Corporate Headquarters
5200 Paramount Parkway
Morrisville, NC 27560 USA
Phone +1.888.628.5521
+1.919.468.5500
Fax: +1.919.380.3862
E-mail: info@tekelec.com

EAGLE XG

Software Install Procedure

DSR 4.X HP C-Class Installation

P. Mouallem, M. Williams

909-2228-001 Revision A, March 2013 **Version 3.3**

CHANGE HISTORY

Date	ENG Version #	ECN Revision #	Author	Description	Approved* (Yes/No)
6/27/12	0.1		P. Mouallem	Copy of DSR 3.0 Install Doc Contents	No
7/02/12	0.2		P. Mouallem, M. Williams	DSR 4.0 Updates	No
7/03/12	0.3		P. Mouallem	Updates and PR Fixes	No
7/05/12	0.4		P. Mouallem	Updates	No
7/20/12	0.5		P. Mouallem	Updates	No
7/25/12	0.6		M. Williams	Updates for Scalability, VM Profiles	No
8/10/12	0.7		P. Mouallem	Additional Updates	No
8/24/12	0.11		P. Mouallem	Updates after Formal Review	No
8/30/12	0.12		M. Williams	Updates from Review and additional documentation for RMS configuration	No
9/10/12	0.13		M.Williams	Further updates after desk review comments	No
9/11/12	0.14		P. Mouallem	Further updates after desk review comments	No
9/11/12	1.1		P. Mouallem	updates after desk review comments	Yes
9/21/12	1.2		M. Williams	Revisions after comments from PSEs	Yes
10/12/12	1.9		P. Mouallem	NetBackup PRs 218480, 218475, 218477	No
10/17/12	1.10		P. Mouallem	Updates after Desk Review	No
10/17/12	1.11		P. Mouallem	Updates after Desk Review, PR 220729	No
10/19/12	2.0		P. Mouallem	Updates after Desk Review	Yes
10/26/12	2.1		M. Williams	Fix for PR#220923	Yes
10/29/12	2.2		P. Mouallem	Fix for PRs 218247, 215306, 212894	Yes
10/30/12	2.5		P. Mouallem	Fix for PRs 220488	Yes
11/07/12	2.7		P. Mouallem	Updates	Yes
11/08/12	2.8		M. Williams	Update for PR#221271	Yes
11/08/12	2.10		P. Mouallem	Misc Updates	Yes
11/08/12	2.13		P. Mouallem	Adding Steps to configure ComAgent Connections	Yes
11/13/12	2.14		P. Mouallem	Misc Updates	Yes
11/13/12	2.16		P. Mouallem	Fix for PRs 221532, 221536, 221548	Yes
11/29/12	2.17		M. Williams	Update to add workaround for Appworks XMI def. route issue	Yes
11/30/12	2.18		P. Mouallem	Misc Updates	Yes
12/11/12	2.19		P. Mouallem	Moving Appendix L to DR Doc (909-2246-001)	Yes
12/11/12	2.20		P. Mouallem	Fix for PR 211593	Yes
12/17/12	2.21		M. Williams	Misc. Updates/Fix for PR 219631	Yes
1/10/13	2.22		M. Williams	Updated section where MP server is inserted to clarify deletion of XMI default route if needed.	Yes
1/25/13	2.23		P. Mouallem	Minor Update	Yes
1/28/13	2.24		P. Mouallem	Fix for PRs 221489, 223446	Yes
1/30/13	2.26		P. Mouallem	Adding step to set the timezone on the SO	Yes
1/30/13	2.28		P. Mouallem	Update to Procedure 6, Step 17 (switch backup user)	Yes
3/7/13	2.29		M. Williams	Fixed problem with table of contents	Yes
3/14/13	2.30		M. Williams	Added installation map, updated sections based on PRs.	Yes
3/15/13	2.31		P. Mouallem	PR 223182, 218359, 220432	Yes
3/19/12	2.32		M. Williams	Update document to be aware of PDRA Installations	Yes

3/19/12	2.33		P. Mouallem	Update after Desk Review	Yes
3/26/13	2.34		M.Williams	Updates after Desk Review and added extra Appendix for openssh tunneling (PR 218359)	Yes
4/19/13	2.35		P. Mouallem	Minor Updates	Yes
6/19/13	2.36		M. Williams	Add PDRA procedures; Update document references	Yes
6/21/13	2.37		P. Mouallem	Minor Updates	Yes
6/26/13	2.38		M. Williams	Minor Updates	Yes
8/16/13	3.0		Duane Orton	Approved DSR 4.x installation procedure for DSR 4.0.x and 4.1.0	Yes
8/22/13	3.1		M. Williams	Updates for NTP configuration on server insert screen for 4.1.X installations	Yes
12/09/13	3.2		P. Mouallem	Changing PMAC's DEVICE.NETWORK.NETBOOT to use Management instead of Control (proc 2 step 7)	Yes
12/12/2013	3.3		M. Williams	Update SOAM procedures to include optional installation of Netbackup client	Yes

TABLE OF CONTENTS

List of Figures

List of Tables

List of Procedures

1.0 INTRODUCTION

1.1 Purpose and Scope

This document describes methods utilized and procedures executed to configure an HP C-class system to be used with Diameter Signaling Router 4.X (DSR 4.X) and to install DSR 4.X. It is assumed that the hardware installation and network cabling were executed before hand.
The audience for this document includes Tekelec customers as well as these groups: Software System, Product Verification, Documentation, and Customer Service including Software Operations and First Office Application.

1.2 References

1.2.1 External

[1] *HP Solutions Firmware Upgrade Pack Release Notes*, 910-6611-001 Rev A, July 2012

[2] *Diameter Signaling Router 4.0 Networking Interconnect Technical References*, TR007133/4/5/6/7/8/9, v. 1.0 or greater, P. Mouallem, 2012

[3] *TPD Initial Product Manufacture*, 909-2130-001, v. 1.0 or greater, D. Knierim, 2011

[4] *Platform 6.x Configuration Procedure Reference*, 909-2209-001, v. 1.0 or greater, L. Antosova et al., 2012

[5] *DSR 4.0 Communication Agent*, 910-6575-001, Latest Revision, Tekelec, 2012

[6] *DSR 4.0 Full Address Based Resolution (FABR)*, 910-6578-001, Latest Revision, Tekelec, 2012

[7] *DSR 41 Full Address Based Resolution (FABR)*, 910-6634-001, Latest Revision, Tekelec, 2012

[8] HP Solutions Firmware Upgrade Pack Upgrade Procedures 2.2, 909-2234-001, Latest Revision, Tekelec, 2012

[9] Policy DRA Activation, WI006835, Latest Revision, Tekelec 2012

1.2.2 Internal (Tekelec)

The following are references internal to Tekelec. They are provided here to capture the source material used to create this document. Internal references are only available to Tekelec personnel.

[1] *Formal Peer Review Process*, PD001866, v6.21, Nov 2008

1.3 Variables

For a list of the variables used throughtout this document and their description, see 4.18Appendix M

1.4 Acronyms

An alphabetized list of acronyms used in the document:

Table 1. Acronyms

Acronym	Definition
BIOS	Basic Input Output System
CD	Compact Disk
DVD	Digital Versatile Disc
EBIPA	Enclosure Bay IP Addressing
FRU	Field Replaceable Unit
HP c-Class	HP blade server offering
iLO	Integrated Lights Out manager
IPM	Initial Product Manufacture – the process of installing TPD on a hardware platform
MSA	Modular Smart Array
NB	NetBackup
OA	HP Onboard Administrator
OS	Operating System (e.g. TPD)
RMS	Rack Mounted Server
PM&C	Platform Management & Configuration
SAN	Storage Area Network
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
TPD	Tekelec Platform Distribution
TVOE	Tekelec Virtual Operating Environment
VM	Virtual Machine
VSP	Virtual Serial Port

1.5 Terminology

Multiple server types may be involved with the procedures in this manual. Therefore, most steps in the written procedures begin with the name or type of server to which the step applies. For example:

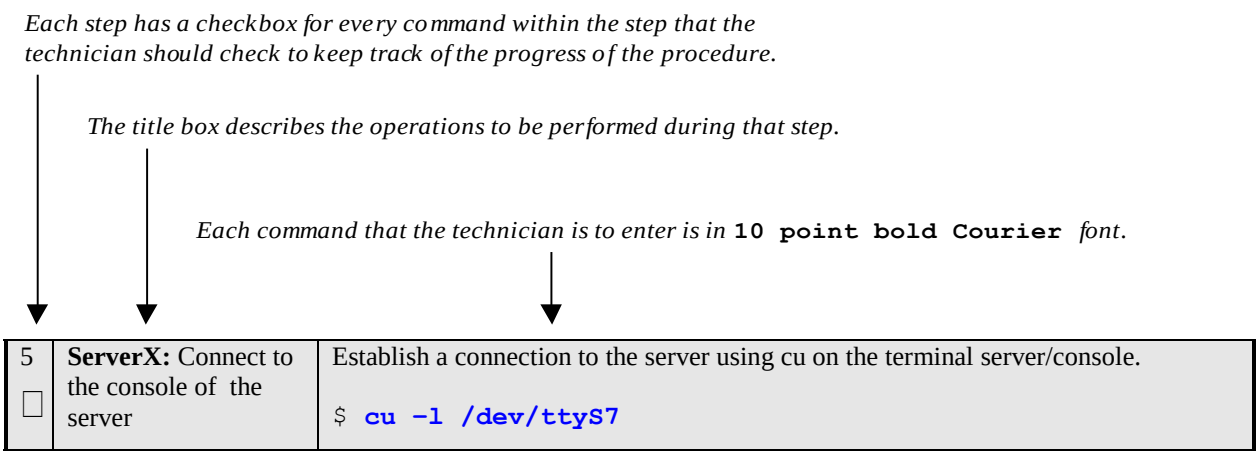


Figure 1. Example of an instruction that indicates the server to which it applies

Management Server	HP ProLiant DL360 or DL380 Rack Mount Seerver deployed to run TVOE and host a virtualized PM&C application. Can also host a virtualized NOAMP. It is also used to configure the Aggregation switches (via the PM&C) and to serve other configuration purposes.
PM&C Application	PM&C is an application that provides platform-level management functionality for HP G6 system, such as the capability to manage and provision platform components of the system so it can host applications.

2.0 GENERAL DESCRIPTION

This document defines the steps to execute the initial installation of the Diameter Signaling Router 4.X (DSR 4.X) application on new HP C-Class Hardware.

DSR 4.X installation paths are shown in the figures below. The general timeline for all processes to perform a software installation/configuration and upgrade is also included below.

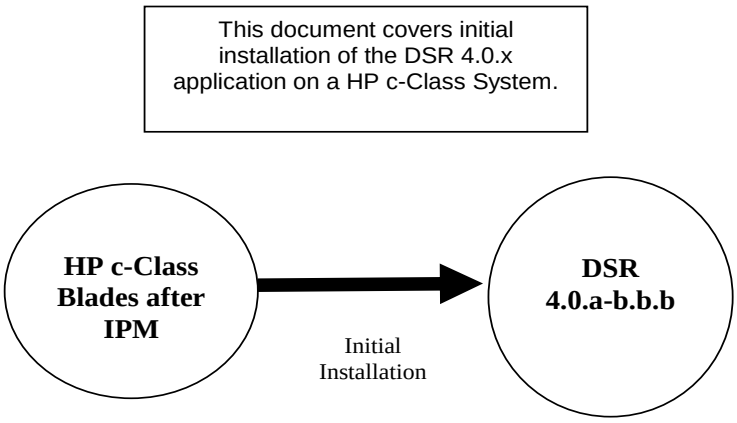


Figure 2. Initial Application Installation Path – Example shown

2.1 ACQUIRING FIRMWARE

Several procedures in this document pertain to the upgrading of firmware on various servers and hardware devices. The required firmware media and binaries are managed and distributed as part of the *HP Solutions Firmware Upgrade Pack 2.2.x*, released under Tekelec Part Number 795-0000-2*yy*[1]. The minimum firmware release required for this product is *HP Solutions Firmware Upgrade Pack 2.2.3* (PN: 795-0000-201) although the latest 2.2.x release is recommended.

The *HP Solutions Firmware Upgrade Pack* contains multiple BOM items including media and documentation. This document only requires access to the media (CD/DVD/USB or ISOs) as well as the *Release Notes [1]* document.

The two pieces of required firmware media provided in the *HP Solutions Firmware Upgrade Kit 2.2.x* releases are:

- HP Smart Update Firmware DVD/USB/ISO
- HP Misc Firmware CD/USB/ISO

Refer to the Release Notes of the target release of the *HP Solutions Firmware Upgrade Pack* used to determine specific media part numbers to use and the specific firmware versions provided.

[1] Where *yy* is a 2-digit number which increases with every new release.

Diameter Signaling Router 4.X Servers and devices requiring possible firmware updates are:

- HP c7000 BladeSystem Enclosure Components:
  - Onboard Administrator
  - Cisco 3020 Network Switches / HP 6120XG Network Switches
  - BL460c Blade Servers
- HP Rack Mount Servers (DL360 / DL380)
- Cisco 4948E/4948E-F Rack Mount Network Switch (Optional)

3.0 INSTALL OVERVIEW

This section provides a brief overview of the recommended method for installing the source release software that is installed and running on an HP c-Class system to the Target Release software. The basic install process and approximate time required is outlined in Table 2.

3.1 Required Materials

1. One (1) target release Application CD-ROM, or a target-release ISO
2. One (1) CD-ROM or ISO of TPD release 6.0.0-80.25.0 64 bits, or later shipping baseline as per Tekelec ECO
3. One (1) CD-ROM or ISO of PM&C release 5.0.0-50.14.0, or later shipping baseline as per Tekelec ECO
4. One (1) CD-ROM or ISO of TVOE release 80.22, or later shipping baseline as per Tekelec ECO
5. Passwords for users on the local system
6. Access to the iLO Terminal or direct access to the server vga port.
7. HP Solution firmware upgrade pack as described in [1].
8. A 1Gb or larger USB Flash Drive
9. All relevant configuration materials for ALL sites involved. This includes host IP addresses, site network element XML files, and netconfig configuration files.

The material for the list above can also be downloaded from Tekelec's secure website, locate at https://secure.tekelec.com/

3.2 Installation Overview

This section describes the overal strategy to be employed for a single or multi-site DSR 4.X installation. It also lists the procedures required for installation with estimated times. Section 3.2.1 discusses the overall install strategy and includes an installation flow chart that can be used to determine exactly which procedures should be run for an installation. Section 3.2.2 lists the steps required to install a DSR 4.X system. These latter sections expand on the information from the matrix and provide a general timeline for the installation.

3.2.1 Installation Strategy

A successful installation of DSR requires careful planning and assessment of all configuration materials and installation variables. Once a site survey has been conducted with the customer, the installer should use this section to map out the exact procedure list that will executed at each site.

Figure 3 Illustrates the overall process that each DSR installation will involve. In summary:

1. An overall installation requirement is decided upon. Among the data that should be collected:
    - The total number of sites
    - The number of servers at each site and their role(s)
    - Does DSR's networking interface terminate on a Layer 2 or Layer 3 boundary?
    - Number of enclosures at each site -- if any at all.
    - Will NOAMPs use rack-mount servers or serever blades?
    - (Per Site) Will MP's be in N+0 configuration or in active/standby?
    - What timezone should be used across the entire collection of DSR sites?
    - Will SNMP traps be viewed at the NOAM, or will an external NMS be used? (Or both?)

2. A site survey is conducted with the customer to determine exact networking and site details.
3. For each site being configured, the installer will consult Figure 4 to determine the exact procedures that are to be executed for that site.
4. The installer will then install the "main" site that contains the NOAMP -- again, consulting Figure 4 to determine the procedure list. (note: for sites where the NOAMP is co-located with the SOAM and other servers, steps 3 and 4 are combined). During this install, he will "bring up" the other sub-sites that were configured in step 3.
5. Once the NOAMP site has been installed according to Figure 4, full DSR installation is complete.

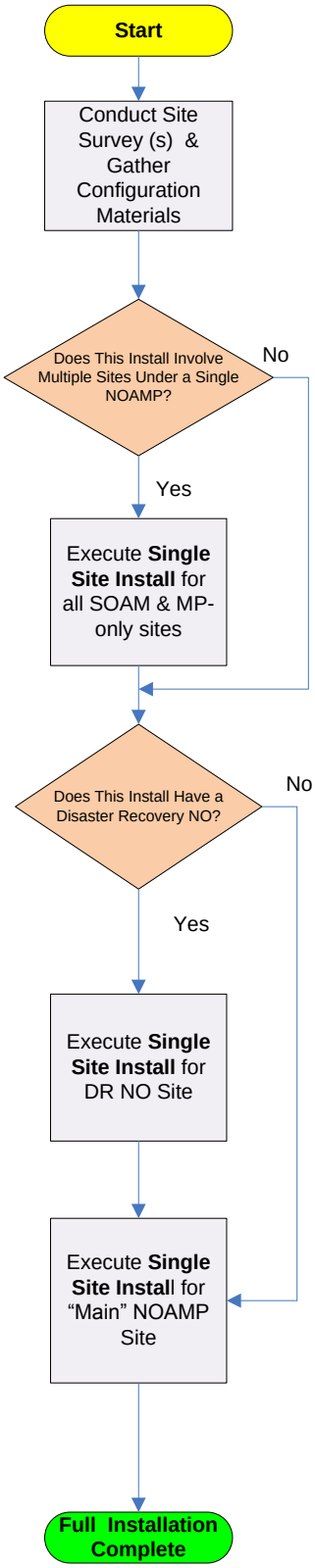


Figure 3 - DSR Installation - High Level Sequence

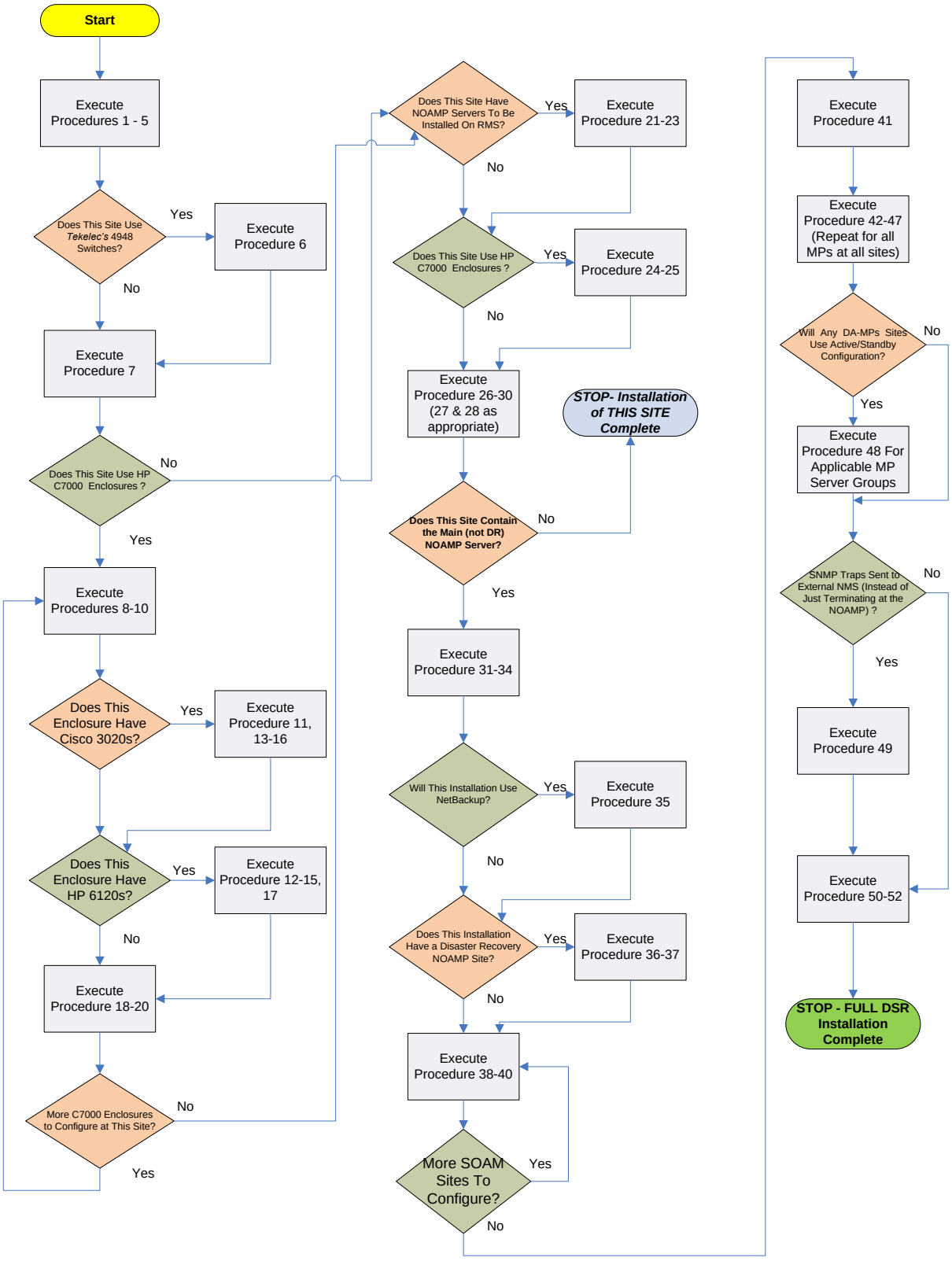


Figure 4: DSR Single Site Installation Procedure Map

3.2.2 SNMP Configuration

The network-wide 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 Auxillary 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 will terminate at the NOAMP and be viewable from the NOAMP GUI (entire network) and the SOAM GUI (site specific). **This is the default configuration option and no changes are required for this to take effect.**
2. Send all their SNMP traps to an external Network Management Station (NMS). The traps will NOT be seen at the SOAM OR at the NOAM. They will be viewable at the configured NMS(s) only.

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

DSR auxillary 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:

- **PMAC (TVOE)**
- **PMAC (App)**
- **OAs**
- **All Switch types (4948, 3020, 6120)**
- **TVOE for DSR Servers**

Should have their SNMP trap destinations set to:

1. **The local SOAM VIP**
2. **The customer NMS, if available**

3.2.3 Installation Procedures

The following table illustrates the progression of the installation process by procedure with estimated times. The estimated times and the phases that must be completed may vary due to differences in typing ability and system configuration. The phases outlined in are to be executed in the order they are listed.

Table 2. Installation Overview

Procedure	Phase	Elapsed Time (Minutes)	
		This Step	Cum.
Procedure 1	Configure the RMS Server BIOS Settings and Update Firmware	30	30

Table 2. Installation Overview

Procedure	Phase	Elapsed Time (Minutes)	
		This Step	Cum.
Procedure 2	Install TVOE 2.0 on First RMS Server	15	45
Procedure 3	TVOE/Management Server Network Configuration	30	75
Procedure 4	PM&C Deployment Procedure	20	95
Procedure 5	Gather/Prepare Configuration Files and start services	10	105
Procedure 6*	Configure Cisco 4948E/4948E-F Switch using NetConfig*	45*	150
Procedure 7	Configure the PM&C Server	10	160
Procedure 8	Configure initial OA IP	10	170
Procedure 9	Configure the OA	40	210
Procedure 10	OA security configuration	5	215
Procedure 11 and/or 12	Upgrade Cisco 3020/HP 6120 switch firmware	30	245
Procedure 13	Upgrade OA firmware	10	255
Procedure 14	Add Cabinet & Enclosure to the PM&C Inventory	20	275
Procedure 15	Configure iLO password for Administrator account	10	285
Procedure 16 and/or 17	Configure Cisco 3020/HP 6120 switch	30	315
Procedure 18	Upgrade blade server firmware	10	325
Procedure 19	Confirm/Update Blade Server BIOS Setup	10	335
Procedure 20	Disable SNMP on iLO Interface	20	355
Procedure 21	Install TVOE on Additional RMSs	25	380
Procedure 22	Continue TVOE Configuration on First RMS	15	395
Procedure 23	Configure TVOE on Addional RMSs	20	415
Procedure 24	Install TVOE on Server Blades	20	435
Procedure 25	Configure TVOE on Server Blades	10	445
Procedure 26	Load Application ISO onto PM&C Server	5	450
Procedure 27	Create NOAMP Guest VMs	5	455
Procedure 28	Create SOAMP Guest VMs	5	460
Procedure 29	IPM blades	20	480
Procedure 30	Install the application software on the blades	20	500
Procedure 31	Configure the First NO Blade Server	25	525
Procedure 32	Configure the NO Server Group	15	540
Procedure 33	Configure the Second NO Server	15	555
Procedure 34	Complete Configuring the NOAMP Server Group	10	565

Table 2. Installation Overview

Procedure	Phase	Elapsed Time (Minutes)	
		This Step	Cum.
Procedure 35	Install NetBackup Client on NOAMP Servers (Optional)	10	575
Procedure 36	NO Configuration for DR Site (Optional)	10	585
Procedure 37	NO Pairing for DSR NO DR Site (Optional)	10	595
Procedure 38	Configure the SOAM NE	15	610
Procedure 39	Configure the SOAM Servers	10	620
Procedure 40	Configure the SOAM Server Group	10	630
Procedure 41	Optimize NO and SO Databases	5	635
Procedure 42	Configure the MP Blade Servers	10	645
Procedure 43	Configure Places and Assign MP Servers to Places (PDRA)	10	655
Procedure 44	Configure the MP Server Groups	10	665
Procedure 45	Configure the Signaling Network	30	695
Procedure 46	Configure the Signaling Devices	10	705
Procedure 47	Configure the Signaling Network Routes	15	720
Procedure 48	Add VIP for Signaling Networks	5	725
Procedure 49 (Optional)	Configure SNMP for Traps Receivers	5	730
Procedure 50	PDRA Resource Domain Configuration (PDRA Only)	15	745
Procedure 51	Activate Optional Features	varies*	745
Procedure 52	Configure ComAgent Connections	15	760

3.3 Optional Features

When DSR installation is complete, further configuration and/or installation steps will need to be taken for optional features that may be present in this deployment. Please refer to these documents for the post-DSR install configuration steps needed for their components.

