on your browser), and save to a local folder.