Feature	Document
IP Front End (IPFE)	*IPFE Installation and Configuration*, WI006837, latest version, Mahoney
Charging Proxy Application (CPA) **Session Binding Repository** (SBR)	*CPA Activation Feature Work Instruction*, WI006780, latest version, Moore *CPA User Guide*, 910-6635-001,Rev A (4.1)

Diameter Mediation	*DSR Meta Administration Feature Activation*, WI006761, latest version, Fisher
Full Address Based Resolution (FABR**)**	*DSR FABR Feature Activation*, WI006771, latest version, Karmarkar; *FABR User Guide*, 910-6634-001,Rev A (4.1.0) *FABR User Guide*, 910-6634-001,Rev B (4.1.5)
Range Based Address Resolution (RBAR**)**	*DSR RBAR Feature Activation*, WI006763, latest version, Fisher *RBAR User Guide*, 910-6633-001,Rev A
BL620(Full Height Card) Capacity Upgrade	*DSR 4.0 Half-Height to Full-Height MP Server Capacity Migration*, WI006766, latest version, Fisher
Per connection ingress message control	*DSR 4.0 – Per connection ingress message control* . WI006764

4.0 SOFTWARE INSTALLATION PROCEDURE

As mentioned earlier, the hardware installation and network cabling should be done before executing the procedures in this document.

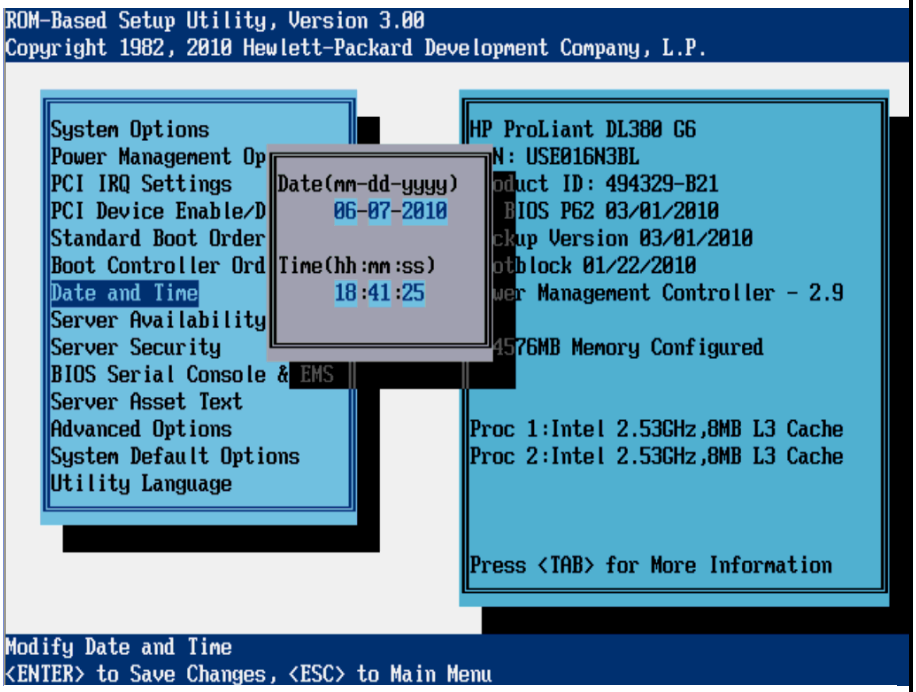
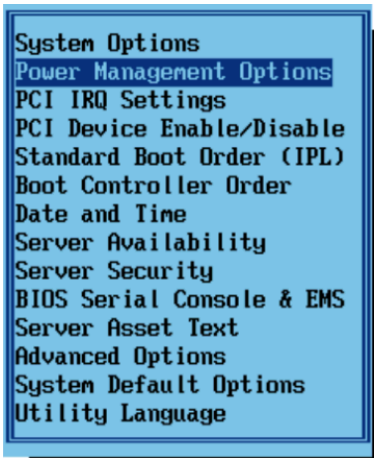
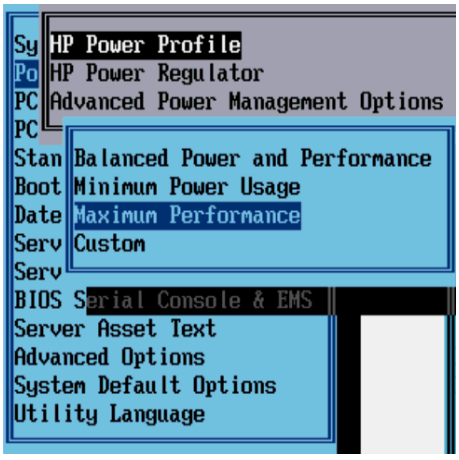
NOTE: Prior to executing the procedures below, please review the DSR release notes, and be aware of any workaround that should be executed.

4.1 Configure and IPM Management Server

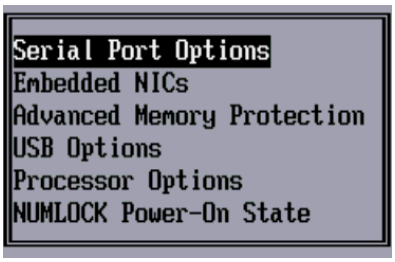
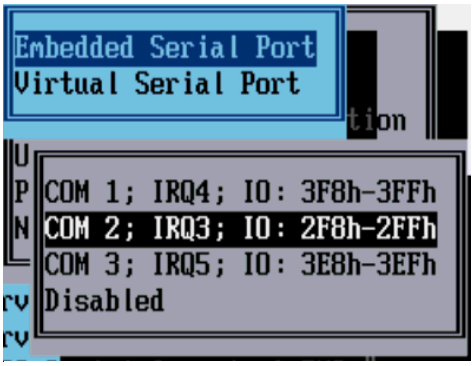
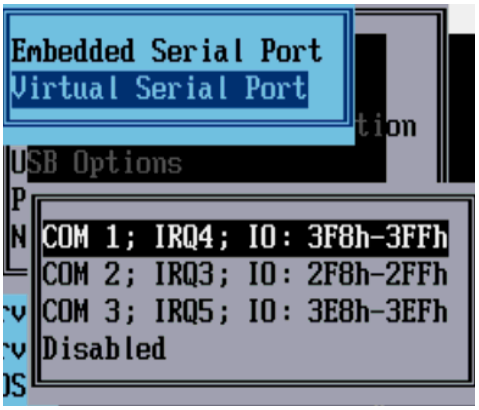
Procedure 1. Configure the RMS Server BIOS Settings and Update Firmware

S T E P #	This procedure will configure the BIOS of the DL380 server and update its firmware if needed **Needed material:** - HP Firmware Maintenance Media - HP Solutions Firmware Upgrade Pack Release Notes [1] Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**DL360/380 server:** Connect to the Server	Connect to the Server using a VGA Display and USB Keyboard, or via the iLO interface using IE. Appendix C though F explains how to access the PM&C iLO and change the address if necessary.
2 ☐	**DL360/380 server:** Prepare to upgrade DL380 server firmware	Insert HP Smart Update Firmware DVD/USB into the server
3 ☐	**DL360/380 server:** Access the Server BIOS	Reboot the server 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.

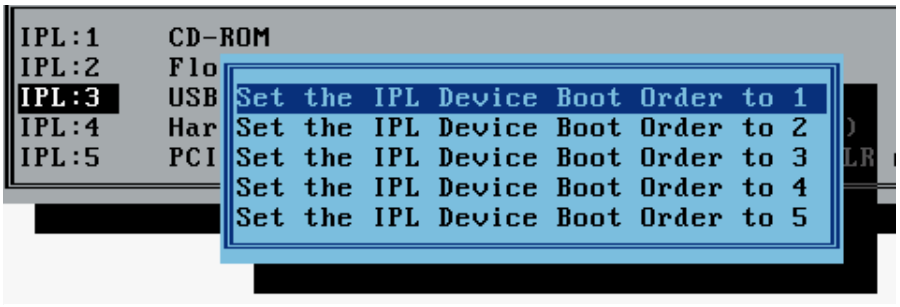
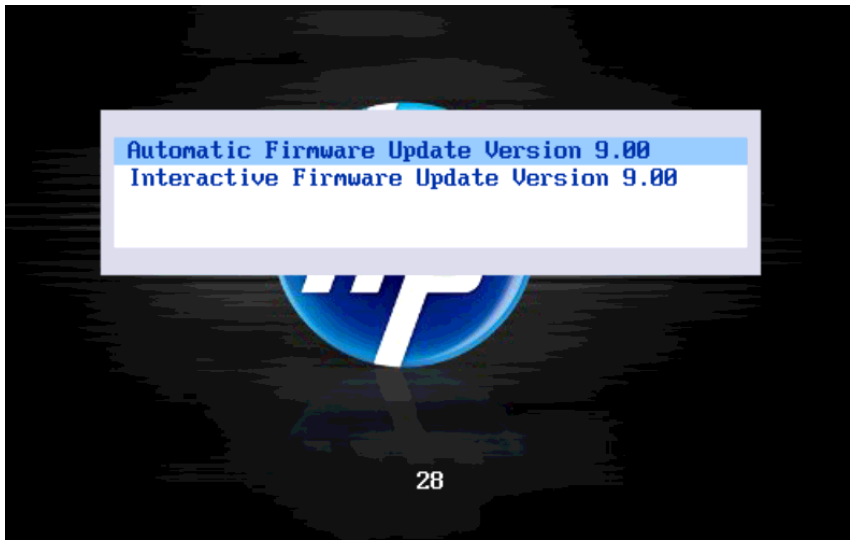
Procedure 1. Configure the RMS Server BIOS Settings and Update Firmware

4 ☐	**DL360/380:** Set CMOS Clock	Scroll to *Date and Time* and press **Enter** Set the date and time to current UTC time and press **Enter**. **NOTE: IT IS CRUCIAL TO CORRECTLY SET THE TIME AND DATE TO THE CURRENT UTC TIME. DO NOT CONTINUE THIS PROCEDURE UNLESS THE TIME AND DATE ARE CORRECTELY SET.**  Go back to the main menu by pressing **<Esc>** and scroll down to *Power Management Options* and press **Enter** Select *HP Power Profile* and press **Enter** Scroll down to *Maximum Performance* and press **Enter**   Press **<Esc>** to return to the main menu

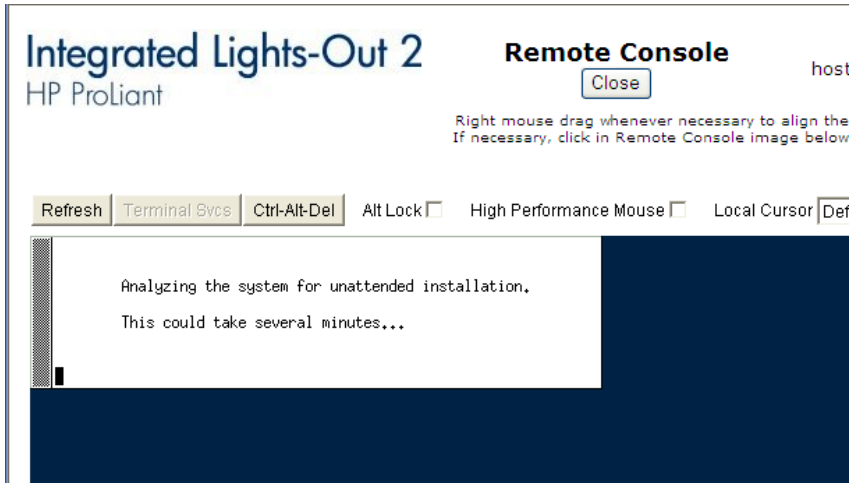
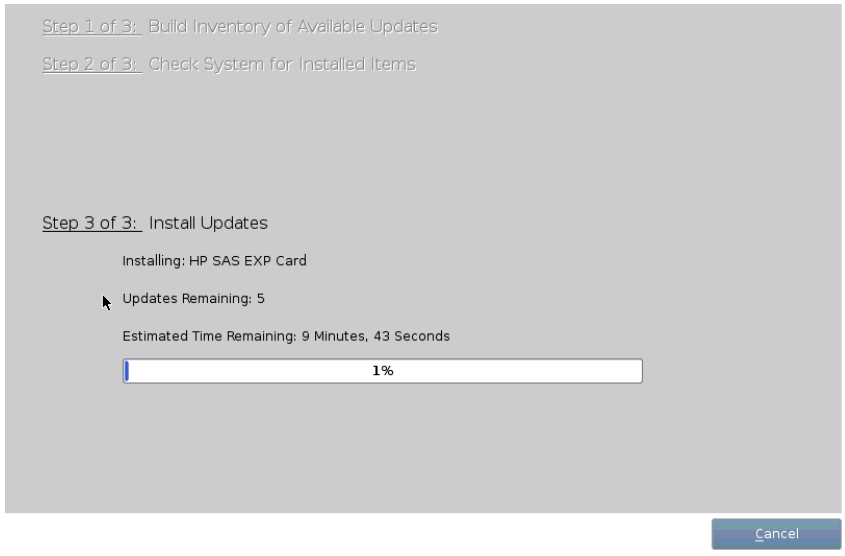
Procedure 1. Configure the RMS Server BIOS Settings and Update Firmware

5 ☐	**DL360/380 server:** Configure iLO Serial Port	Scroll to *System Options* and press **Enter** **Change power profile (same as blades)** Select *Serial Port Options* and press **Enter**  Press **Enter** to select *Embeded Serial Port* and change it to *COM2* and press **Enter**  Press **Enter** to select *Virtual Serial Port* and change it to *COM1* and press **Enter**  Press **<ESC>** 2 times to return to the main menu

Procedure 1. Configure the RMS Server BIOS Settings and Update Firmware

6 ☐	**DL360/380 server:** Double Check boot Order	Scroll to *Standard Boot Order (IPL)* and press **Enter** **If DL360 of DL380 Gen6:** Select *CD-ROM*, and set its boot order to 1 as shown below **If DL380 Gen8:** Select *USB DriveKey*, and set its boot order to 1 as shown below  Press **Enter** Press **<ESC>** to return to the main menu.
7 ☐	**DL360/380 server:** Configure Server Availability	Select "Server Availability" Change "Automatic Power-On" to "Always Power On" Verify that Power-On Delay" is set to "No Delay", if it is not, then set it.
8 ☐	**DL360/380 server:** Save Configuration and Exit	Press **<ESC>** twice then press **F10** to save the configuration and exit. The server will reboot
9 ☐	**DL360/380 server:** Perform an unattended firmware upgrade	The server will reboot into the *HP Smart Update Firmware* ISO and present the following boot prompt. Press **[Enter]** to select the **Automatic Firmware Update** procedure.  **If no key is pressed in 30 seconds the system will automatically perform an Automatic Firmware Update.**

Procedure 1. Configure the RMS Server BIOS Settings and Update Firmware

10 ☐	**DL360/380 server:** System analysis	The firmware install will perform a system scan of the server in which it will identify all of the firmware components that are eligible for upgrade. This process may take up to 10 minutes and during that time the following screen is displayed on the console.  **Note**: No progress indication is displayed during the system scan and analysis stage. In about 10 minutes the installation will automatically proceed to the next step.
11 ☐	**DL360/380 server:** Monitor installation	Once analysis is complete the installer will begin to upgrade the eligible firmware components. A progress indicator is display at this time as shown below.  **Note**: If the iLO2 firmware is to be upgraded it will be upgraded last. At this point the iLO2 session will be terminated and you will lose the remote console, virtual media and Web GUI connections to the server. This is expected and will not impact the firmware upgrade process.
12 ☐	**Local Workstation:** Clean up	Once the firmware updates have been completed the server will automatically be rebooted. At this time you may close the remote console and the iLO2 Web GUI browser session.

Procedure 1. Configure the RMS Server BIOS Settings and Update Firmware

13 ☐	**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.
14 ☐	**DL360/380 server:** Remove the firmware Media	Remove the HP Smart Update Firmware DVD/USB media from the drive. Exit from the `Integrated Remote Console`.
15 ☐	**Repeat for all remaining RMS**	Repeat this procedure for all remaining RMS Server, if any.

Procedure 2. Install TVOE 2.0 on First RMS Server

STEP #	This procedure will install TVOE 2.0 on the First RMS Server **Needed material:** - TVOE 2.0 Media on DVD or bootable USB Drive (if DL380 Gen8) Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**Connect to the First RMS Server**	Connect to the Server using a VGA Display and USB Keyboard, or via the iLO interface using IE. Appendix C though F explains how to access the PM&C iLO and change the address if necessary.
2 ☐	**DL360/380 Server 1:** Insert TVOE Media into Server	Insert the DVD or Bootable USB Drive (if DL380 Gen8) containg the TVOE media. .
3 ☐	**DL360/380 Server 1:** Begin IPM Process	Once the Server reboots, it will reboot from the TVOE media and a boot prompt shall be displayed. IPM the server using the following command: **`TPDnoraid diskconfig=HPHW,force console=tty0`**

Procedure 2. Install TVOE 2.0 on First RMS Server

4 ☐	**DL360/380 Server 1:** IPM Complete	The IPM process takes about 30 minutes, you will see several messages and screens in the process. Once the IPM is complete, you will be prompted to press Enter as shown below. Remove the media from the drive or unmount the TPD image from the iLO and press **Enter** to reboot the server. Note that the CD may eject automatically. 
5 ☐	**DL360/380 Server 1:** Server Reboot	Once the Server Reboots, you should see a login prompt. Note that during the first system boot, swap files may be initialized and activated. Each swap file will take about 2 minutes. If no login prompt is displayed after waiting 15 minutes, contact Tekelec Customer Support for Assistance.

Procedure 3. TVOE/Management Server Network Configuration

S T E P #	This procedure will configure the Network on the TVOE/Management Server **Prerequisite:** *Procedure 1.* has been completed. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE. Refer to the table below to determine the Ethernet port names to use throughout this procedure based on the hardware type and configuration.

Network Interface	DL360 (w/o HP NC364T 4pt Gigabit)	DL360 (with HP NC364T 4pt Gigabit in PCI Slot 1)	DL380	DL380 (with HP NC364T 4pt Gigabit in PCI Slot 1)
<ethernet_interface_1>	eth01	eth01	eth01	eth01
<ethernet_interface_2>	eth02	eth02	eth02	eth02
<ethernet_interface_3>		eth21	eth03	eth03
<ethernet_interface_4>		eth22	eth04	eth04
<ethernet_interface_5>		eth23		eth11

<table>
<tr>
<td>1
☐</td>
<td>Determine Bridge names and interfaces</td>
<td>Determine the bridge name to be used on the TVOE management server for the management network and fill in the <TVOE_Management_Bridge> and <TVOE_Management_Bridge_Interface> values in the table below.

If netbackup is to be used, determine the bridge name to be used for the netbackup network and fill in the <TVOE_NetBackup_Bridge> and <TVOE_NetBackup_Bridge_Interface> values in the table below
<table>
<tr><th>PM&C Interface Alias</th><th>TVOE Bridge Name</th><th>TVOE Bridge Interface</th></tr>
<tr><td>control</td><td>control</td><td>Fill in the appropriate value (default is bond0):

<TVOE_Control_Bridge_Interface></td></tr>
<tr><td>management</td><td>Fill in the appropriate value: (default is management)

<TVOE_Management_Bridge></td><td>Fill in the appropriate value:

<TVOE_Management_Bridge_Interface></td></tr>
<tr><td>Netbackup (if applicable)</td><td>Fill in the appropriate value: (default is netbackup)

<TVOE_NetBackup_Bridge></td><td>Fill in the appropriate value:

<TVOE_NetBackup_Bridge_Interface></td></tr>
</table>
</td>
</tr>
<tr>
<td>2
☐</td>
<td>TVOE iLO: Login and launch the integrated remote console</td>
<td>Log in to iLO in IE using password provided by application:
http://<management_server_iLO_ip>

Click in the Remote Console tab and launch the Integrated Remote Console on the server.

Click Yes if the Security Alert pops up.</td>
</tr>
</table>

3 ☐	**TVOE iLO:** Verify the Control Network	Verify the control network by running the following command
		Note: The output below is for illustrative purposes only. The example output below shows the control bridge configured.
		
		`# netAdm query --type=Bridge --name=control`
		`Bridge Name: control`
		`On Boot: yes`
		`Protocol: dhcp`
		`Persistent: yes`
		`Promiscuous: no`
		`...`
		
		If the output matches the one above, then the Control Bridge already exists, do not execute the rest of this step and skip to the next step.
		
		Create control bridge (<TVOE_Control_Bridge>).
		`# netAdm add --device=bond0 --onboot=yes --type=Bonding --mode=active-backup --miimon=100`
		`Interface <TVOE_Control_Bridge_Interface> added`
		
		`# netAdm set --device=eth01 --type=Ethernet --master=<TVOE_Control_Bridge_Interface> --slave=yes --onboot=yes`
		`Interface <ethernet_interface_1> updated`
		
		`# netAdm set --device=eth02 --type=Ethernet --master-<TVOE_Control_Bridge_Interface> --slave=yes --onboot=yes`
		`Interface <ethernet_interface_2> updated`
		
		`# netAdm add --type=Bridge --name=control --bootproto=dhcp --onboot=yes --bridgeInterfaces=<TVOE_Control_Bridge_Interface>`

	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. Otherwise, skip on to the next step.
		
		`# netAdm set --type=Bridge --name=control --delBridgeInt=bond0`
		`Interface bond0 updated`
		`Bridge control updated`
		
		`# netAdm add --device=<TVOE_Control_Bridge_Interface>`
		`Interface <TVOE_Control_Bridge_Interface> created`
		
		`# netAdm set --type=Bridge --name=control --bridgeInterfaces=<TVOE_Control_Bridge_Interface>`

5 ☐	**TVOE iLO:** Verify the Manamgent Network	Verify the management network by running the following command
		Note: The output below is for illustrative purposes only. The example output below shows the control bridge configured.
		
		`# netAdm query --type=Bridge --name=management`
		`Bridge Name: manamgent`
		`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: bond0.2`
		
		If the bridge has been configured, skip to the next step.
		
		Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.
		
		If the management interface is on a separate bond then the bond which control uses (and already exists), execute the next 3 commands to create the new bond, otherwise skip to executing example 1 or example 2.
		
		`# netAdm add --device=<TVOE_Management_Bridge_Interface>`
		`--onboot=yes --type=Bonding --mode=active-backup --miimon=100`
		`Interface <TVOE_Management_Bridge_Interface> added`
		
		`# netAdm set --device=<ethernet_interface_3> --type=Ethernet`
		`--master=<TVOE_Management_Bridge_Interface> --slave=yes --`
		`onboot=yes`
		`Interface <ethernet_interface_3> updated`
		
		`# netAdm set --device=<ethernet_interface_4> --type=Ethernet`
		`--master-<TVOE_Management_Bridge_Interface> --slave=yes`
		`--onboot=yes`
		`Interface <ethernet_interface_4> updated`
		
		EXAMPLE 1: Create Management bridge using untagged interfaces (<TVOE_Management_Bridge>).
		
		`# netAdm add --type=Bridge --name=<TVOE_Management_Bridge>`
		`--bootproto=none --onboot=yes --`
		`address=<Management_Server_TVOE_IP> --`
		`netmask=<Management_Server_TVOE_Netmask>`
		`--bridgeInterfaces=<TVOE_Management_Bridge_Interface>`
		
		EXAMPLE 2: Create Management bridge using tagged interfaces
		
		`# netAdm add --device=<TVOE_Management_Bridge_Interface>`
		
		`# netAdm add --type=Bridge --name=<TVOE_Management_Bridge>`
		`--address=<Management_Server_TVOE_IP> --`
		`netmask=<Management_Server_TVOE_Netmask> --onboot=yes`
		`--bridgeInterfaces=<TVOE_Management_Bridge_Interface>`

6 ☐	**TVOE iLO:** Add/Verify the NetBackup Network (Optional)	If NetBackup is to be used, execute this step, otherwise skip to the next step.
		
		NetBackup is a tool that allows the customer to take remote backups of the system.
		
		Note: The output below is for illustrative purposes only. The example output below shows the control bridge configured.
		
		`# 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:29:58`
		`MTU:`
		`Bridge Interface: bond2`
		
		If the bridge has been configured, skip to the next step.
		Note: The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure.
		Note: 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.
		Note: 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 a bond containing an untagged interface
		`# netAdm add --device=<TVOE_NetBackup_Bridge_Interface>`
		`--onboot=yes --type=Bonding --mode=active-backup --miimon=100`
		`--MTU=<NetBackup_MTU_size>`
		`Interface <TVOE_NetBackup_Bridge_Interface> added`
		
		`# netAdm set --device=<ethernet_interface_5> --type=Ethernet`
		`--master=<TVOE_NetBackup_Bridge_Interface> --slave=yes`
		`--onboot=yes`
		`Interface <ethernet_interface_5> updated`
		
		`# netAdm add --type=Bridge --name=<TVOE_NetBackup_Bridge>`
		`--onboot=yes --bootproto=none --MTU=<NetBackup_MTU_size>`
		`--bridgeInterfaces=<TVOE_NetBackup_Bridge_Interface>`
		`--address=<TVOE_NetBackup_IP>`
		`--netmask=<TVOE_NetBackup_Netmask>`
		
		Option 2: Create NetBackup bridge using an untagged native interface:
		
		`# netAdm add --type=Bridge --name=<TVOE_NetBackup_Bridge>`
		`--onboot=yes --bootproto=none --MTU=<NetBackup_MTU_size>`
		`--bridgeInterfaces=<Ethernet_Interface_5>`
		`--address=<TVOE_NetBackup_IP>`
		`--netmask=<TVOE_NetBackup_Netmask>`
		
		Option 3: Create NetBackup bridge using a tagged device:
		
		`# netAdm add --device=<TVOE_NetBackup_Bridge_Interface>`
		`--onboot=yes`
		`Interface <TVOE_NetBackup_Bridge_Interface> added`

		# **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>**
7 ☐	**TVOE iLO:** Verify the Default Route	Note: The output below is for illustrative purposes only. The example output below shows the control bridge configured. # **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. **Note:** The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure. For this example add default route on management network. # **netAdm add --route=default --device=<TVOE_Management_Bridge>** **--gateway=<mgmt_gateway_address>** Route to <TVOE_Management_Bridge> added
8 ☐	**TVOE iLO:** Add NetBackup Route (Optional)	Add a route to the NetBackup network using one of the following commands. If the NetBackup network is routed: # **netAdm add --route=net** **--device=<TVOE_NetBackup_Bridge>** **--address=<NetBackup_Gateway_Network_Address>** **--netmask=<NetBackup_Gateway_netmask>** **--gateway=<NetBackup_gateway_ip_address>** Route to <TVOE_NetBackup_Bridge> added
9 ☐	**TVOE iLO:** Restart the network interfaces	Restart the network interfaces # **service network restart**
10 ☐	**TVOE iLO:** Set Hostname	Set the server hostname by running the following: # **su - platcfg** **1.** Navigate to **Server Configuration ➤ Hostname ➤ Edit**. **2.** Set TVOE Management Server hostname **3.** Press OK. **4.** Navigate out of Hostname
11 ☐	**TVOE iLO:** Set the time zone and/or hardware clock	**1.** Navigate to **Server Configuration ➤ Time Zone.** **2.** Select Edit. **3.** Set the time zone and/or hardware clock to **UTC** or appropriate time zone value. **4.** Press OK. **5.** Navigate out of Server Configuration

12 ☐	**TVOE iLO:** Set NTP	**1.** Navigate to **Network Configuration ➢ NTP**. **2.** Set NTP server IP address to point to the customer provided NTP server. **3.** Press OK. 4. Exit platcfg. Ensure that the time is set correctly by executing the following commands: # **service ntpd stop** # **ntpdate ntpserver1** # **service ntpd start**
13 ☐	**TVOE iLO:** Set SNMP	Set SNMP by running the following: # **su - platcfg** 1. Navigate to **Network Configuration ➢ SNMP Configuration ➢ NMS Configuration**. 2. Select **Edit** and then choose Add a New NMS Server. The 'Add an NMS Server' page will be displayed. 3. Complete the form by entering in all information about the SNMP trap destination. Create an entry for the customer SNMP server and another entry for the 4. NO VIP (if 2 tier deployment) or SO VIP (if 3 tier system. Select **OK** to finalize the configuration. The 'NMS Server Action Menu' will now be displayed. Select **Exit**. The following dialogue will then be presented. 5. Select **Yes** and then wait a few seconds while the Alarm Routing Service is restarted. At that time the SNMP Configuration Menu will be presented. 6. exit platcfg.

14 ☐	**TVOE iLO:** Configure NetBackup (Optional)	If the NetBackup feature is enabled for this system, configure the appropriate NetBackup client on the PM&C TVOE host.
		
		1. Enable and start the TVOE-netbackup service using the following commands:
		
		`# service_conf add TVOE-netbackup rc runlevels=345`
		`# service_conf reconfig`
		`# service TVOE-netbackup start`
		
		2. Enable platcfg to show the Netbackup Menu Items by executing the following commands:
		
		`# platcfgadm --show NBConfig;`
		`# platcfgadm --show NBInit;`
		`# platcfgadm --show NBDeInit;`
		`# platcfgadm --show NBInstall;`
		`# platcfgadm --show NBVerifyEnv;`
		`# platcfgadm --show NBVerify;`
		
		3. Create LV and filesystem for Netbackup client software on the vgguests volume group:
		
		`# echo "lv --mountpoint=/usr/openv --size=2G --name=netbackup_lv --vg=vgguests" > /tmp/nb.lvm`
		
		`# /usr/TKLC/plat/sbin/storageMgr /tmp/nb.lvm`
		
		This will create the LV, format it with a filesystem, and mount it under /usr/openv/. Example output is shown below:
		`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.`
		`The LV for netbackup has been created!`
		
		4. Install the netbackup client software:
		
		Refer to Appendix J on instructions how to install the netbackup client.
		
		Note: Skip any steps relating to copying netbackup "notify" scripts to /usr/openv/netbackup/bin. The TVOE netbackup notify scripts are taken care of in the next step.
		
		5. Create softlinks for TVOE specific netbackup notify scripts.
		
		`# ln -s /usr/TKLC/plat/sbin/bpstart_notify /usr/openv/netbackup/bin/bpstart_notify`
		
		`# ln -s /usr/TKLC/plat/sbin/bpend_notify /usr/openv/netbackup/bin/bpend_notify`
		
		Note: Once the Netbackup Client is installed on TVOE, the NetBackup Master should be configured to backup the following files form the TVOE host:
		• `/var/TKLC/bkp/*.iso`

15 ☐	**Management server iLO:** Setup syscheck	syscheck must be configured to monitor bonded interfaces. Replace "bondedInterfaces" with "bond0" or "bond0,bond1" if segregated networks are used: # **syscheckAdm net ipbond --set --var=DEVICES --val=<bondedInterfaces>** # **syscheckAdm net ipbond --enable** # **syscheck –v net ipbond**
16 ☐	**TVOE iLO:** Verify Server Health	Execute the following: # **alarmMgr --alarmStatus** This command should return no output on a healthy system. If any alarms are reported, contact Customer Care Center.
17 ☐	**Management server iLO:** Perform a TVOE backup using TPD platcfg utility	Execute the following: # **su - platcfg** Navigate to **Maintenance ➢ Backup and Restore** Select "**Backup Platform (CD/DVD)**" **Note:** If no cdrom device is found by TPD, you will receive an error dialog with the message: "No disk device available. This is normal on systems without a cdrom device." Press enter to continue. Select an applicable backup option (e.g. Build ISO file only), and press enter to continue. Exit from TPD platcfg utility. The TVOE backup can be found in the "/var/TKLC/bkp/" directory, and is prefixed by the server hostanem. An example of a TVOE backup ISO follows: /var/TKLC/bkp/RMS503u14-plat-app-201210301505.iso Move the TVOE backup to a customer provided backup server for safe keeping.

4.2 Install PM&C

Procedure 4. PM&C Deployment Procedure

S T E P #	This procedure will deploy PM&C on the TVOE Host **Prerequisite:** Procedure 3. TVOE/Management Server Network Configuration has been completed. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**TVOE iLO:** Login and launch the integrated remote console	Log in to iLO in IE using password provided by application: `http://<management_server_iLO_ip>` Click in the `Remote Console` tab and launch the `Integrated Remote Console` on the server. Click `Yes` if the `Security Alert` pops up.

2 ☐	**TVOE iLO:** Mount the PM&C media to the TVOE Management server	If using a DVD media, insert the pmac DVD into the optical drive and execute the following to get the Optical Drive letter and mount it:
		
		`# getCDROM`
		`DV-W28E-RW|sr0`
		`/dev/sr0`
		
		`# mount -t iso9660 /dev/sr0 /mnt/upgrade/`
		
		If using a USB Drive, run the following to mount it:
		
		`# ls /media/*/*.iso`
		`/media/sdd1/872-2441-104-5.0.0_50.8.0-PMAC-x86_64.iso`
		
		Use the output of the previous command to populate the next command
		
		`# mount -o loop /media/sdd1/872-2441-104-5.0.0_50.8.0-PMAC-x86_64.iso /mnt/upgrade`
		
		If using an ISO image, run the following to mount it:
		
		`# mount -o loop ISO_FILENAME.iso /mnt/upgrade`
		
		Validate the pmac media by executing the following commands:
		
		`# cd /mnt/upgrade/upgrade`
		
		`# .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 failes, the media is not valid and should not be used.

3 ☐	**TVOE iLO:** deploy PM&C	Using the pmac-deploy script, deploy the PM&C instance using the configuration captured during the site survey. # **cd /mnt/upgrade/upgrade** If deploying PM&C without netbackup feature, run the following command: # **./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>** **--routeGW=<PMAC_Management_gateway_address>** **--ntpserver=<TVOE_Management_server_ip_address>** If deploying PM&C with netbackup feature, run the following command: # **./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>** **--routeGW=<PMAC_Management_gateway_address>** **--ntpserver=<TVOE_Management_server_ip_address>** **--netbackupVol** **--bridge=<TVOE_NetBackup_Bridge>** **--nic=netbackup** The PM&C will deploy and boot. The management and control network will come up based on the settings that were provided to the pmac-deploy script. Note that this step takes between 5 and 10 minutes.
4 ☐	**TVOE iLO:** Unmount the media	The media should auto-unmount, if it does not, unmout the media using the following command: # **cd /** # **umount /mnt/upgrade** Remove the media from the drive.

5 ☐	**TVOE iLO:** SSH into the Management Server	Using an SSH client such as putty, ssh to the TVOE host using root credentials.
		
		Login using **virsh**, and wait until you see the login prompt :
		
		`virsh # list`
		`Id Name State`
		`----------------------------------`
		`13 myTPD running`
		`20 pmacdev7 running`
		
		`virsh # console pmacdev7`
		
		`[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`
		`pmacdev7 login:`

6 ☐	**Virtual PM&C:** Verify the PM&C is configured correctly on first boot	Run the following command (there should be no output): `# ls /usr/TKLC/plat/etc/deployment.d/`

7 ☐	**Virtual PM&C:** Set the PM&C timezone	Determine the TimeZone to be used for the PM&C
		
		Note: Valid time zones can be found in Appendix J
		
		Run
		
		`# set_pmac_tz.pl <timezone>`
		
		For example
		
		`# set_pmac_tz.pl Etc/UTC`
		
		Verify that the timezone has been updated:
		
		`# date`

8 ☐	**Virtual PM&C:** Set SNMP	Set SNMP by running the following: `# su - platcfg` 1. Navigate to **Network Configuration ➢ SNMP Configuration ➢ NMS Configuration**. 2. Select **Edit** and then choose Add a New NMS Server. The 'Add an NMS Server' page will be displayed. 3. Complete the form by entering in all information about the SNMP trap destination (generally the SO VIP should be used). Select **OK** to finalize the configuration. The 'NMS Server Action Menu' will now be displayed. Select **Exit**. The following dialogue will then be presented. 4. Select **Yes** and then wait a few seconds while the Alarm Routing Service is restarted. At that time the SNMP Configuration Menu will be presented. 5. exit platcfg.

9 ☐	**Virtual PM&C:** Reboot the server	Reboot the server by running: # **init 6**

4.3 Gather and Prepare Configuration Files

Procedure 5. Gather/Prepare Configuration Files

S T E P #		
	Use this procedure to gather and prepare configuration files that are required to proceed with the DSR 4.x installation. **Needed material:** - HP Misc. Firmware DVD - HP Solutions Firmware Upgrade Pack Release Notes [1] - Application CD or ISO Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	

1
☐
	TVOE Host: Get the application ISO	Once the PM&C is done rebooting, SSH to the PM&C server as root using the PM&C Management Network IP. Depending on whether the PM&C server is a VM guest, or installed directly on a rack-mount server, and depending on whether your upgrade media is an actual DVD disk or an ISO image, make the upgrade media available to the server.
		
		Since the PM&C is installed as a guest VM on TVOE, mount the media on the TVOE Host using one of the following commands:
		
		1. If the DSR 4.x application in on a physical disk, insert disk into the drive. Determine the cdrom of the server
		`# getCDROM`
		`/dev/sr0` (the physical Optical Drive for this server)
		`/dev/sr1` (Virtual Optical Drive)
		Mount the Optical media
		`# mkdir /media/cdrom`
		`# mount /dev/sr0 /media/cdrom`
		
		2. If using a USB Drive, run the following to mount it:
		`# ls /media/*/*.iso`
		`/media/sdd1/872-2507-111-4.1.0_41.16.2-DSR-x86_64.iso`
		
		Use the output of the previous command to populate the next command
		`# mount -o loop /media/sdd1/872-2507-111-4.1.0_41.16.2-DSR-x86_64.iso /mnt/upgrade`
		
		3. If the DSR in on an ISO, mount it using the following commands
		`# mkdir /media/cdrom`
		`# mount -o loop <path to ISO> /media/cdrom`

Procedure 5. Gather/Prepare Configuration Files

2 ☐	**Management server:** Get Netconfig , csv, and other support files from the application ISO	If the PM&C in installed on directly on the RMS, execute the following commands to copy the required files (Optionally, these files can be retrieved from the NAPD):
		`# cp -R /media/cdrom/upgrade/overlay/* /usr/TKLC/smac/etc`
		If using a CDROM or ISO, unmount it using the following command:
		`# umount /media/cdrom`
		If the PM&C in installed as a TVOE Guest, execute the following commands to copy the required files: Note that the **<PMAC Management_IP Address>** is the one used to deploy PM&C in procedure 4, step 3
		`# scp -R /media/cdrom/upgrade/overlay/*`
		`root@<PMAC Management_IP Address>:/usr/TKLC/smac/etc`
		If using a CDROM or ISO, unmount it using the following command:
		`# umount /media/cdrom`
		Remove the DSR 4.x application media from the management server.

3 ☐	**Management server:** Copy IOS images into place (this will copy both the 4948E and 3020 IOS images into place).	Insert the *Misc. Firmware* media into the CD or USB drive of the management server. For this step, be sure to use the correct IOS version specified by the *Firmware Upgrade Pack Release Notes[1]*. Copy each IOS image called out by the release notes [1].
		If using a CDROM drive, mount it using the following command. If using a USB, skip this command as it will get auto-mounted:
		`# mount /dev/sr0 /media/cdrom`
		Execute the following commands to copy the required files. Note that the **<PMAC Management_IP Address>** is the one used to deploy PM&C in procedure 4, step 3
		`# scp –p /media/cdrom/files/<4948E_IOS_image_filename>`
		`root@<PMAC Management_IP Address>:/var/TKLC/smac/image`
		`# scp –p`
		`/media/cdrom/files/<3020(6120)_IOS_image_filename>`
		`root@<PMAC Management_IP Address>:/var/TKLC/smac/image`
		Note that If both 3020 and 6120 enclosure switches are present, make sure you copy the images for both type of switches by re-running the previous command.
		If using a CDROM drive, unmount it using the following command:
		`# umount /media/cdrom`
		Remove the *Misc. Firmware* media from the drive.

4 ☐		If configuring a system with Aggregation switches, continue to procedure 6. If configuring a system without aggregation switches, skip to procedure 7.

4.4 Configure Cisco 4948E Aggregation Switch

4.4.1 Configure Cisco 4948E/4948E-F Switch

The procedures in this section uses NetConfig to configure the switches.

Procedure 6. Configure Cisco 4948E/4948E-F Switch using NetConfig

S T E P #		
	This procedure will configure 4948E-4948E-F switches with an appropriate IOS and configuration specified by Platform Engineering and Application requirements. **Prerequisite:** This procedure assumes a recently IPM'ed TVOE server with a VM hosting the PM&C application. **Note:** Uplinks must be disconnected from the customer network prior to executing this procedure. One of the steps in this procedure will instruct when to reconnect these uplink cables. Refer to [2] *Diameter Signaling Router 4.0 on HP C-Class Networking Interconnect Technical Reference*, for more details. **Needed material:** - HP Misc. Firmware DVD - HP Solutions Firmware Upgrade Pack Release Notes [1] - Application CD/DVD Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**Management server iLO:** Log into Management Server	Log in to iLO in IE using password provided by application: **`http://<management_server_iLO_ip>`** Click in the **`Remote Console`** tab and launch the **`Integrated Remote Console`** on the server. Click **`Yes`** if the `Security Alert` pops up. If not already done so, login as root.

Procedure 6. Configure Cisco 4948E/4948E-F Switch using NetConfig

2 ☐	**Management server:** setup conserver serial access to the switches	Before executing the step, make sure the switch is set to default. (refer to step 13 of this procedure on how to reset a switch back to default state).
		
		Configure the conserver service to enable serial access to the switches if you haven't already done so in the previous procedure:
		
		For switch1A:
		
		`# conserverAdm --addConsole --name=switch1A_console --device=/dev/ttyS4`
		
		For switch1B:
		
		`# conserverAdm --addConsole --name=switch1B_console --device=/dev/ttyS5`
		
		Note: if the name above was incorrectly entered, the console should be deleted using the following command and added again using the command above:
		
		`# conserverAdm --delConsole --name=<console_name>`
		
		Once the console is added, you should be returned to the command line prompt. If so, continue to the next step; if not, contact Customer Care Center for assistance.
		
		Open the conserver port on the firewall of the TVOE management server:
		
		`# iptables -I INPUT -s <pmac_mgmtVlan_ip_address>/255.255.255.255 -p all -j ACCEPT`
		
		`# service iptables save`

3 ☐	**Management server:** Login to the console of the virtual PM&C	Verify virtual PM&C installation by issuing the following commands as root on the management server:
		
		`# virsh list --all`
		
		`Id Name State`
		`----------`
		`6 vm-pmac1A running`
		
		Connect to the pmac VM name listed above using the following command, and login as root.
		
		`# 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`
		`vm-pmac1A login: root`
		`Password:`
		`Last login: Fri May 25 16:39:04 on ttyS4`

4 ☐	**Virtual PM&C:** Get IOS image information on the switches	Connect to switch1A, check the IOS version. Connect serially to switch1A by issuing the following command. `# /usr/bin/console -M <TVOE_server_mgmtVLAN_ip_address> -l platcfg switch1A_console` `Enter platcfg@pmac5000101's password: <platcfg_password>` `[Enter `^Ec?' for help]` `Press Enter`

Procedure 6. Configure Cisco 4948E/4948E-F Switch using NetConfig

		Switch> **show version | include image** System image file is "bootflash:cat4500-ipbasek9-mz.122-53.SG2.bin" Note the image version for comparison in a following step. To exit from the console, enter **<ctrl-e><c><.>** and you will be returned to the server prompt. Connect to switch1B, check the IOS version. Connect serially to switch1B by issuing the following command: # **/usr/bin/console -M <TVOE_server_mgmtVLAN_ip_address> -l platcfg switch1B_console** Enter platcfg@pmac5000101's password: **<platcfg_password>** [Enter `^Ec?' for help] Press **Enter** Switch> **show version | include image** System image file is "bootflash:cat4500-ipbasek9-mz.122-53.SG2.bin" Note the image version for comparison in a following step. To exit from the console, enter **<ctrl-e><c><.>** and you will be returned to the server prompt.
5 ☐	**Virtual PM&C:** Determine if switch IOS upgrade is required	For each switch, compare the IOS version from previous step with the IOS version specified in the Firmware Upgrade Pack Release Notes *[1]* for the switch model being used. If the version from previous step is equal the version from the release notes and it has "k9" in the name, denoting it has crypto support, then there is no upgrade necessary for this switch, instead skip to step 13 to erase any existing switch configuration. If only switch1B requires upgrade, skip to step 14. Otherwise, (upgrading only switch1A or upgrading both switch1A & switch1B), continue to step 6.
6 ☐	**Virtual PM&C:** Prepare the Virtual PM&C for tftp transfer of IOS file	Ensure that the tftp service is not running. A zero is expected. # **tpdProvd --client --noxml --ns=Xinetd getXinetdService service tftp** Login on Remote: **platcfg** Password of platcfg: 1 # If it returns a 1, need to stop it first by executing this command. # **tpdProvd --client --noxml --ns=Xinetd stopXinetdService service tftp force yes** Login on Remote: **platcfg** Password of platcfg: 1 # This should return a 1. Edit the `/etc/xinetd.d/tftp` file for the values in bold so that tftp will work appropriately: # **vim /etc/xinetd.d/tftp**

Procedure 6. Configure Cisco 4948E/4948E-F Switch using NetConfig

		service tftp
		{
		socket_type = dgram
		protocol = udp
		wait = yes
		user = root
		server = /usr/sbin/in.tftpd
		server_args = -s **/var/TKLC/smac/image**
		disable = **no**
		per_source = 11
		cps = 100 2
		flags = IPv4
		}
		#
		
		Ensure that the tftp service is now running. A "1" is expected.
		
		# tpdProvd --client --noxml --ns=Xinetd getXinetdService service tftp
		Login on Remote: **platcfg**
		Password of platcfg:
		1
		#
		
		If the output is "0" then, execute the commands that enable tftp transfer.
		
		# tpdProvd --client --noxml --ns=Xinetd startXinetdService service tftp
		Login on Remote: **platcfg**
		Password of platcfg: **<platcfg_password>**

7 ☐	**Virtual PM&C -> TVOE Server:** Manipulate host server physical interfaces.	Exit from the virtual pmac console, by entering < **ctrl-]** > and you will be returned to the server prompt. If upgrading the IOS on switch1A: Ensure that 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: **# ifdown <ethernet_interface_2>** **# ifup <ethernet_interface_1>** **# ip addr show <management_server_mgmtInterface> | grep inet** The command output should contain the IP address of the variable **<management_server_mgmtVLAN_ip_address>,** note it down. If upgrading the IOS on switch1B: Ensure that 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: **# ifdown <ethernet_interface_1>** **# ifup <ethernet_interface_2>** **# ip addr show <management_server_mgmtInterface> | grep inet** The command output should contain the IP address of the variable **<management_server_mgmtVLAN_ip_address>,** note it down. Connect to the Virtual PMAC by logging into the console of the virtual pmac instance found in step 3.

Procedure 6. Configure Cisco 4948E/4948E-F Switch using NetConfig

		# **virsh console vm-pmac1A**
8 ☐	**Virtual PM&C:** Attach to switch console	If upgrading the firmware on switch1A, connect serially to switch1A by issuing the following command as root on management server1A: # **/usr/bin/console -M <TVOE_server_mgmtVLAN_ip_address> -l platcfg switch1A_console** Enter platcfg@pmac5000101's password: **<platcfg_password>** Press RETURN to get started. 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** Switch# If upgrading the firmware on switch1B, connect serially to switch1A by issuing the following command as root on management server1B: # **/usr/bin/console -M <TVOE_server_mgmtVLAN_ip_address> -l platcfg switch1B_console** Enter platcfg@pmac5000101's password: **<platcfg_password>** Press RETURN to get started. 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** Switch#
9 ☐	**Virtual PM&C:** Configure port on the switch to be upgraded. To ensure connectivity, ping the management server's management vlan ip address from the switch.	Platform version specific to be on the management vlan: Switch# **conf t** Switch(config)# **vlan <switch_mgmtVLAN_id>** Switch(config)# **int vlan <switch_mgmtVLAN_id>** **If configuring switch1A, use this command:** Switch(config-if)# **ip address <switch1A_mgmtVLAN_ip_address> <netmask>** **If configuring switch1B, use this command:** Switch(config-if)# **ip address <switch1B_mgmtVLAN_ip_address> <netmask>** **If configuring either switch1A or switch1B, execute these commands:** Switch(config-if)# **no shut** Switch(config-if)# **int gi1/40** Switch(config-if)# **switchport mode trunk**

Procedure 6. Configure Cisco 4948E/4948E-F Switch using NetConfig

		Switch(config-if)# **spanning-tree portfast trunk** Switch(config-if)# **write mem** Switch(config-if)# **end** **Now issue ping command:** Switch# **ping <PM&C_mgmtVLAN_ip_address>** Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to <management_server_mgmtVLAN_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 , doublecheck that the procedure was completed correctly by repeating all steps up to this point. If after repeating those steps, ping is still unsuccessful, contact Tekelec Customer Service.
10 ☐	**Virtual PM&C (switch console session):** Upload the IOS to the switch and set it to be the active IOS and delete the previous IOS verison..	On the switch, copy the IOS file over to the switch by issuing the following command sequence: Switch> **en** Switch# **copy tftp: bootflash:** Address or name of remote host []? **<pmac_mgmtVLAN_ip_address>** Source filename []?**<IOS_Image_File>** Destination filename [<IOS_Image_File>]? **Enter** Press Enter here, you do NOT want to change the filename Accessing tftp://<pmac_mgmtVLAN_ip_address>/<IOS_Image_File>.. Loading <IOS_Image_File> from < pmac_mgmtVLAN_ip_address> (via Vlan2): !!!!!! [OK - 45606 bytes] 45606 bytes copied in 3.240 secs (140759 bytes/sec) Switch# **dir bootflash:** Directory of bootflash:/ 1 -rwx 17779888 May 11 2011 02:25:23 -05:00 cat4500-entservicesk9-mz.122-53.SG.bin 2 -rwx 17779888 May 11 2011 02:25:23 -05:00 cat4500-ipbasek9-mz.122-53.SG2.bin 60817408 bytes total (43037392 bytes free)
11 ☐	**Virtual PM&C (switch console session):** Set the active IOS image and config-register from the switch console session that was	Set the active IOS image: Switch# **conf t** Switch(config)# **boot system flash bootflash:<ios_image_file>** Switch(config)# **no boot system flash bootflash:< OLD_IOS_image_file>** Switch(config)# **config-register 0x2102**

Procedure 6. Configure Cisco 4948E/4948E-F Switch using NetConfig

	established.	Switch(config)# **end** Switch# **write memory** Switch# Verify the changes: Switch# **show run | include boot** boot-start-marker boot system flash bootflash: <ios_image_file> boot-end-marker Switch# **show version | include register** Configuration register is 0xXXXX (will be 0x2102 at next reload) Switch# **reload** Proceed with reload? [confirm] Wait until the switch reloads, then issue the following command to ensure the switch is at the appropriate IOS version: Switch> **show version | include image** System image file is "bootflash:cat4500-ipbasek9-mz.122-53.SG2.bin" If the switch is not at the appropriate version, stop here and contact Customer Care Center. If it is, move on to the next step.
12 ☐	**Virtual PM&C (switch console session):** Delete any other IOS images if there are multiple IOS images on the switch, delete the unused images.	Switch> **en** Switch# **show bootflash:** -#- --length-- -----date/time------ path 1 25771102 Jan 20 2012 08:20:08 <ios_image_file> 2 16332568 Jan 24 2012 18:54:44 <OLD_IOS_image> Switch# **delete /force /recursive bootflash:<OLD_IOS_image>** Repeat this step until the only image on the switch is <ios_image_file>
13 ☐	**Virtual PM&C (switch console session):** Reset the switch to factory defaults	Switch# **conf t** Switch(config)# **config-register 0x2101** Switch(config)# **no vlan 2-4094** Switch(config)# **end** Switch# **write erase** Switch# **reload** Wait until the switch reloads, then exit from console, enter **<ctrl-e><c><.>** and you will be returned to the server prompt.
14 ☐	**Virtual PM&C (switch console session):** Repeat for switch1B	Repeat steps 7-13 for switch1B, the continue to the next step.

Procedure 6. Configure Cisco 4948E/4948E-F Switch using NetConfig

15 ☐	**Virtual PM&C:** Turn off the tftp service of the virtual PM&C.	Issue the following command to stop the tftp service:
		
		`# tpdProvd --client --noxml --ns=Xinetd stopXinetdService service tftp`
		`Login on Remote: platcfg`
		`Password of platcfg: <platcfg_password>`

16 ☐	**Virtual PM&C:** Setup netConfig repository with necessary console information	Use netConfig to create a repository entry that will use the conserver service that was configured in the previous steps. This command will give the user several prompts. The prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as an answer must be entered EXACTLY as they are shown here.
		
		`# netConfig --repo addService name=console_service`
		`Service type? (tftp, ssh, conserver, oa) conserver`
		`Service host? <TVOE_server_mgmtVLAN_ip_address>`
		`Enter an option name (q to cancel): user`
		`Enter a value for user: platcfg`
		`Enter an option name(q to cancel): password`
		`Enter a value for password: <platcfg_password>`
		`Enter an option name(q to cancel): q`
		`Add service for console_service successful`
		
		To check that you entered the information correctly, use the following command:
		
		`# netConfig --repo showService name=console_service`
		
		and check the output, which will be similar to the one shown below:
		
		`[root@pmac5000101 ~]# netConfig --repo showServices --name=console_service`
		
		`Services:`
		`  Service Name: console_service`
		`  Type: conserver`
		`  Host: 10.240.8.47`
		`  Options:`
		`  password: D8396824B3B2B9EE`
		`  user: platcfg`
		`[root@pmac5000101 ~]#`

Procedure 6. Configure Cisco 4948E/4948E-F Switch using NetConfig

17 ☐	**Virtual PM&C:** Setup netConfig repository with necessary tftp information	Use netConfig to create a repository entry that will use the tftp service. This command will give the user several prompts. The prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as an answer must be entered EXACTLY as they are shown here.
		
		`# netConfig --repo addService name=tftp_service`
		`Service type? (tftp, ssh, conserver, oa) tftp`
		`Service host? <pm&c_mgmtVLAN_ip_address>`
		`Enter an option name (q to cancel): dir`
		`Enter a value for user: /var/TKLC/smac/image`
		`Enter an option name(q to cancel): q`
		`Add service for tftp_service successful`
		
		To check that you entered the information correctly, use the following command:
		
		`# netConfig --repo showService name=tftp_service`
		
		and check the output, which will be similar to the one shown below:
		
		`Services:`
		`Service Name: tftp_service`
		`Type: tftpr`
		`Host: 10.240.8.4`
		`Options:`
		`dir: /var/TKLC/smac/image`
		`[root@pmac5000101 ~]#`

Procedure 6. Configure Cisco 4948E/4948E-F Switch using NetConfig

18 ☐	**Virtual PM&C:** Setup netConfig repository with necessary ssh information.	Use netConfig to create a repository entry that will use the ssh service. This command will the user several prompts. The prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as answer must be entered EXACTLY as they are shown here.
		
		Note that the switch_backup_user_password below is not the same as the switch password (for c-Class it is the password of the PMAC).
		
		`# netConfig --repo addService name=ssh_service`
		`Service type? (tftp, ssh, conserver, oa) ssh`
		`Service host? <pm&c_mgmtVLAN_ip_address>`
		`Enter an option name (q to cancel): user`
		`Enter a value for user: <switch_backup_user>`
		`Enter an option name(q to cancel): password`
		`Enter a value for password: <switch_backup_user_password>`
		`Enter an option name(q to cancel): q`
		`Add service for console_service successful`
		
		To check that you entered the information correctly, use the following command:
		
		`# netConfig --repo showService name=ssh_service`
		and check the output, which will be similar to the one shown below:
		
		`[root@pmac5000101 ~]# netConfig --repo showServices --name=ssh_service`
		
		`Services:`
		`Service Name: ssh_service`
		`Type: ssh`
		`Host: 10.240.8.4`
		`Options:`
		`password: D8396824B3B2B9EE`
		`user: root`
		`[root@pmac5000101 ~]#`

Procedure 6. Configure Cisco 4948E/4948E-F Switch using NetConfig

19 ☐	**Virtual PM&C:** Setup netConfig repository with switch1A information	Use netConfig to create a repository entry for switch1A. This command will give the user several prompts. The prompts with <variables> as the answers are site specific that the user MUST modify.
		Other prompts that don't have a <variable> as an answer must be entered EXACTLY as they are shown here.
		
		`# netConfig --repo addDevice name=switch1A --reuseCredentials`
		`Device Vendor? Cisco`
		`Device Model? 4948E`
		`Should the init oob adapter be added (y/n)? y`
		
		`Adding consoleInit protocol for switch1A 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?`
		`switch1A_console`
		`What is the device console password? <switch_console_password>`
		`Verify Password <switch_console_password>`
		`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 live network adapter be added (y/n)? y`
		`Adding cli protocol for switch1A using network...`
		`What is the address used for network device access?`
		`<switch1A_mgmtVLAN_ip_address>`
		`Should the live oob adapter be added (y/n)? y`
		`Adding cli protocol for switch1A using oob...`
		`OOB device access already set: console_service`
		`Device named switch1A successfully added.`
		
		To check that you entered the information correctly, use the following command:
		`# netConfig --repo listDevices`
		and check the output, which will be similar to the one shown below.
		Note: Only switch 1A info has been shown in this example.
		`[root@pmac5000101 ~]# netConfig --repo listDevices`
		`Devices:`
		
		`Device: switch1A`
		`  Vendor: Cisco`
		`  Model: 4948`
		`  Access: Network: 10.240.8.2`
		`  Access: OOB:`
		`  Service: console_service`
		`  Console: switch1A_console`
		`  Init Protocol Configured`
		`  Live Protocol Configured`
		`[root@pmac5000101 ~]#`

Procedure 6. Configure Cisco 4948E/4948E-F Switch using NetConfig

20 ☐	**Virtual PM&C:** Setup netConfig repository with switch1B information	Use netConfig to create a repository entry for switch1B. This command will give the user several prompts. The prompts with <variables> as the answers are site specific that the user MUST modify.
		Other prompts that don't have a <variable> as an answer must be entered EXACTLY as they are shown here.
		
		`# netConfig --repo addDevice name=switch1B --reuseCredentials`
		`Device Vendor? Cisco`
		`Device Model? 4948E`
		`Should the init oob adapter be added (y/n)? y`
		
		`Adding consoleInit protocol for switch1B 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?`
		`switch1B_console`
		`What is the device console password? <switch_console_password>`
		`Verify Password <switch_console_password>`
		`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 live network adapter be added (y/n)? y`
		`Adding cli protocol for switch1A using network...`
		`What is the address used for network device access?`
		`<switch1B_mgmtVLAN_ip_address>`
		`Should the live oob adapter be added (y/n)? y`
		`Adding cli protocol for switch1B using oob...`
		`OOB device access already set: console_service`
		`Device named switch1B successfully added.`
		
		To check that you entered the information correctly, use the following command:
		`# netConfig --repo listDevices`
		and check the output, which will be similar to the one shown below.
		Note: Only the switch1B info has been shown in this example. If the previous step and this step were done correctly, both switch1A and switch1B entries would show up.
		`[root@pmac5000101 ~]# netConfig --repo listDevices`
		`Devices:`
		
		`Device: switch1B`
		`  Vendor: Cisco`
		`  Model: 4948`
		`  Access: Network: 10.240.8.3`
		`  Access: OOB:`
		`  Service: console_service`
		`  Console: switch1B_console`
		`  Init Protocol Configured`
		`  Live Protocol Configured`
		`[root@pmac5000101 ~]#`

Procedure 6. Configure Cisco 4948E/4948E-F Switch using NetConfig

21 ☐	**Virtual PM&C:** Modify configure xml file with information needed to initialize the switch.	Note that the files that are created in this step can be prepared ahead of time using the NAPD.
		
		Extract the configuration files from the tar file copied in procedure 5
		
		`# cd /usr/TKLC/smac/etc`
		
		`# tar xvzf DSR4.0_NetConfig_templates*`
		
		This will create a directory called **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
		
		`# cp init/Aggregation/* .`
		`# cp config/TopoX/* .` (Make sure to replace X with the appropriate Topology number)
		
		Update the 4948E init and configure xml files to match your network parameters. Values to be modified by the user will be notated in this step by a preceding dollar sign. So a value that has **$<some_variable_name>** will need to be modified, removing the dollar sign and the less than, greater than sign.
		
		`# vi /usr/TKLC/smac/etc/switch1A_4948_E_E-F_cClass_template_init.xml`
		
		`# vi /usr/TKLC/smac/etc/switch1B_4948_E_E-F_cClass_template_init.xml`
		
		`# vi /usr/TKLC/smac/etc/4948E-F_L3_configure.xml`

22 ☐	**Virtual PM&C:** Initialize switch1A	Initialize switch1A by issuing the following command: `# netConfig --file=/usr/TKLC/smac/etc/switch1A_4948_4948E_init.xml` Processing file: /usr/TKLC/smac/etc/switch1A_4948_4948E_init.xml # Note: This step takes about 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 Customer Care Center. A successful completion of netConfig will return the user to the prompt.
23 ☐	**Virtual PM&C:** Initialize switch1B	Initialize switch1B by issuing the following command: `# netConfig --file=/usr/TKLC/smac/etc/switch1B_4948_4948E_init.xml` Processing file: /usr/TKLC/smac/etc/switch1B_4948_4948E_init.xml # Note: This step takes about 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 Customer Care Center. A successful completion of netConfig will return the user to the prompt.

Procedure 6. Configure Cisco 4948E/4948E-F Switch using NetConfig

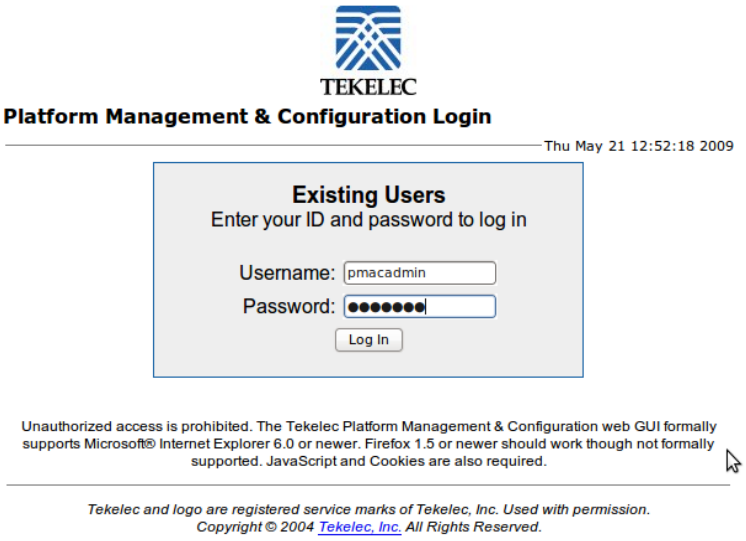
24 ☐	**Virtual PM&C:** Configure the switches	Configure both switches by issuing the following command: # **netConfig --file=/usr/TKLC/smac/etc/4948_4948E_configure.xml** Processing file: /usr/TKLC/smac/etc/4948_4948E_configure.xml **Note:** This step takes about 2-3 minutes to complete. Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Customer Care Center.
25 ☐	**Virtual PM&C:** Verify switch configuration	Ping each of the interfaces to verify switch configuration # **ping <switch1A_mgmtVLANIP>** # **ping <switch1B_mgmtVLANIP>**
26 ☐	**Cabinet:** Connect Uplinks of Switch1A	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.
27 ☐	**Virtual PM&C:** Verify access to customer network	Verify connectivity to the customer network by issuing the following command # **ping <customer_supplied_ntp_server_address>**
28 ☐	**Cabinet:** Connect Uplinks of Switch1B	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.
29 ☐	**Virtual PM&C:** Verify access to customer network	Verify connectivity to the customer network by issuing the following command # **ping <customer_supplied_ntp_server_address>**
30 ☐	**Virtual PM&C:** Re-attach uplinks of switch1A	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
31 ☐	**Management server:** Restore the TVOE host back to its original state.	Exit from the virtual pmac console, by entering **<ctrl-]>** and you will be returned to the server prompt. Restore the server networking back to original state: # **service network restart**

Procedure 6. Configure Cisco 4948E/4948E-F Switch using NetConfig

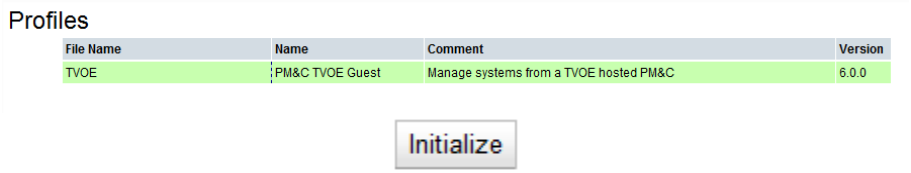
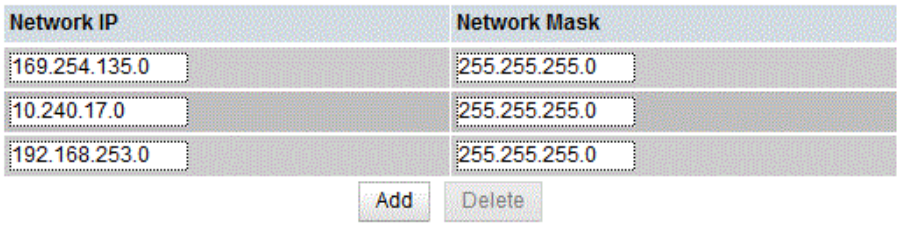
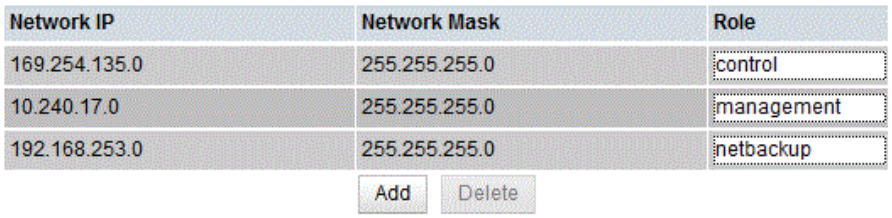
32 ☐	**Management server:** Backup Switch Configuration	Ensure the directory where the backups will be stored exists using the following command: # **ls /usr/TKLC/smac/etc/switch/backup** If an error is returned saying "No such file or directory", then create the directory using the following command # **mkdir /usr/TKLC/smac/etc/switch/backup** Change the currect path to the newly created directory using the following command # **cd /usr/TKLC/smac/etc/switch/backup** Execute the backup command to backup switch 1A # **netConfig --device=switch1A backupConfiguration service=ssh_service filename=switch1A-backup** Execute the backup command to backup switch 1B # **netConfig --device=switch1B backupConfiguration service=ssh_service filename=switch1B-backup** Verify switch configuration was backed up by cat <switch_name>-backup and inspect its contents to ensure it reflects the latest knwon good switch configurations.

4.5 Configure PM&C Server

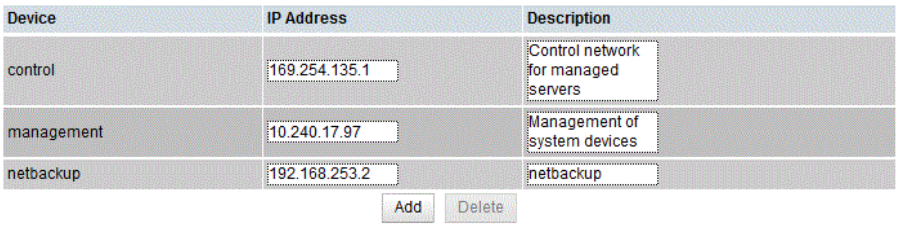
Procedure 7. Configure the PM&C Server

S T E P #		
	This procedure will provide PM&C configuration using the web interface. **Prerequisite:** *Procedure 4. PM&C Deployment Procedure* has been completed. **Note:** The installer must be knowledgeable of the network. If you make mistake, click Cancel and try again. The finish step may take longer time because it reconfigures the network and attempts to connect may fail. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**PM&C GUI:** Load GUI initialization wizard	Open web browser and enter: **http://<management_network_ip>/gui** Login as pmacadmin user. 

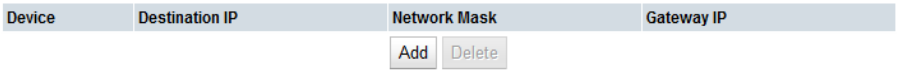
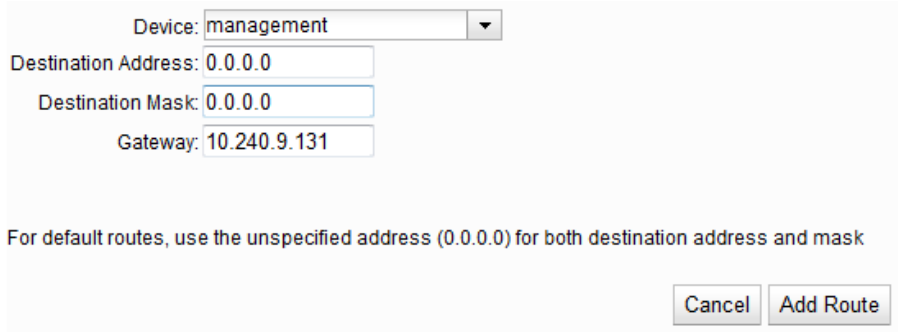
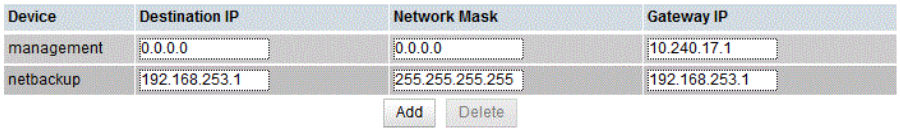
Procedure 7. Configure the PM&C Server

2 ☐	**PM&C GUI:** Select a profile	The first screen will be similar to image below.  Select the TVOE profile and click on **Initialize**, then set the role for SERVER.IPM are set to **Control** while the roles for all other features is set to **Management.** Also make sure that the enabled checkbox is checked for the following: DEVICE.NETWORK.NETBOOT DEVICE.NTP PMAC.REMOTE.BACKUP SERVER:IPM PMAC.NETBACKUP (only if NetBackup is used) And click on **Next.** 
3 ☐	**PM&C GUI:** Network Description	You will see this default screen similar to: **Note:** In the example below the NetBackup network was provisioned and added.  Enter the `Network IPs` and `Netmasks` for the control and Management Networks. Click **`Next`**.
4 ☐	**PM&C GUI:** Network Roles	You will see this default screen similar to: **Note:** In the example below the NetBackup network was provisioned and added  Verify the `Roles` and update if necessary. Click **`Next`**.

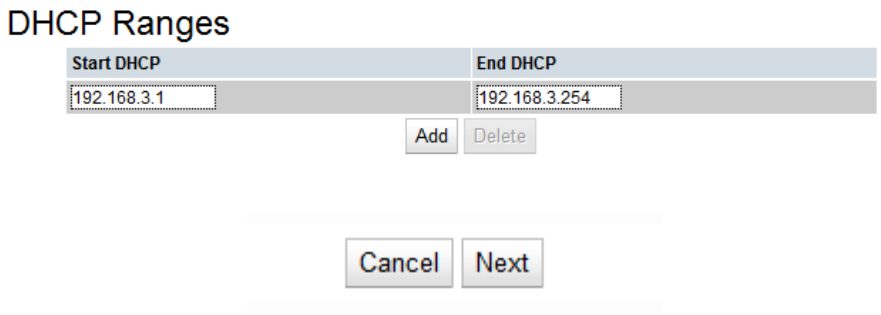
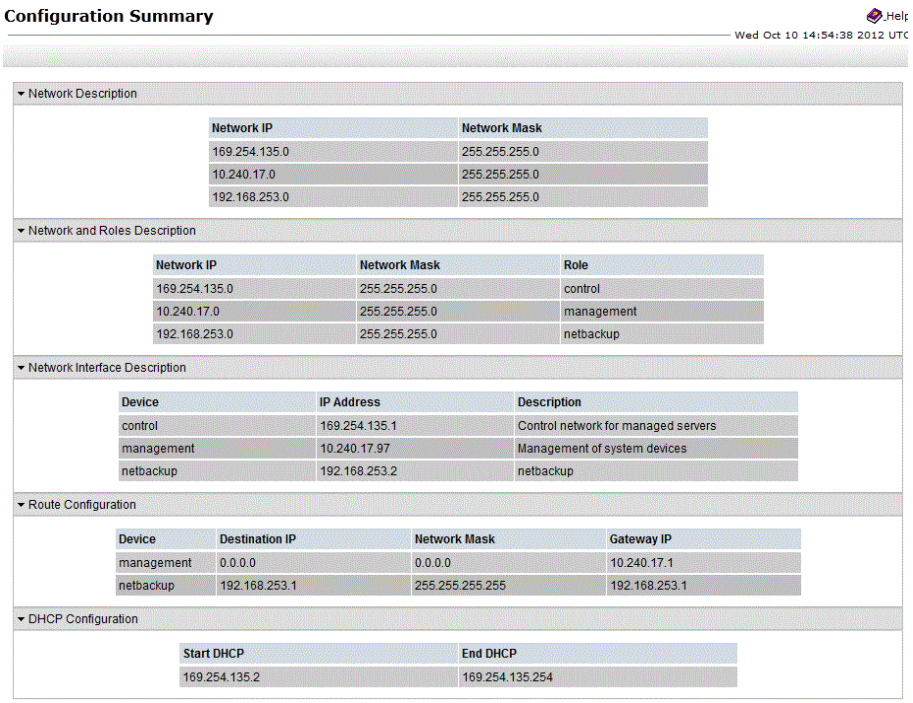
Procedure 7. Configure the PM&C Server

5 ☐	**PM&C GUI:** Network Interface	You will see this default screen similar to: **Note:** In the example below the NetBackup network was provisioned and added  Verify the IP addresses for each Device and update if necessary. Click **Next**.

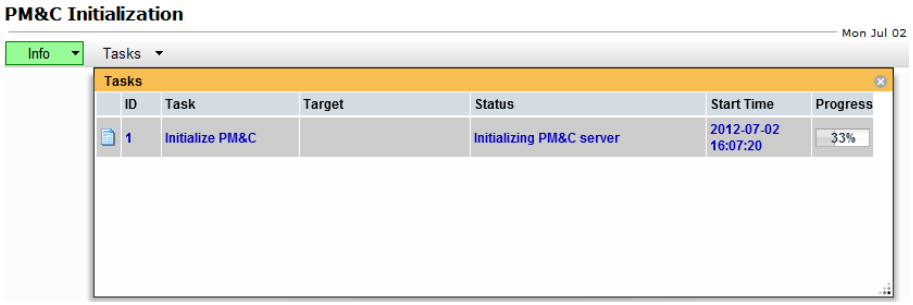
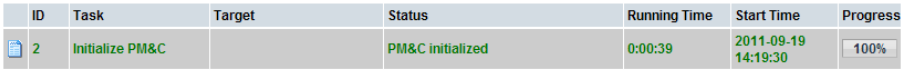
Procedure 7. Configure the PM&C Server

6 ☐	**PM&C GUI:** Network Route	You will see a screen similar to:  Click **Add** to create new routes. For the default route, select the "management" Device, enter "0.0.0.0" for both Destination Address and Destination Mask, and enter the gateway IP under Gateway as shown below  If NetBack is defined, add a corresponding NetBackup Route **NOTE:** If the NetBackup network in non-routed, a host route should be used instead of a network route. (A host route has the following values: Netmask=255.255.255.255 and Gateway IP = Netbackup IP) Below is an example of default and Netbackup routes. In this example, a host route is used to the NetBackup Network.  Click **Add Route.** Repeat to define more route. Click **Next** when done.

Procedure 7. Configure the PM&C Server

7 ☐	**PM&C GUI:** DHCP Ranges	You will see this default screen similar to:  If you need to define additional DHCP ranges, press Add (most deployments DO NOT require additional DHCP Ranges, Otherwise, click **Next**.
8 ☐	**PM&C GUI:** Settings summary	The following summary screen will be displayed.  Verify the values and click **Finish**.

Procedure 7. Configure the PM&C Server

9 ☐	**PM&C GUI:** Complete the configuration	The following summary screen will be displayed, click on Tasks to view the Initialization Progress.  Click **`Task Monitoring`** for status of this task.  Wait till the Progress bar turns green, that signifies that the PMAC Initialization was successful.

10 ☐	**PM&C Command Line:** Perform a system healthcheck	Execute the following commands:
		`# alarmMgr --alarmStatus`
		This command should return no output on a healthy system.
		`# sentry status`
		All Processes should be running, displaying output similar to the following:
		`PM&C 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.`

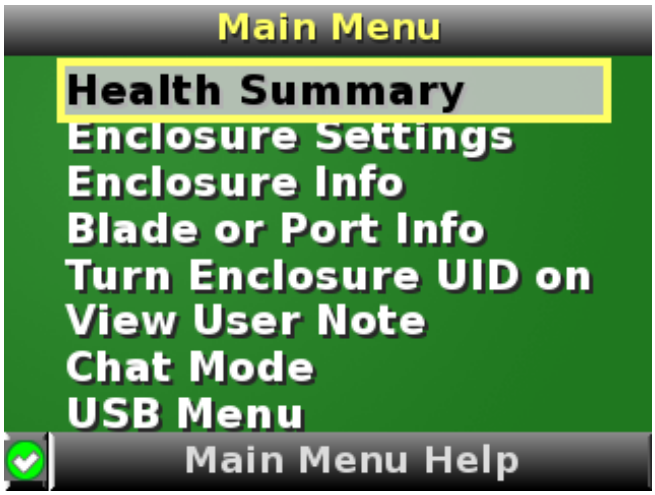
Procedure 7. Configure the PM&C Server

11 ☐	**PM&C Command Line:** Install NetBackup (Optional)	1. If the NetBackup client installation will rely on the TPD "nbAutoInstall" process to configure the PM&C NetBackup client perform the following at the PM&C Command Line, otherwise continue to sub bullet 2 below.
		`# mkdir -p /usr/openv/netbackup/bin/`
		`# ln -s /usr/TKLC/smac/sbin/bpstart_notify /usr/openv/netbackup/bin/`
		`# ln -s /usr/TKLC/smac/sbin/bpend_notify /usr/openv/netbackup/bin/`
		
		Use TPD platcfg utility to add the NetBackup Server's alias and IP to the "/etc/hosts" file.
		
		2. Refer to [4] Platform 6.x Configuration Procedure Reference, procedure 3.8.14 for instructions on installing the NetBackup client on the Management Server.

12 ☐	**PM&C Command Line:** Perform a backup	Perform PM&C application backup using the following command:
		
		`# pmacadm backup`
		`PM&C backup been successfully initiated as task ID 7`
		`[root@PMACDev3 ~]#`
		
		Note: The backup runs as a background task. To check that status of the background task use the PM&C GUI Task Monitor page, or issue the command " **pmaccli getBgTasks** ". The result should eventually be "PM&C Backup successful" and the background task should indicate "COMPLETE".
		Note: The "pmacadm backup" command uses a naming convention which includes a date/time stamp in the file name (Example file name: backupPmac_20111025_100251.pef). In the example provided, the backup file name indicates that it was created on 10/25/2011 at 10:02:51 am server time.
		
		Next Verify that the backup was successful using the following command:
		`# pmaccli getBgTasks`
		`2: Backup PM&C COMPLETE - PM&C Backup successful`
		`Step 2: of 2 Started: 2012-07-05 16:53:10 running: 4`
		`sinceUpdate: 2 taskRecordNum:`
		`...`
		
		Once the backup has been verified that it was successful, copy the backup file to a remote location.

4.6 HP C-7000 Enclosure Configuration

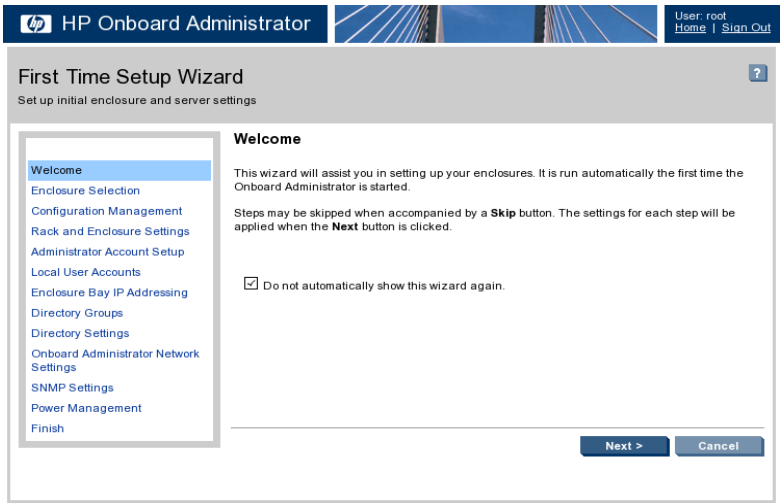
Procedure 8. Configure initial OA IP

S T E P #	This procedure will set initial OA IP address using the front panel display. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	Configure OA's IP	Configure OA's IP address using insight display on the front side of the enclosure. You will see following:  Navigate to **Enclosure Settings** ,press **OK**. 1. Go to the **OA1 IP** v4 and press **OK**. 2. Go to **OA1 IP** v4 and press **OK**. On the **OA1 Network Mode** screen choose **static** and press **Accept**. On the **OA1 IP address** screen fill in **IP**, **mask** and **gateway**. Press **Accept,** then press **Accept All,** and finally press **Accept All**. Note that the OA IP address should belong to the Plat Management Network

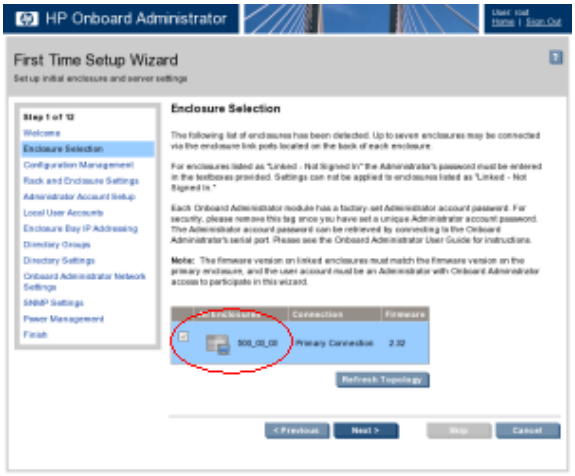
Procedure 9. Configure the OA (OA Configuration Wizard)

S T E P #	This procedure will configure initial OA settings. Configuration wizard will be used. **Prerequisite:** *Procedure 8. Configure initial OA IP* has been completed. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.

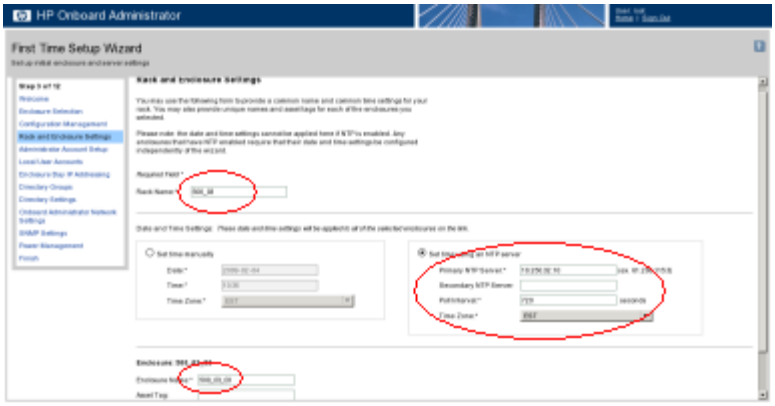
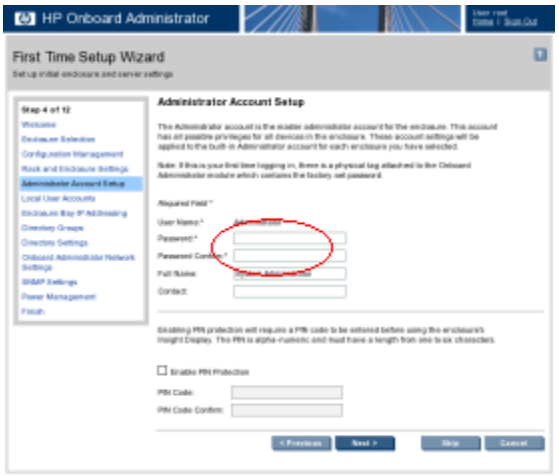
Procedure 9. Configure the OA (OA Configuration Wizard)

1 ☐	**OA GUI:** Login	Open your web browser and navigate to the OA IP address You will see following:  Login to HP OA as Administrator. Original password is on paper card attached to each OA.
2 ☐	**OA GUI:** Run First Time Setup wizard	You will see the main wizard window:  Click on **Next** to choose enclosure you want to configure .

Procedure 9. Configure the OA (OA Configuration Wizard)

3 ☐	**OA GUI:** Select enclosure	Choose enclosure:  Click on **Next**.
4 ☐	**OA GUI:** Skip Configuration Management	You will see *Configuration Management*. Skip this step. Click **Next**.

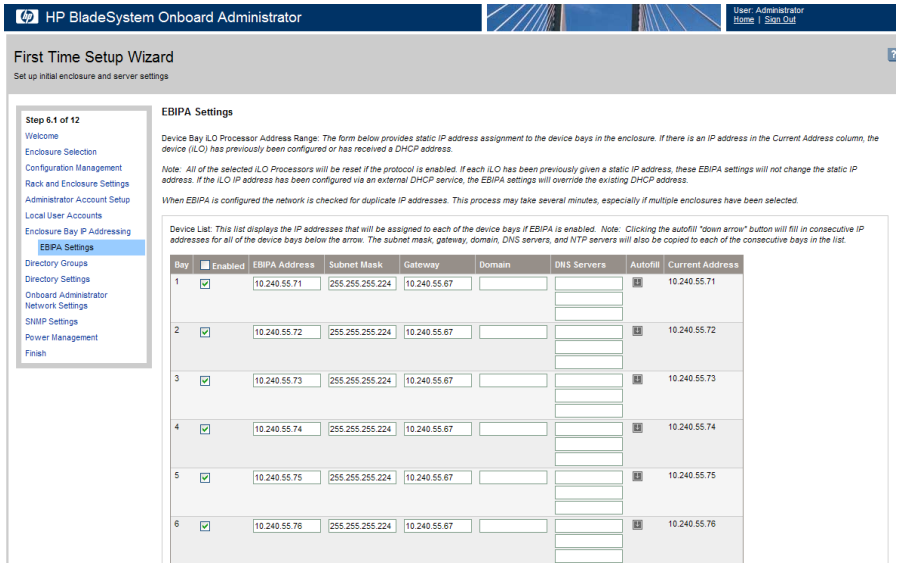
Procedure 9. Configure the OA (OA Configuration Wizard)

5 ☐	**OA GUI:** Rack and Enclosure Settings	You should see this screen:  Fill in **Rack Name** in format `xxx_xx`, where xxx_xx might refer to the lab name and rack position, e.g. 500_09 Fill in **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** item and fill in `Primary NTP server` (Should be the NTP Server provided by the customer). Set **Poll interval** to **720**. Set **Time Zone** to UTC or appropriate time zone value. Click on **Next**.
6 ☐	**OA GUI:** Change administrator password	You can see `Administrator Account Setup`:  `Change Administrator's password and click on` **Next**.

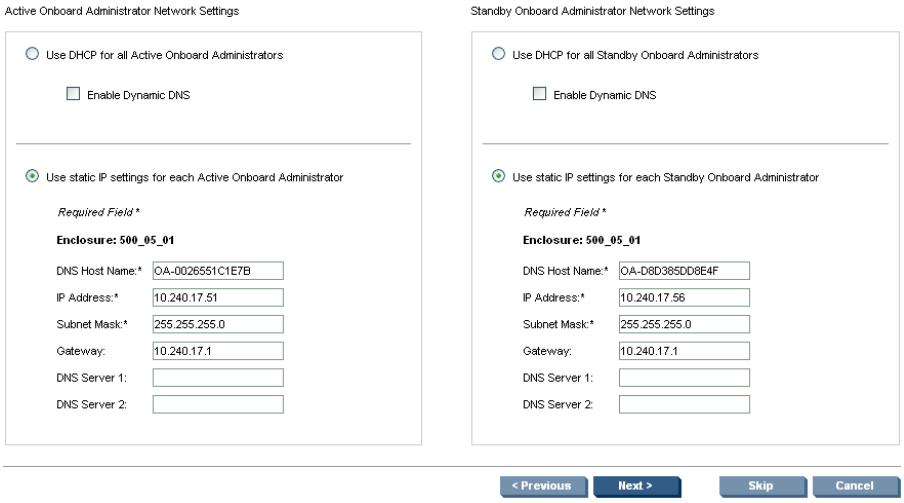
Procedure 9. Configure the OA (OA Configuration Wizard)

7 ☐	**OA GUI:** Create pmacadmin and root user	On the `Local User Accounts` screen click on **`New`** to add `pmacadmin` user. You will see `User Settings` screen. Fill in **`User Name`** and **`Password`**. **`Privilege Level`** set to **`Administrator`**. You will need to create the user: **`pmacadmin`**. Note that the password of the pmacadmin user defined on the OA is not the same as the pmacadmin password of PM&C GUI. Check the checkbox for **`Onboard Administrator Bays`** under the User Permissions section. Then click on **`Add User`**. In the same way create **`root`** user. Then click on **`Next`**.

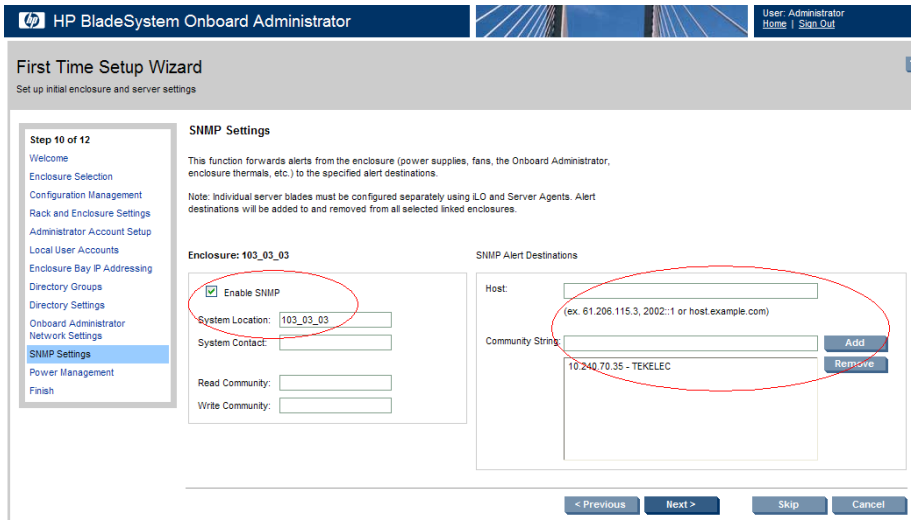
Procedure 9. Configure the OA (OA Configuration Wizard)

8 ☐	**OA GUI:** EBIPA settings	On the `EBIPA Settings` (Enclosure Bay IP Addressing) screen click on **`Next`** to continue or **`Skip`** if you have already did it. If you pressed **`Skip`** go to the Step 9 of this procedure. **Note:** Setting up the EBIPA addresses is required.  Fill in ILO's IPs, Subnet Masks and Gateways in the `Device list`. Note that those IPs need to belong to the Plat Mgmt Network. You can use autofill button which will sequentially fill in IP addresses below the current entry. Click **`Enabled`** to enable all servers. Also note that for full height blades (which each takes 2 slots in the enclosure eg slot 1 and slot 9), provision the IP for the upper slot and leave the bottom slot blank. Do not fill ILO IPs for the Bays 1A-16A and 1B-16B. We do not use them. **Note:** bays 1A-16A and 1B-16B are used for double-density blades (f.e. BL2x220c) which are not supported in this release. Click on the `Interconnect Bays` tab and fill in the IP addresses, Subnet Masks, and Gateways that will be assigned to the interconnect bays in the rear of the enclosure (3020 or 6120 switches) and enable them. By clicking **`Next`** you will apply those settings. System will restart devices such as interconnect devices or iLOs to apply new addresses. After finishing press **`Previous`** and then **`Next`** to check the IP addresses and ensure that apply was successful, if they were successfully applied, press **`Skip`**.
9 ☐	**OA GUI:** Skip Directory Groups step	To skip `Directory Groups` step, click **`Next`**.
10 ☐	**OA GUI:** Skip Directory Settings step	To skip `Directory Settings` step, click **`Next`**.

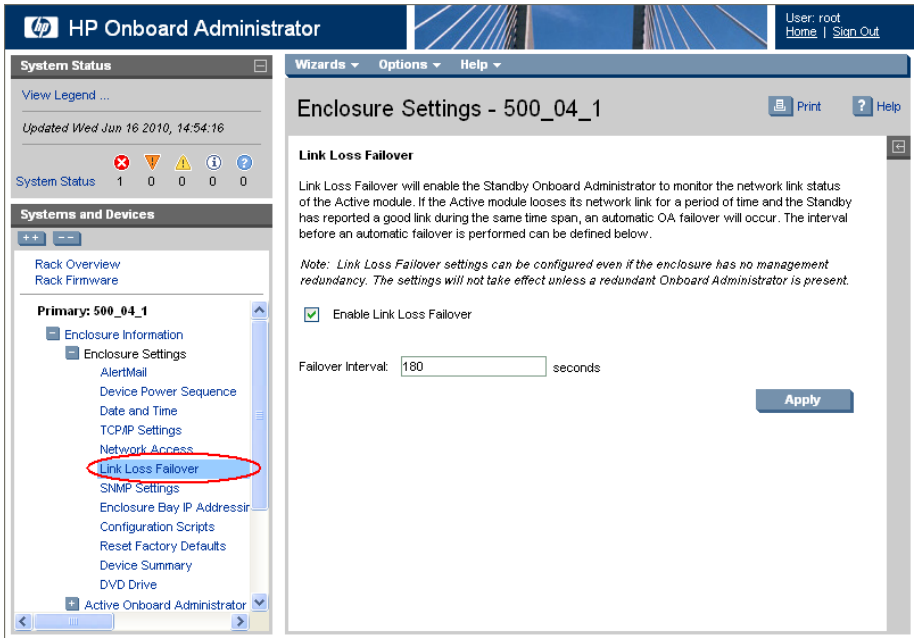
Procedure 9. Configure the OA (OA Configuration Wizard)

11 ☐	**OA GUI:** OA network settings	On the `Onboard Administrator Network Settings` tab, change the IP address and the network settings of the second OA.  Click on **`Next`**. **Note**: If you will change IP address of the OA though which you are signed on, you will be disconnected. Then you have to close browser and sign in again using the new IP address.

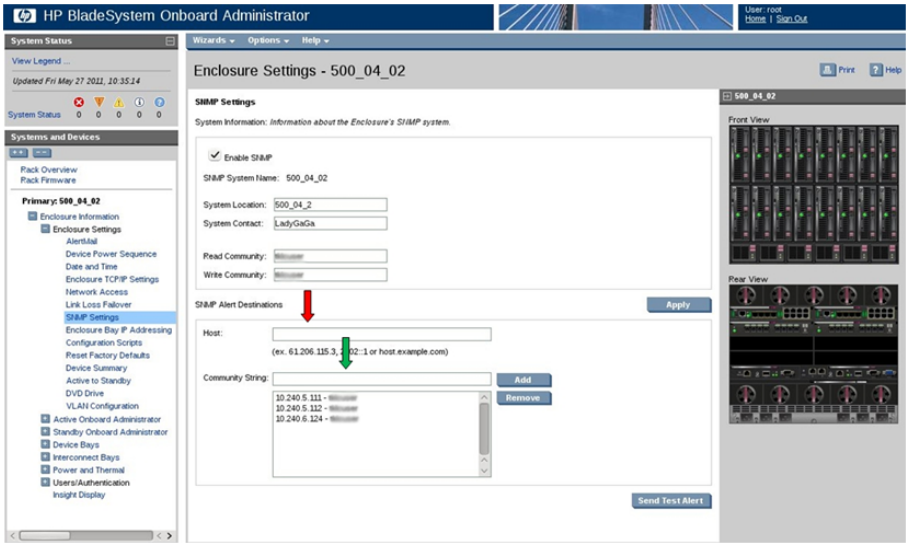
Procedure 9. Configure the OA (OA Configuration Wizard)

12 ☐	**OA GUI:** SNMP Settings	Mark **Enable SNMP**.  Fill in **System Location** that is equal to `Enclosure name` you have filled in Step 5. Do not set `Read Community` and `Write Community`. Click on **Next**.
13 ☐	**OA GUI:** Power Management	The Power Mode setting on the Power Management screen must be configured for power supply redundancy. The first available setting on the Power Management screen will be either "AC Redundant" or "Redundant" depending on whether the Enclosure is powered by AC or DC. In either case, select the **second** radio button, "Power Supply Redundant". For all other settings on the Power Management screen, leave the default settings unchanged. Click on **Next**.
14 ☐	**OA GUI:** Finish First Time Setup Wizard	Click on **Finish**.

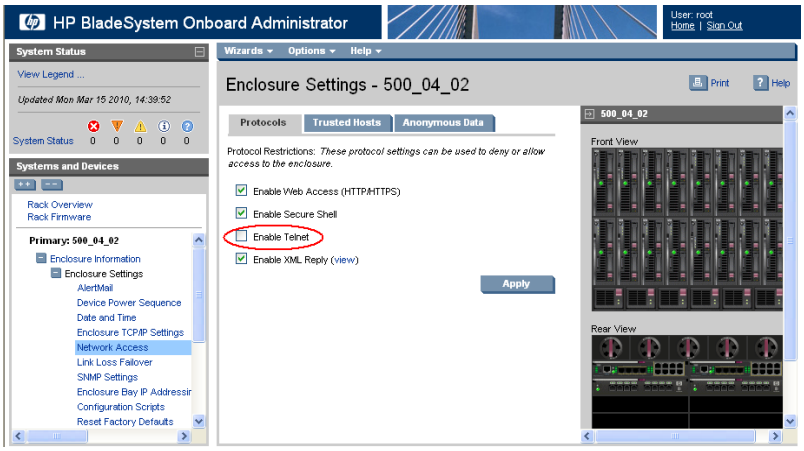
Procedure 9. Configure the OA (OA Configuration Wizard)

15 ☐	**OA GUI:** Set Link Loss Failover	Navigate to Enclosure Information -> Enclosure Settings -> Link Loss Failover  Check the Enable Link Loss Failover and specify Failover Interval to be 180 seconds. Click **Apply**.

Procedure 9. Configure the OA (OA Configuration Wizard)

16 ☐	**OA GUI:** Set SNMP	Navigate to Enclosure Information ➢ Enclosure Settings ➢ SNMP Settings. Type the host destination information into the 'Host box' (red arrow in the figure below) of the Customer's NMS Server as defined in the NAPD. Additionally, type the community string to the 'Community String' box (indicated by the green arrow in the following figure) and click **Add**. Additionally, enter the SO VIP (if 3 tier deployment) or NO VIP (if 2 tier deployment) into the 'Host box' and the community string to the 'Community String' and click **Add** again.  The SNMP trap destination has now been added to the configuration and should show up in the list of configured destinations. Click **Apply** to activate the configuration. A progress meter may appear, when it disappears, the configuration has been applied.

Procedure 10. OA Security Configuration

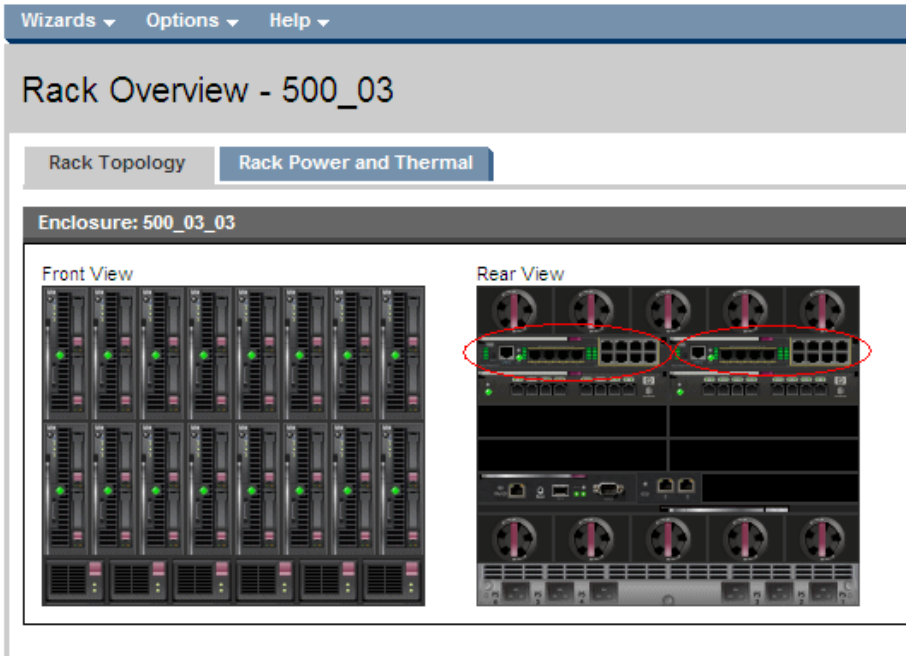
S T E P #	This procedure will disable telnet access to OA. ***Prerequisite:*** Configure the OA procedure *has been completed.* Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**OA GUI:** Login	Login to HP Onboard Administrator as Administrator.
2 ☐	**OA GUI:** Disable telnet	Navigate to **Enclosure Information** -> **Enclosure Settings** -> **Network Access**  Then uncheck the `Enable Telnet`  Click on **Apply**.

4.7 Enclosure Switches Firmware Update

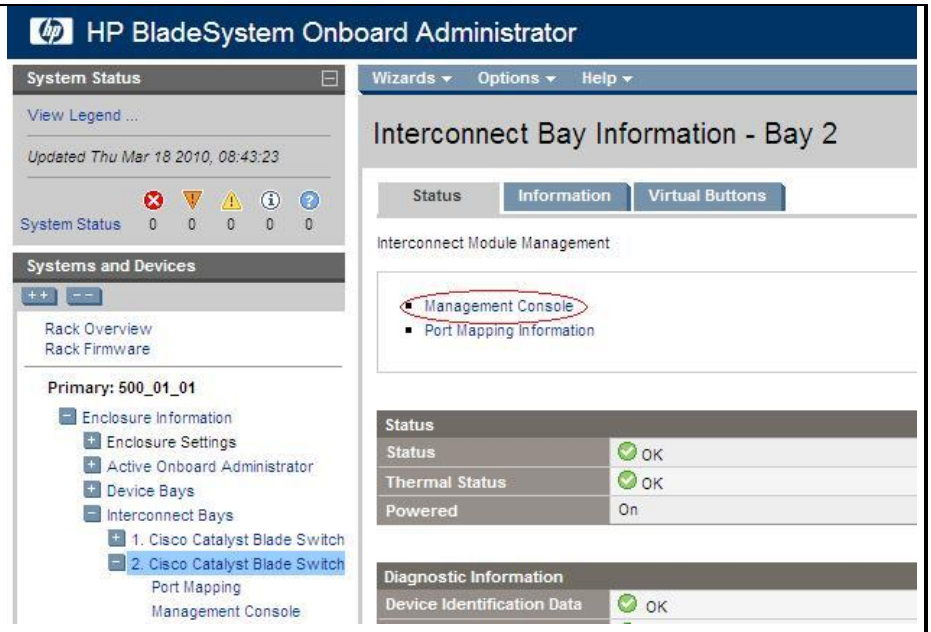
If the enclosure switches used are Cisco 3020, execute the procedure in section 4.7.1. If the switches used are HP 6120XG, execute the procedure in section 4.7.2.

4.7.1 Cisco 3020 Switch Update

Procedure 11. Update Cisco 3020 Switch Firmware

S T E P #		
	This procedure will describe the steps how to upgrade firmware for the 3020 switches. **Needed material:** - HP Misc. Firmware DVD - HP Solutions Firmware Upgrade Pack Release Notes [1] Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**OA GUI:** Run OA	Log into the active OA as Administrator. Navigate to Home page. You should see the Front View and Rear View of the enclosure. 
2 ☐	**OA GUI:** Run Catalyst Blade Switch 3020 Device Manager	**Note: Repeat the following steps for all 3020 switches in the enclosure.** Click on **`interconnect bay 1`** on the Rear View image of the middle pane. Alternatively, on the left pane, one could expand `Interconnect Bays` , then click **`1. Cisco Catalyst Blade Switch`**. Then click on **`Management Console`**.

Procedure 11. Update Cisco 3020 Switch Firmware

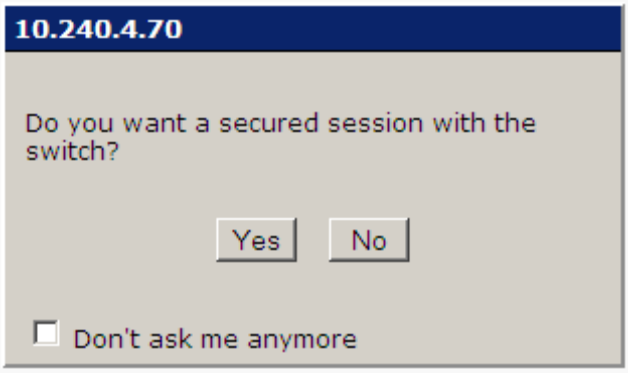


A new page will be opened. If you are asked for a username and password, leave the username blank and for password use “cisco”. Then click **OK**.

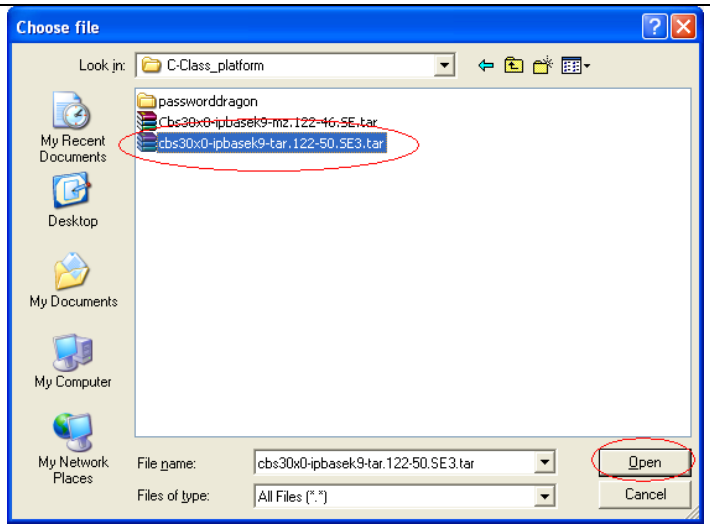
If you get an Express Setup page, click on **Refresh** to skip past the Express setup and proceed to the main switch screen.

If you are prompted with "Do you want a secured session with the switch?", click on **No**.

Procedure 11. Update Cisco 3020 Switch Firmware

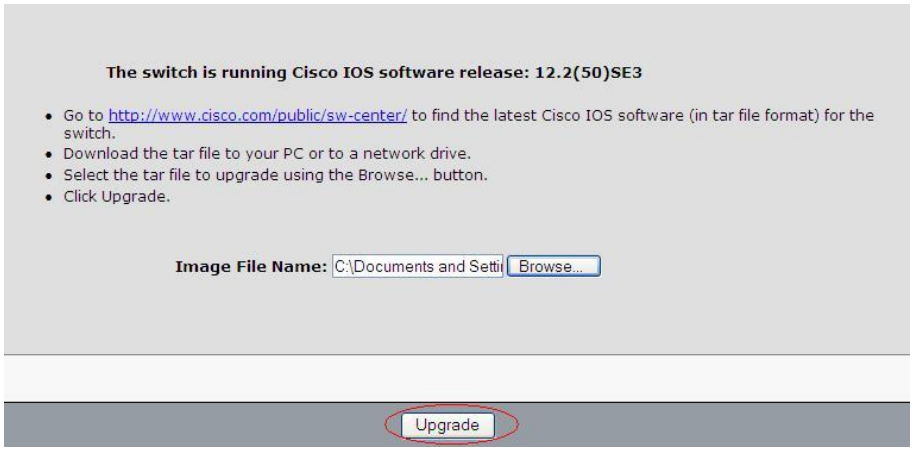
		 Then a new Catalyst Blade Switch 3020 Device Manager will be opened.
3 ☐	**OA GUI:** Upgrade switch IOS	Navigate to **Maintenance -> Software Upgrade**.  Check IOS software release (circled above). If the software release is at or above the expected level based on the *Firmware Upgrade Pack Release Notes [1]* then the current switch firmware does not need to be updated, Skip the rest of this procedure.
4 ☐	Copy switch firmware tar file	If you haven't done so, copy the Cisco 3020 firmware tar file onto your machine from the firmware upgrade disk.
5 ☐	**OA GUI:** Upgrade switch IOS	In the OA GUI, Navigate to **Maintenance -> Software Upgrade**.  click **Browse** and navigate to the tar image you copied to your PC in step 4.

Procedure 11. Update Cisco 3020 Switch Firmware

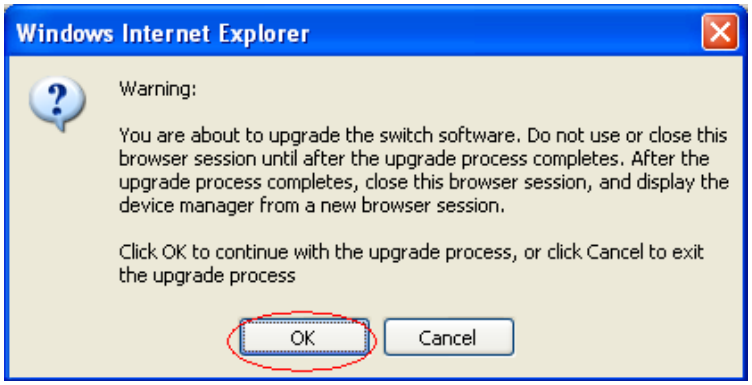


Select the tar file and click **Open**.

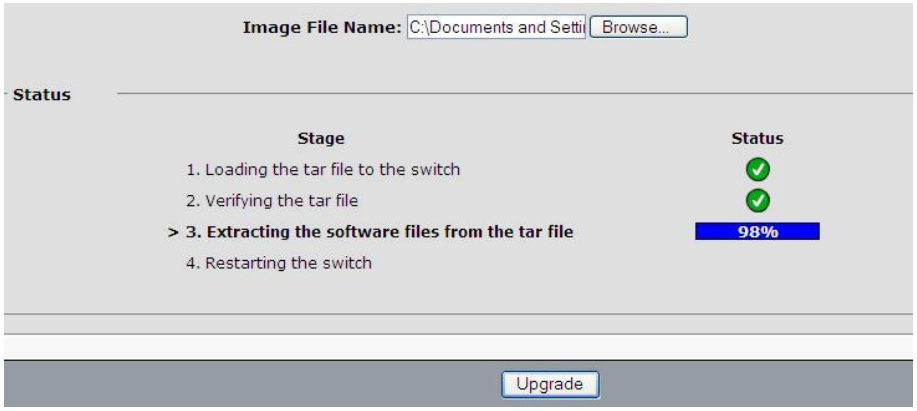
then click **Upgrade**.



Click **OK** to continue the upgrade.



Procedure 11. Update Cisco 3020 Switch Firmware

		The upgrade process will take approximately 10 minutes. In approximately 10 minutes, click the **Refresh** button to verify the new image has loaded successfully. 
6 ☐	Repeat for remaining switch	Go back to Step 2 and repeat for the remamining 3020 switches.
7 ☐	Remove the tar file	The tar file from step 1 may now be deleted from your computer.

4.7.2 HP 6120XG Switch Firmware Update

Procedure 12. Update HP 6120XG Switch Firmware

S T E P #	This procedure provides the steps neccesary to upgrade firmware for the 6120XG switches. Prerequisites: Configure initial OA IP and Configure the OA procedures must be completed. Needed material: - HP Misc. Firmware DVD - HP Solutions Firmware Upgrade Pack Release Notes [1] - WinSCP - SSH client (eg. PuTTY) Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact Tekelec Technical Services and ask for ASSISTANCE.

Procedure 12. Update HP 6120XG Switch Firmware

1 ☐	**Manaement Server:**	Using the OA GUI, check the Rack FW levels shown below to determine the current FW and if at the desired level skip the rest of the procedure
		
		Interconnect Firmware Information
		Bay | Device Model | Firmware Version
		1 | HP ProCurve 6120XG Blade Switch | Z.14.32.10
		2 | HP ProCurve 6120XG Blade Switch | Z.14.32.10
		5 | HP ProCurve 6120XG Blade Switch | Z.14.32.10
		6 | HP ProCurve 6120XG Blade Switch | Z.14.32.10
		7 | HP 1Gb Ethernet Pass-Thru Module for c-Class BladeSystem | Not Available
		8 | HP 1Gb Ethernet Pass-Thru Module for c-Class BladeSystem | Not Available
		
		Verify that the appropriate version of HP 6120XG firmware, as specified by the *HP Solutions Firmware Upgrade Pack Release Notes [1]* from the *Misc Firmware DVD*, exists under /var/TKLC/smac/image. If it doesn't exist, Insert the *Misc. Firmware CD* media into the CD drive of the management server and copy the IOS image called out by the release notes [1].
		
		`# mount /dev/sr0 /media/cdrom`
		
		Execute the following commands to copy the required files. Note that the **<PMAC Management_IP Address>** is the one used to deploy PM&C in procedure 4, step 3
		
		`# scp -p /media/cdrom/files/<6120_IOS_image_filename> root@<PMAC Management_IP Address>:/var/TKLC/smac/image`
		
		Unmount the media using the following command:
		
		`# umount /media/cdrom`
		
		Remove the *Misc. Firmware CD* media from the CD drive.

2 ☐	**6120XG Switch:** Login	Login to the switch as *manager* via ssh.(accepting switch's key if prompted)
		
		`login as: manager`
		
		Press any key to continue as prompted by the switch.
		
		`Switch#`
		
		Note that if logging with "manager" is unsuccessful, hold the "Clear" button on the 6120 switch for greater than 30 seconds to clear the password.

3 ☐	**6120XG Switch:** Enter global configuration.	Re-login to the switch via ssh as done in step 2 above. Next enter config mode by running the following: `Switch# config`

Procedure 12. Update HP 6120XG Switch Firmware

4 ☐	**6120XG Switch:**
	Find current firmware version and compart to release notes.
		`Switch(config)# show version`
		`Image stamp: /sw/code/build/vern(Z_14_zin_t4b)`
		`Jun 23 2010 16:48:29`
		`Z.14.12`
		`31`
		`Boot Image: Secondary`
		
		Record the firmware version (z.14.12 in this case) and the current Boot Image location being used (Secondary in this case). Compare the firmware version currently being used to the latest version specified in the *HP Solutions Firmware Upgrade Pack Release Notes.* Continue with this upgrade procedure if necessary.
		
		Whatever Boot Image is being used the opposite one will be upgrade. So in this case since the Secondary Boot Image is being used the Primary Boot image will be upgraded.

5 ☐	**6120XG Switch:**
	Record current firmware version of Boot Image to be upgraded.
		Record the current version of the Boot Image to be upgraded. This will be used to compare after upgrading to check for sucess of the upgrade. (Primary Image in this case)
		
		`Switch(config)# show flash`
		`Image Size(Bytes) Date Version`
		`----- ---------- -------- -------`
		`Primary Image : 7595562 02/17/10 Z.14.09`
		`Secondary Image : 7193633 06/23/10 Z.14.12`
		`Boot Rom Version: Z.14.09`
		`Default Boot : Secondary`

6 ☐	**6120XG Switch:**
	Make sure Secure Copy is enbled
		Enter the following command:
		
		`Switch(config)# show ip ssh`
		`SSH Enabled : Yes Secure Copy Enabled : Yes`
		`TCP Port Number : 22 Timeout (sec) : 120`
		`Host Key Type : RSA Host Key Size : 2048`
		
		`Ciphers :`
		`MACs :`
		
		`Ses Type | Source IP Port`
		`--- -------- + ----------- -----`
		`1 console |`
		`. . . .`
		
		Look at the output of **`show ip ssh`**. If ***`Secure Copy Enabled = Yes`*** then continue to the next step. If ***`Secure Copy Enabled = No`*** then perform the command below.
		
		`Switch(config)# ip ssh filetransfer`
		`Tftp and auto-tftp have been disabled.`
		`Switch(config)#`
		
		Enter **`show ip ssh`** again to make sure Secure Copy has been enabled.

Procedure 12. Update HP 6120XG Switch Firmware

7 ☐	**6120XG Switch:**
	Open the event log.
		Go into the switch's menu interface and type "y" to save the configuration.
		`Switch(config)# menu`
		`Do you want to save current configuration [y/n/^C]? y`
		`Select:`
		`4. Event Log`
		`Then Select:`
		`End`
		Keep this terminal window open.

8 ☐	**Management Server:** Copy firmeware file to switch	Execute the following command to copy the firmware file onto the switch: Note: If updating the secondary image instead of primary, replace primary with secondary in the command below. # `scp /var/TKLC/smac/image/<6120_IOS_image_filename manager@<6120XG IP>:/os/primary`
9 ☐	**6120XG Switch:** Go back to the Event Log on the SSH session with the switch.	Go Back to the switch ssh window where you have the ***Event Log*** open. If the connection has timed out redo Steps 2,3, and 6. Watch for the following log event (it can take a few minutes) : `update: Primary Image updated` In this example the Primary Image is being updated if you were updating the Secondary Image it would say "Secondary" instead of "Primary".

10 ☐	**6120XG Switch:**
	Get Back to the Command Line Interface (CLI).
		Now that you have seen the "updated" message select:
		`Back`
		Then select:
		`5. Command Line (CLI)`
		`Switch(config)#`

11 ☐	**6120XG Switch:**
	Check the firmware version.
		Run the `show flash` command to make sure the Image you were updating has the correct firmware version. (in this example ***`Primary Image`*** has changed to ***`Z.14.22`***)
		`Switch(config)# show flash`
		`Image Size(Bytes) Date Version`
		`----- ---------- -------- -------`
		`Primary Image : 7732899 10/21/10 Z.14.22`
		`Secondary Image : 7193633 06/23/10 Z.14.12`
		`Boot Rom Version: Z.14.09`
		`Default Boot : Secondary`

Procedure 12. Update HP 6120XG Switch Firmware

12
☐
	6120XG Switch:
	Reboot into the new firmware.
		Now you will reboot the switch into the new Boot Image. (***primary*** in this example).
		If you have updated the ***Secondary Image*** replace "primary" with "secondary" in the command below.
		`Switch(config)# boot system flash primary`
		`Device will be rebooted, do you want to continue [y/n]? y`

13
☐
	6120XG Switch:
	Log back in.
		Once the switch has rebooted, login back into the switch as *manager* via ssh.
		`login as: manager`
		Press any key to continue as prompted by the switch.
		`Switch#`

14 ☐	**6120XG Switch:** Re-enter global configuration.	`Switch# config`

15
☐
	6120XG Switch:
	Make sure the switch has booted properly into the new firmware image.
		Run the `show version`. Make sure the new firmware version is displayed.
		`Switch(config)# show version`
		`Image stamp: /sw/code/build/vern(Z_14_zin_t4b)`
		`Oct 21 2010 16:48:29`
		`Z.14.22`
		`31`
		`Boot Image: Primary`

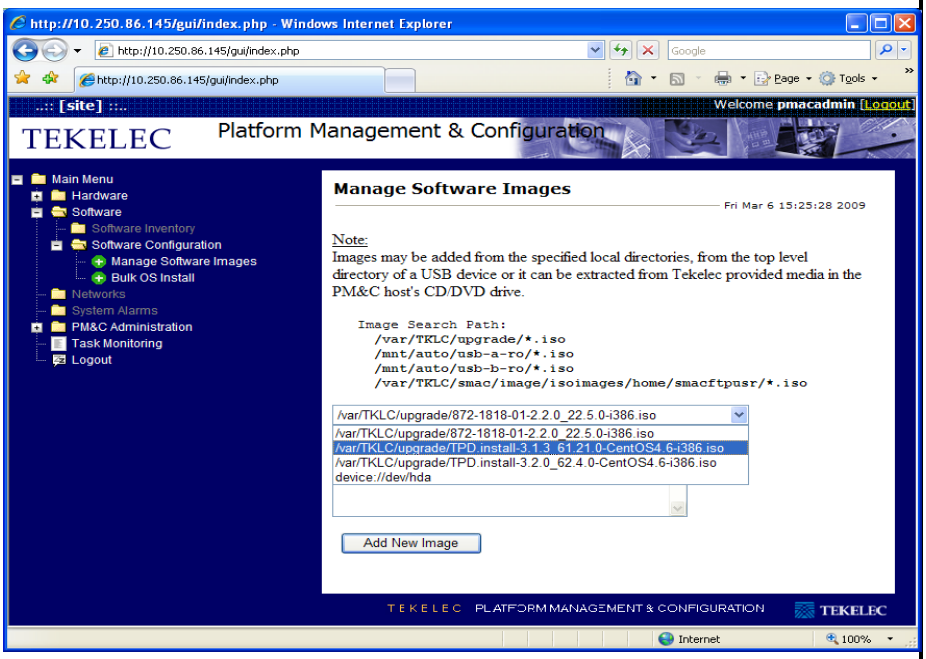
16
☐
	6120XG Switch:
	Verify the "Default Boot" has changed.
		Run the `show flash` command, checking to make sure the image you upgraded has been set as the "Default Boot". (`Primary` in this example)
		`Switch(config)# show flash`
		`Image Size(Bytes) Date Version`
		`----- ---------- -------- -------`
		`Primary Image : 7732899 10/21/10 Z.14.22`
		`Secondary Image : 7193633 06/23/10 Z.14.12`
		`Boot Rom Version: Z.14.09`
		`Default Boot : Primary`

4.8 OA Firmware Update

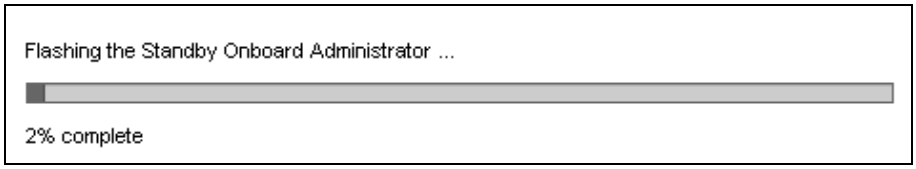
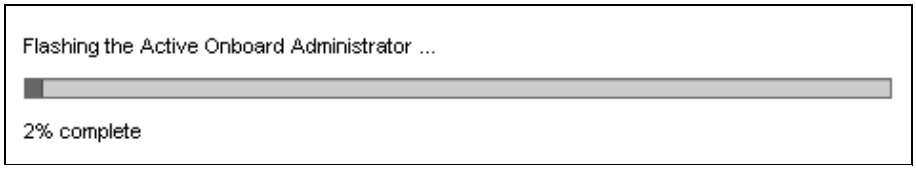
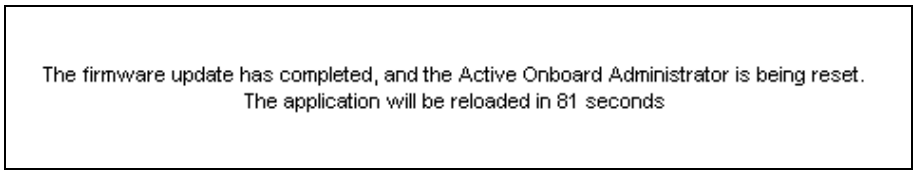
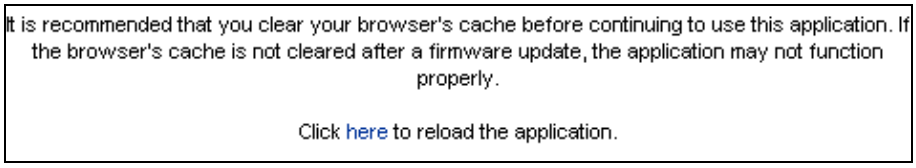
Procedure 13. Upgrade OA Firmware

S T E P #		
	This procedure will upgrade the firmware on the OA. **Needed material:** - HP Misc. Firmware DVD - HP Solutions Firmware Upgrade Pack Release Notes [1]. **Note:** This procedure should be used to upgrade firmware or to ensure both OA's have same firmware in a system with redundant OA. When the firmware update is initiated, the standby OA is automatically flashed first. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**OA GUI:** Login	Login to HP OA as Administrator. Original password is on paper card attached to each OA.
2 ☐	**OA GUI:** Determine if firmware upgrade is required	In the left navigation area, click on **`Active Onboard Administrator`** Examine the `Firmware Version` shown in the `Firmware Information table`. Verify the version meets the minimum requirement specified by Release Notes [1] and that the firmware versions match for both OA's. If it is so the firmware does not need to be upgraded. Skip the rest of this procedure.
3 ☐	Make the image available to PM&C	Insert the OA firmware disc as specified in HP Solutions firmware upgrade pack [1] into the removable media drive of the management server.
4 ☐	**PM&C GUI:** Login	Open a new web browser window and enter: **`http://<management_network_ip>/gui`** Login as pmacadmin user.
5 ☐	**PM&C GUI:** Navigate to Manage Software Images	If the image is on a CD or USB device, In the PM&C GUI, nevigate to **Main Menu ➤ VM Managmenet.**. In the "**VM Entities**" list, select the PM&C guest. On the resulting "**View VM Guest**" page, 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 will appear in the "**Attached Media**" list.

Procedure 13. Upgrade OA Firmware

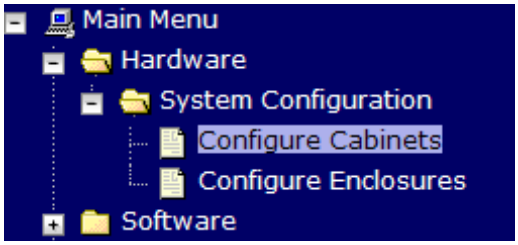
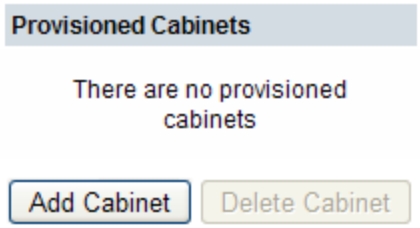
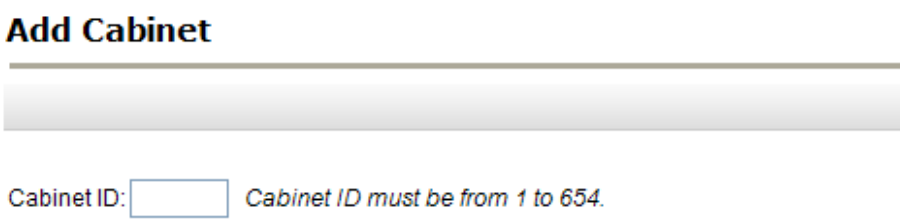
6 ☐	**PM&C GUI:** Add image	Press **Add Image** button. Use the dropdown to select the image you just transferred. **Note:** optical media device appears as `device://dev/scd0` Add appropriate image description and press **Add New Image** button.  You may check the progress using the `Task Monitoring` link. Observe the green bar indicating success. Once the green bar is displayed, remove the Misc. Firmware CD from the optical drive of the management server.
7 ☐	**OA GUI:** Upgrade OA firmware	Switch back to the OA, click on **Firmware Update** in the left navigation area. Enter the appropriate URL in the bottom text box labeled "Image URL". The syntax is: `http://<PM&C_ Management _Network _IP>/TPD/<HPFW_mount_point>/files/<OA_firmware_version>.bin` For example: http://10.240.4.198/TPD/HPFW--2.1.1-10.1.0--872-2161-101--i386/files/hpoa300.bin Click **Apply** Click **OK** **Note:** The upgrade may take few minutes in a system with one OA and about 25 minutes on a system with redundant OA present.

Procedure 13. Upgrade OA Firmware

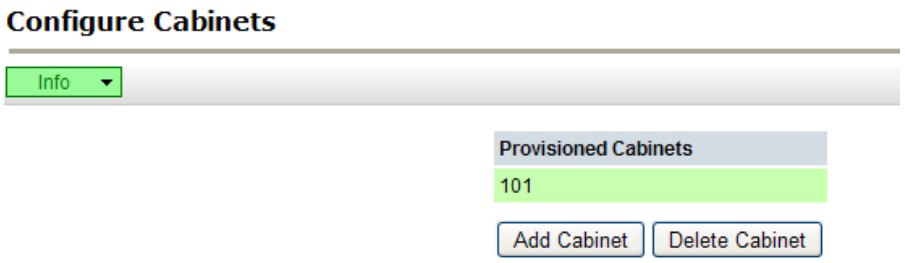
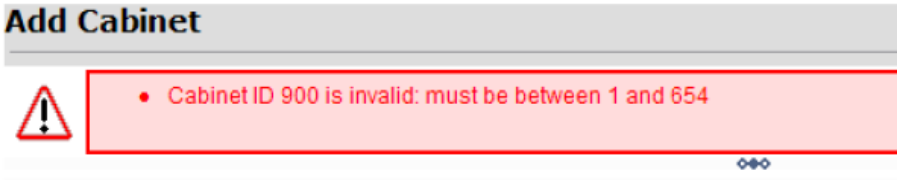
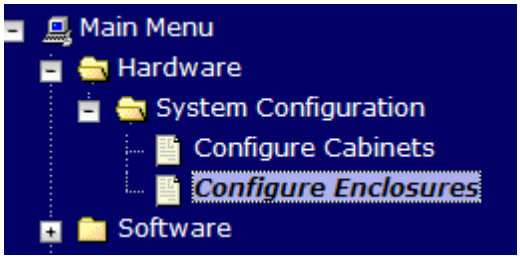
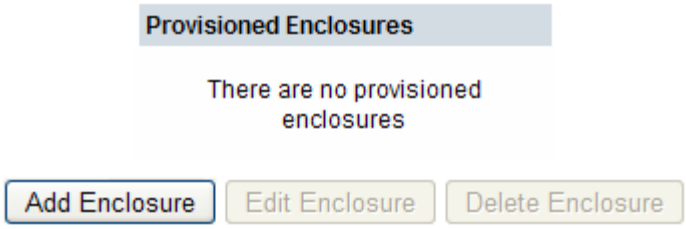
8 ☐	**OA GUI:** Observe OA firmware upgrade progress	You shoould observe the following updates during the upgrade.    
9 ☐	**OA GUI:** Reload the HP OA application	The upgrade is complete when the following is displayed:  Clear your browser‘s cache and click to reload the application . The login page should appear momentarily.
10 ☐	**OA GUI:** Verify the firmware upgrade	Login to the OA again. It may take few minutes before the OA is fully functinal and accepts the credentials. In the left navigation area, navigate to Enclosure Information -> Active Onboard Administrator -> Firmware Update Examine the Firmware Version shown in the Firmware Information table. Verify the firmware version information is correct.

4.9 Enclosure and Blades setup

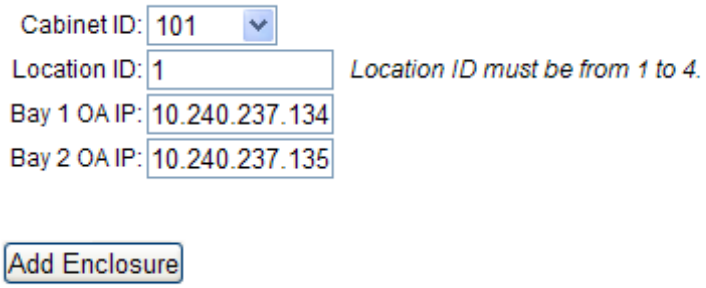
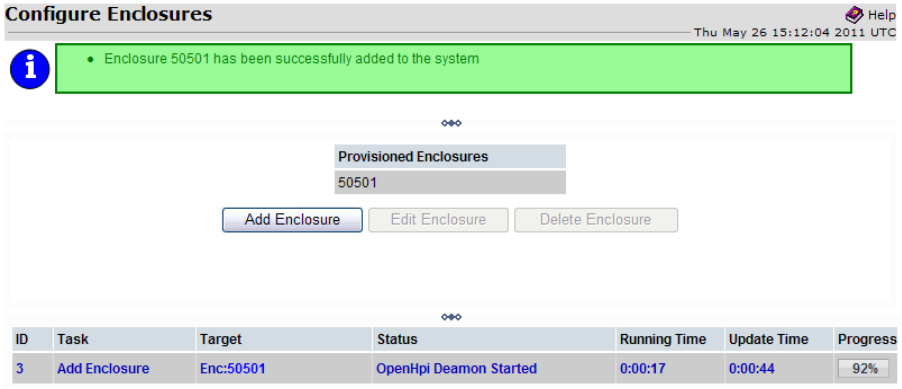
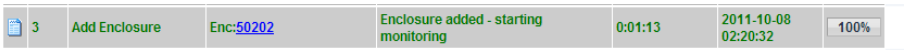
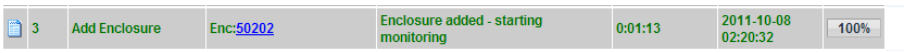
Procedure 14. Add Cabinet and enclosure to the PM&C System

S T E P #	This procedure provides instructions to add a cabinet and an enclosure to the PM&C system inventory. ***Prerequisite: Procedure 7. Configure the PM&C Server*** *has been completed.* **Note:** The installer must be knowledgeable of the network. If you make mistake, hit cancel and try again. The finish step may take longer time because it reconfigures the network and attempts to connect may fail. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**PM&C GUI:** Login	Open web browser and enter: **`http://<management_network_ip>/gui`** Login as pmacadmin user.
2 ☐	**PM&C GUI:** Configure Cabinets	Navigate to **`Main Menu`** -> **`Hardware`** -> **`System Configuration`** -> **`Configure Cabinets`**. 
3 ☐	**PM&C GUI:** Add Cabinet	On the `Configure Cabinets` panel click on **`Add Cabinet...`** 
4 ☐	**PM&C GUI:** Enter Cabinet ID	Enter `CabinetID` and press **`Add Cabinet`**. 

Procedure 14. Add Cabinet and enclosure to the PM&C System

5 ☐	**PM&C GUI:** Check errors	If no error is reported to the user you will see the following:  Or you will see an error message: 
6 ☐	**PM&C GUI:** Go to Configure HPC Enclosures	Navigate to **Main Menu -> Hardware -> System Configuration -> Configure Enclosures**. 
7 ☐	**PM&C GUI:** Go to Add Enclosure	On the `Configure Enclosures` panel click on **Add Enclosure...** 

Procedure 14. Add Cabinet and enclosure to the PM&C System

8 ☐	**PM&C GUI:** Add Enclosure	In the Add Enclosure panel enter `Cabinet ID`, `Location ID` and `Bay 1 OA IP` and `Bay 2 OA IP`. Then click on **`Add Enclosure`**.  **Notes:** Location ID is used to uniquely identify the enclosure within the cabinet. It can have a value of 1, 2, 3 or 4. The cabinet id and location id will be combined to create a globally unique id for the enclosure (for example, an enclosure in cabinet 502 at location 1, will have an enclosure id of 50201).
9 ☐	**PM&C GUI:** Monitor the Enclosure discovery status	When the task is complete, the text will change to green and the Progress bar will indicate "100%". 
10 ☐	**PM&C GUI:** Background Task monitoring	This page allows the user to monitor status updates:  **NOTE:** DO NOT click the ⊠ button as this will delete the selected task from the Background Task Monitoring status screen.
11 ☐	**PM&C GUI:** Wait until the Add Enclosure task finishes	The color of the progress bar will change to green when complete:  If the `Add Enclosure` task fails the `Status` will display information concerning the failed step and the color of the `Progress` bar will change to red.

Procedure 15. Configure iLO password for Blades'Administrator account

S T E P #	This procedure will set iLO passwords for Administrator and root accounts on all blades. ***Prerequisite:*** Procedure 8. Configure initial OA IP *has been completed.* Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**Management server:** Edit xml file	Edit the following file by running: # **chmod 664 /usr/TKLC/smac/etc/change_ilo_admin_passwd.xml** # **vi /usr/TKLC/smac/etc/change_ilo_admin_passwd.xml** Update the **<root password>**, **<iLo root password>** and **<iLo Administrator password>** fields. Now copy the xml file to **/usr/TKLC/smac/html/public-configs/** by running the following command: # **cp /usr/TKLC/smac/etc/change_ilo_admin_passwd.xml /usr/TKLC/smac/html/public-configs/**
2 ☐	**OA shell:** Run hponcfg	Connect to the active OA via ssh as root. Run the following command: **> hponcfg all http://<management_server_ip>/public-configs/change_ilo_admin_passwd.xml**
3 ☐	**OA shell:** Check for error	After the command is done executing, Scroll up and check for any errors that might've occured
4 ☐	**OA shell:** Logout	After the command is done executing, Logout from the OA **> exit**

4.10 Configure Enclosure Switches

If the enclosure switches used are Cisco 3020, execute the procedure in section 4.10.1. If the switches used are HP 6120XG, execute the procedure in section 4.10.2.

4.10.1 Configure Cisco 3020 Enclosure Switches

Procedure 16. Configure Cisco 3020 Switch Pair(s) using NetConfig

S T E P #		
	This procedure will configure up to 3 Cisco 3020 switch pairs with an appropriate IOS and configuration specified by Platform Engineering and Application requirements. **Needed material:** - Switch Configuration files in an application ISO on an application CD Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**Virtual PM&C:** Prepare for switch configuration	login to the management server, then run: # **ping <switch_mgmtVLAN_VIP>** If aggregation switches are present # **ping <switch1A_mgmtVLAN_address>** # **ping <switch1B_mgmtVLAN_address>** Repeat for other expected application VLANs. If all IP addresses respond positively, then the aggregation switches have been configured. For each 3020 switch, verify network reachability # **ping <enclosure_switch_IP>**

2
☐
	Virtual PM&C:
	Check TFTP Service Configuration
		Check the TFTP configuration file to verify it is configured properly. If the /etc/xinetd.d/tftp file matches the output below, skip to step 4. Otherwise move on to step 3.
		
		# **cat /etc/xinetd.d/tftp**
		
		service tftp
		{
		socket_type = dgram
		protocol = udp
		wait = yes
		user = root
		server = /usr/sbin/in.tftpd
		server_args = -s **/var/TKLC/smac/image**
		disable = no
		per_source = 11
		cps = 100 2
		flags = IPv4
		}

Procedure 16. Configure Cisco 3020 Switch Pair(s) using NetConfig

3 ☐	**Virtual PM&C:** Configure tftp service	Ensure that the tftp service is not running. A zero is expected.
		
		`# tpdProvd --client --noxml --ns=Xinetd getXinetdService service tftp`
		
		`Login on Remote: platcfg`
		`Password of platcfg:`
		`0`
		`#`
		
		If 1 is returned, need to stop it first by executing the following command.
		
		`# tpdProvd --client --noxml --ns=Xinetd stopXinetdService service tftp force yes`
		
		`Login on Remote: platcfg`
		`Password of platcfg:`
		`0`
		`#`
		
		This should return a 0.
		Edit the /etc/xinetd.d/tftp file for the values in bold so that tftp will work appropriately:
		
		`# vi /etc/xinetd.d/tftp`
		
		`service tftp`
		`{`
		`socket_type = dgram`
		`protocol = udp`
		`wait = yes`
		`user = root`
		`server = /usr/sbin/in.tftpd`
		`server_args = -s /var/TKLC/smac/image`
		`disable = no`
		`per_source = 11`
		`cps = 100 2`
		`flags = IPv4`
		`}`

4 ☐	**Virtual PM&C:** Modify PM&C Feature to allow TFTP	Enable the DEVICE.NETWORK.NETBOOT feature with the management role to allow tftp traffic by running the following commands:
		
		`# pmacadm editFeature --featureName=DEVICE.NETWORK.NETBOOT --enable=1 --role=management`
		
		`# pmacadm resetFeatures`

Procedure 16. Configure Cisco 3020 Switch Pair(s) using NetConfig

5 ☐	**Virtual PM&C:** Verify netConfig Services	Verify that the netConfig tftp_service has been configured. If the service is configured the output will look similar to below:
		
		`# netConfig --repo showService name=tftp_service`
		
		and check the output, which will be similar to the one shown below
		
		`Services:`
		`  Service Name: tftp_service`
		`  Type: tftp`
		`  Host: 10.240.8.4`
		`  Options:`
		`  dir: /var/TKLC/smac/image`
		
		`[root@pmac5000101 ~]#`
		
		If tftp_service is already configured, skip to step 7. Otherwise, continue on to step 6.

6 ☐	**Virtual PM&C:** Setup netConfig repository with necessary tftp information	Use netConfig to create a repository entry that will use the tftp service. This command will give the user several prompts. The prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as an answer must be entered EXACTLY as they are shown here.
		
		`# netConfig --repo addService name=tftp_service`
		`Service type? (tftp, ssh, conserver, oa) tftp`
		`Service host? <pmac_mgmtVLAN_ip_address>`
		`Enter an option name (q to cancel): dir`
		`Enter a value for user: /var/TKLC/smac/image`
		`Enter an option name(q to cancel): q`
		`Add service for tftp_service successful`
		
		To check that you entered the information correctly, use the following command:
		
		`# netConfig --repo showService name=tftp_service`
		
		and check the output, which will be similar to the one shown below:
		
		`Services:`
		`  Service Name: tftp_service`
		`  Type: tftpr`
		`  Host: 10.240.8.4`
		`  Options:`
		`  dir: /var/TKLC/smac/image`
		`[root@pmac5000101 ~]#`

Procedure 16. Configure Cisco 3020 Switch Pair(s) using NetConfig

7 ☐	**Virtual PM&C:** Setup netConfig repository with necessary ssh information	check that the ssh_service is present by running the following command:
		
		`# netConfig --repo showService name=ssh_service`
		
		and check the output, which will be similar to the one shown below:
		
		`[root@pmac5000101 ~]# netConfig --repo showServices --name=ssh_service`
		
		`Services:`
		`Service Name: ssh_service`
		`Type: ssh`
		`Host: 10.240.8.4`
		`Options:`
		`password: D8396824B3B2B9EE`
		`user: root`
		`[root@pmac5000101 ~]#`
		
		If the output returns that the service isn't present. Run the following command to add it. Note that prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as answer must be entered EXACTLY as they are shown here.
		Note that <switch_backup_user_password> is not the same as the switch password (for c-Class it is the password of the PMAC).
		
		`# netConfig --repo addService name=ssh_service`
		`Service type? (tftp, ssh, conserver, oa) ssh`
		`Service host? <pmac_mgmtVLAN_ip_address>`
		`Enter an option name (q to cancel): user`
		`Enter a value for user: root`
		`Enter an option name(q to cancel): password`
		`Enter a value for password: <switch_backup_user_password>`
		`Enter an option name(q to cancel): q`
		`Add service for console_service successful`
		
		Run the following command again to check that the service was added sucessfully
		
		`# netConfig --repo showService name=ssh_service`

Procedure 16. Configure Cisco 3020 Switch Pair(s) using NetConfig

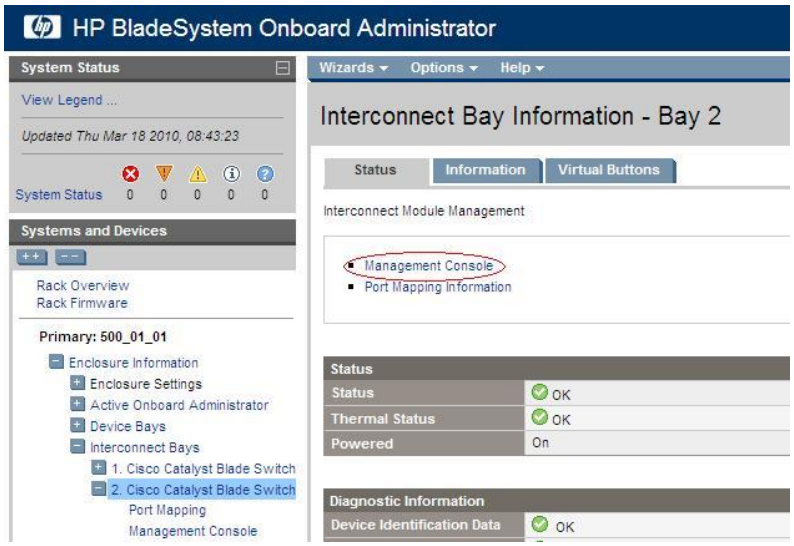
8 ☐	**Virtual PM&C:** Setup NetConfig repository with switch information	Use netConfig to create a repository entry for each 3020. This command will give the user several prompts. The prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as an answer must be entered EXACTLY as they are shown here. If you do not know, stop now and contact Customer Care Center.
		
		NOTE: Switch Name must not exceed 20 characters.
		
		`# netConfig --repo addDevice name=C3020_IOBAY1 --reuseCredentials`
		
		`Device Vendor? Cisco`
		`Device Model? 3020`
		
		`Should the init network adapter be added (y/n)? y`
		`Adding netBootInit protocol for C3020_IOBAY1 using network...`
		
		`What is the address used for network device access? <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 C3020_IOBAY1 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 C3020_IOBAY1 using network...`
		`Network device access already set: 10.240.8.7`
		`Device named C3020_IOBAY1 successfully added."`
		
		To check that you entered the information correctly, use the following command
		
		`# netConfig --repo listDevices`
		
		and check the output, which will be similar to the one shown below
		
		`Device: C3020_IOBAY1`
		`  Vendor: Cisco`
		`  Model: 3020`
		`  Access: Network: 10.240.8.7`
		`  Init Protocol Configured`
		`  Live Protocol Configured`
		`[root@pmac5000101 ~]#`
		
		Repeat for each 3020, using appropriate values for those 3020s.

Procedure 16. Configure Cisco 3020 Switch Pair(s) using NetConfig

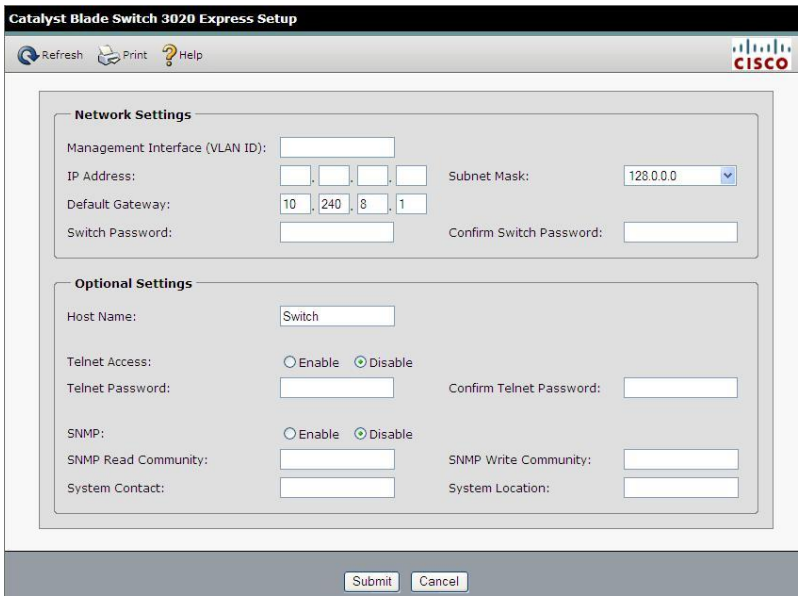
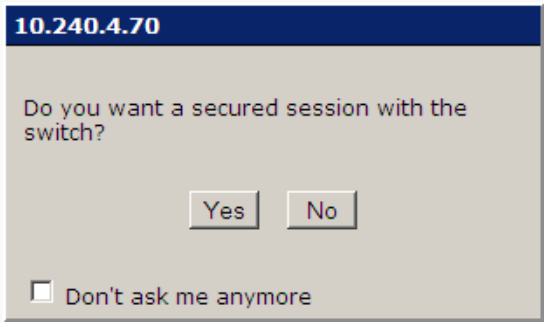
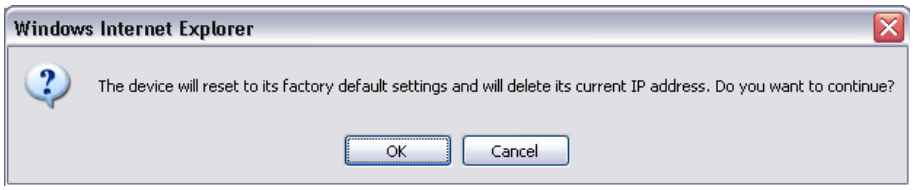
9 ☐	**Virtual PM&C:** Prepare the system for tftp	Execute the following command to turn on tftp:
		`# tpdProvd --client --noxml --ns=Xinetd startXinetdService service tftp`
		`Login on Remote: platcfg`
		`Password of platcfg: <platcfg_password>`
		
		Ensure the firewall on the virtual pmac allows for tftp access.
		
		`# service iptables status | grep 69`
		
		`1 ACCEPT udp -- 10.240.8.0/26 0.0.0.0/0 udp dpt:69`
		`#`
		
		If the output is not similiar to the one shown above, with site specific network information in it, then issue the following commands:
		
		`# iptables -I INPUT -s <management_network_subnet_id>/<netmask> -p udp --dport 69 -j ACCEPT`
		
		`# service iptables save`
		
		Otherwise, continue to the next step.

10 ☐	**Virtual PM&C:** Modify 3020_configure.xml file for information needed to configure the switch	Update the 3020_init.xml and 3020_configure.xml files for the values noted in the next sentence. Values to be modified by the user will be notated in this step by a preceding dollar sign. So a value that has **$<some_variable_name>** will need to be modified, removing the dollar sign and the less than, greater than sign. Optionally, these files can be updated ahead of time vis the NAPD.
		
		`# vi /usr/TKLC/smac/etc/3020_init.xml`
		
		`# vi /usr/TKLC/smac/etc/3020_configure.xml`

Procedure 16. Configure Cisco 3020 Switch Pair(s) using NetConfig

11 ☐	**Virtual PM&C/OA GUI:** Reset Switch to factory defaults	If the 3020 switch has been previously configured, it needs to be reset to manufacturer default to enable GUI access using the following command, otherwise skip to the next step. # **netConfig --device=<switchname> setFactoryDefault** Otherwise continue. Log onto the OA GUI and click on **interconnect bay 1** on the Rear View image of the middle pane. Alternatively, on the left pane, one could expand Interconnect Bays, then click **1. Cisco Catalyst Blade Switch**. Then click on **Management Console** as shown below.  A new page will be opened. If you are asked for a username and password, leave the username blank and use the appropriate password provided by the application documentation. Then click **OK**. 

Procedure 16. Configure Cisco 3020 Switch Pair(s) using NetConfig

		If you are prompted with the "Express Setup" screen, click Refresh.  If you are prompted with "Do you want a secured session with the switch?", click on **No**.  Then a new Catalyst Blade Switch 3020 Device Manager will be opened.
12 ☐	**OA GUI:** Restore switch to factory defaults	Navigate to **Configure > Restart/Reset**: Click the circle that says "Reset the switch to factory defaults, and then restart the switch". Then click the "**Submit**" button. A pop-up window will appear that looks like this:  Click OK and the switch will be reset to factory defaults and reloaded. **Continue to the next step, do not wait for the switch to finish rebooting.**

Procedure 16. Configure Cisco 3020 Switch Pair(s) using NetConfig

13 ☐	**Virtual PM&C:** Initialize the Switch	Note: This command must be entered at most 5 minutes after step 8 is completed. If it is not, repeat step 12.
		Execute the following commands:
		`# netConfig --file=/usr/TKLC/smac/etc/3020_init.xml`
		`Processing file: /usr/TKLC/smac/etc/3020_init.xml`
		Note: This step takes about 4-5 minutes to complete, it is imperative that you wait until returned to the command prompt. **DO NOT PROCEED UNLESS RETURNED TO THE COMMAND PROMPT**
		Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Customer Care Center.
		A successful completion of netConfig will return the user to the prompt.
		Go back to Step 9 and repeat steps 11 through 13 for the remainging 3020 switches.

14 ☐	**Virtual PM&C:** Configure the switches	Configure both switches by issuing the following command.
		`# netConfig --file=/usr/TKLC/smac/etc/3020_configure.xml`
		`Processing file: /usr/TKLC/smac/etc/3020_configure.xml`
		Note: This step takes about 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 Customer Care Center.
		A successful completion of netConfig will return the user to the prompt.

15 ☐	**Virtual PM&C:** Verify switch Configuration	To verify the configuration was completed successfully, ssh to each switch and attempt to log in. If log in is successful, execute the following: `Switch# show run` Inspect the output of "show run", and ensure that it is configured as per site requirements.

16 ☐	**Virtual PM&C:** Turn off tftp	Execute the commands that disable tftp transfer.
		`# tpdProvd --client --noxml --ns=Xinetd stopXinetdService service tftp`
		`Login on Remote: platcfg`
		`Password of platcfg: <platcfg_password>`

Procedure 16. Configure Cisco 3020 Switch Pair(s) using NetConfig

17 ☐	**Management server: Backup Switch Configuration**	Ensure the directory where the backups will be stored exists using the following command: # **ls /usr/TKLC/smac/etc/switch/backup** If an error is returned saying "No such file or directory", then create the directory using the following command # **mkdir /usr/TKLC/smac/etc/switch/backup** Change the currect path to the newly created directory using the following command # **cd /usr/TKLC/smac/etc/switch/backup** Execute the backup command to backup switch 1A # **netConfig device--device=<switch_name> backupConfigurationservice=ssh_service filename=<switch_name>-backup** Repeat the command above for the remaining switches. Verify switch configuration was backed up by cat <switch_name>-backup and inspect its contents to ensure it reflects the latest knwon good switch configurations.

4.10.2 Configure HP6120XG Enclosure Switches

Procedure 17. Configure HP 6120XG Switch Pair(s) using NetConfig

S T E P #	This procedure will configure up to 3 HP 6120XGswitch pairs with an appropriate IOS and configuration specified by Platform Engineering and Application requirements. **Needed material:** - Application 6120 configuration file in an application ISO on an application CD Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.

Procedure 17. Configure HP 6120XG Switch Pair(s) using NetConfig

1 ☐	**Management server:** Prepare for switch configuration	If the aggregation switches are provided by Tekelec, login to the management server, then run:
		# **ping <switch1A_mgmtVLAN_address>**
		# **ping <switch1B_mgmtVLAN_address>**
		# **ping <switch_mgmtVLAN_VIP>**
		
		If the aggregation switches are provided by the customer, login to the management server, then run:
		# **ping <customer_switch1A_mgmtVLAN_address>**
		# **ping <customer_switch1B_mgmtVLAN_address>**
		# **ping <customer_switch_mgmtVLAN_VIP>**
		
		check that the ssh_service is present by running the following command:
		
		# **netConfig --repo showService name=ssh_service**
		
		and check the output, which will be similar to the one shown below:
		
		`[root@pmac5000101 ~]# netConfig --repo showServices --name=ssh_service`
		
		`Services:`
		`Service Name: ssh_service`
		`Type: ssh`
		`Host: 10.240.8.4`
		`Options:`
		`password: D8396824B3B2B9EE`
		`user: root`
		`[root@pmac5000101 ~]#`
		
		If the output returns that the service isn't present. Run the following command to add it. Note that prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as answer must be entered EXACTLY as they are shown here.
		Note that the <switch_backup_user_password> below is not the same as the switch password (for c-Class it is the password of the PMAC).
		
		# **netConfig --repo addService name=ssh_service**
		`Service type? (tftp, ssh, conserver, oa) ssh`
		Service host? <management_server_mgmtVLAN_ip_address>
		Enter an option name (q to cancel): user
		Enter a value for user: root
		Enter an option name(q to cancel): password
		Enter a value for password: < switch_backup_user_password>
		Enter an option name(q to cancel): q
		Add service for console_service successful
		
		Run the following command again to check that the service was added sucessfully
		
		# **netConfig --repo showService name=ssh_service**

Procedure 17. Configure HP 6120XG Switch Pair(s) using NetConfig

2 ☐	**Management server:** Reset the switch to factory defaults	Log in to the switch using SSH
		
		`# ssh manager@<enclosure_switch_IP>`
		
		`Switch# config`
		
		`Switch(config)# no password all`
		
		`Password protection for all will be deleted, continue [y/n]? y`
		
		`Switch(config)# no include-credentials`
		
		`Switch(config)# end`
		
		`Switch# erase startup-config`
		
		`Configuration will be deleted and device rebooted, continue [y/n]? y`
		
		The switch will automatically reboot, reboot takes about 120-180 seconds.
		Note: Upon switch reboot, it is likely the user will be returned to the PMAC command prompt. This is not normally a "clean" exit back to the command prompt. If the user does get an error message, the user should execute the telent session below, as a secondary measure to ensure the switch gets reset to factory defaults.
		
		If the above procedures fails, log in via telnet and reset the switch to manufacturing defaults. If the above ssh procedures fails, log in via telnet and reset the switch to manufacturing defaults
		
		`# 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: Upon switch reboot, the user will be returned back to the PM&C command prompt.

3 ☐	**Management server:** Edit the switch configuration file template 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. Values to be modified by the user will be notated in this step by a preceding dollar sign. So a value that has $<some_variable_name> will need to be modified, removing the dollar sign and the less than, greater than sign.
		
		`# vi /usr/TKLC/smac/etc/6120XG_init.xml`
		`# vi /usr/TKLC/smac/etc/6120XG_[single,LAG]Uplink_configure.xml`

Procedure 17. Configure HP 6120XG Switch Pair(s) using NetConfig

4 ☐	**Management server:** setup netconfig repository	Use netConfig to create a repository entry for each 6120XG and/or 3020. This command will give the user several prompts. The prompts with <variables> as the answers are site specific that the user MUST modify. Other prompts that don't have a <variable> as an answer must be entered EXACTLY as they are shown here. If you do not know, stop now and contact Customer Care Center. Note that the "name=<switchType_location>" variable in the addDevice command needs to match the hostname of the switch ("<device>$swname</device>" in the xml file created in Step 2). Also the name parameter below should be switchType_Location, for example: ***name=3020_IOBAY1*** ***name=6120XG_IOBAY3*** **# netConfig --repo addDevice name=<switchType_location_name> --reuseCredentials** Device Vendor? HP Device Model? 6120 Should the init network adapter be added (y/n)? y Adding cli protocol for 6120XGC3020_IOBAY1 using network... What is the address used for network device access? <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 live oob adapter be added (y/n)? n Should the live network adapter be added (y/n)? y Adding sshInit protocol for 6120XG_IOBAY1 using network... Network device access already set: 10.240.8.7 Device named 6120XG_IOBAY1 successfully added. To check that you entered the information correctly, use the following command **# netConfig --repo listDevices** and check the output, which will be similar to the one shown below Device: 6120XG_IOBAY1 Vendor: HP Model: 6120 Access: Network: 10.240.8.10 Init Protocol Configured Live Protocol Configured [root@pmac5000101 ~]#

Procedure 17. Configure HP 6120XG Switch Pair(s) using NetConfig

5 ☐	**Management server:** Apply include-credentials command to the switch	Log in to the switch using SSH
		
		`# ssh manager@<enclosure_switch_IP>`
		
		`Switch# config`
		
		`Switch(config)# include-credentials`
		
		If prompted, answer yes to both questions.
		
		Log out of the switch, by running the following command. Answer yes to both questions when prompted.
		
		`Switch(config)# logout`
		
		`Do you want to log out [y/n]? y`
		`Do you want to save current configuration [y/n/^C]? y`

6 ☐	**Management server:** Initialize the switch	Run the following command to initialize the switch `# netConfig --file=/usr/TKLC/smac/etc/6120XG_init.xml` This should take about 2-3 minutes.

7 ☐	**Management server:** Configure the switch	Run the following command to configure the switch
		
		`# netConfig --file=`
		`/usr/TKLC/smac/etc/6120XG_[single,LAG]Uplink_configure.xml`
		
		This should take about 2-3 minutes.

8 ☐	**Management server:** Apply QoS Settings	Apply the QoS traffic template settings.
		
		`# netConfig --`
		`file=/usr/TKLC/smac/etc/switch/xml/addQOS_trafficTemplate_6120XG_BAY1.xml`
		
		Note: The switch will reboot after this command. This step will take 2-5 minutes.

9 ☐	**Management server:** Repeat for remaining 6120XG switches	For each HP 6120XG, repeat steps 2-8.

Procedure 17. Configure HP 6120XG Switch Pair(s) using NetConfig

10 ☐	**Management server:** Verify proper configuration of HP 6120XG switches	For each HP 6120XG, verify network reachability and configuration.
		
		`# ping -w3 <enclosure_switch_IP>`
		
		`# ssh manager@<enclosure_switch_IP>`
		
		`manager@10.240.8.10's password: <manager_password>`
		
		`Switch# show run`
		
		Inspect the output of "show run", and ensure that it is configured as per site requirements.

11 ☐	**Management server:** Backup Switch Configuration	Ensure the directory where the backups will be stored exists using the following command:
		
		`# ls /usr/TKLC/smac/etc/switch/backup`
		
		If an error is returned saying "No such file or directory", then create the directory using the following command
		
		`# mkdir /usr/TKLC/smac/etc/switch/backup`
		
		Change the currect path to the newly created directory using the following command
		
		`# cd /usr/TKLC/smac/etc/switch/backup`
		
		Execute the following commands to backup the switch
		
		`# netConfig --device=<switch_name> backupConfiguration service=ssh_service filename=<switch_name>-backup.orignet`
		
		Repeat the 2 commands above for the remaining switches.
		
		Verify switch configuration was backed up by cat <switch_name>-backup and inspect its contents to ensure it reflects the latest knwon good switch configurations.

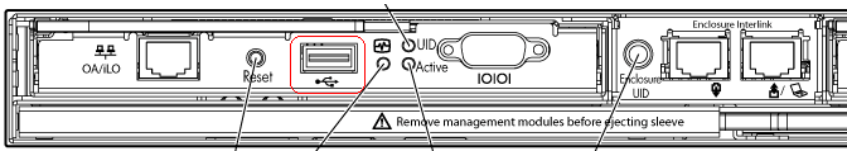
4.11 Server Blades Installation Preparation

Procedure 18. Upgrade Blade server Firmware

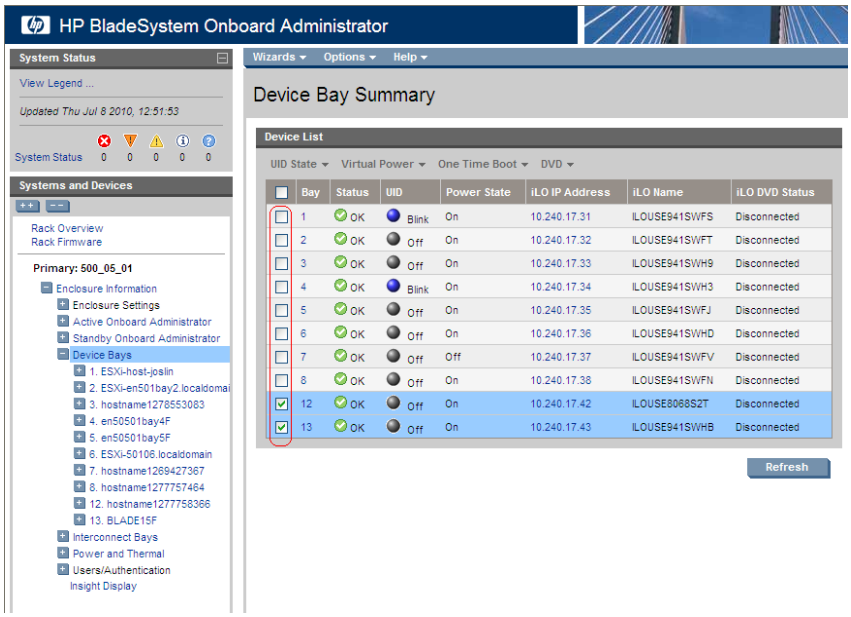
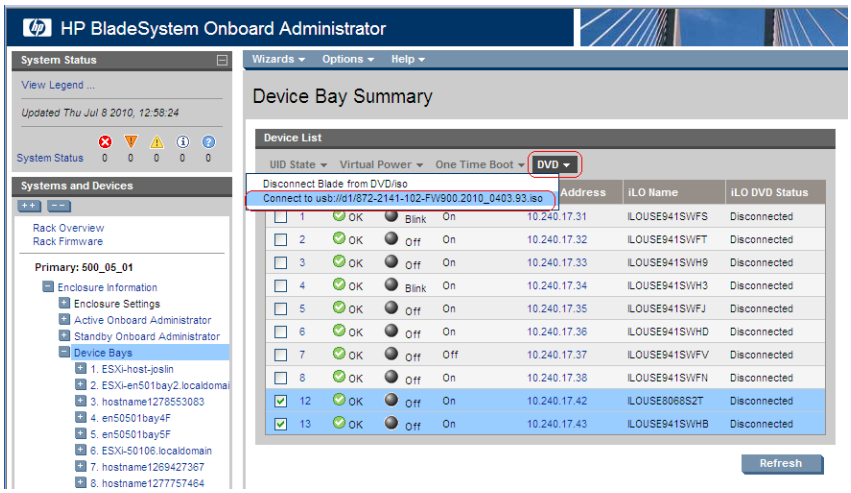
S T E P #		
	This procedure will provide the steps to upgrade the firmware on the Blade servers. **Prerequisite:** ***Procedure 16 and 17*** has been completed. **Needed material:** - HP Smart Update Firmware DVD - HP Solutions Firmware Upgrade Pack Release Notes [1] Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**OA iLO:** Check if Firmware upgrade is needed	Log onto the OA iLO using IE and navigate to **`Rack Firmware,`** you should be presented with the overview of all components in the enclosure as shown below. Scroll down the view the blades firmware. Check the ROM Version for all the blades in the enclosure. Device Firmware Information If the current verion is at or greater than the minimum supported version, skip this procedure, no upgrade is necessary.

Bay	Device Model	Firmware Component	Current Version
1	ProLiant BL460c G6	System ROM	I24 05/20/2010
		iLO2	iLO2 2.00 Jun 21 2010
		Power Management Controller	3.4
2	ProLiant BL460c G6	System ROM	I24 05/20/2010
		iLO2	iLO2 2.00 Jun 21 2010
		Power Management Controller	3.4
3	ProLiant BL460c G6	System ROM	I24 05/20/2010
		iLO2	iLO2 2.00 Jun 21 2010
		Power Management Controller	3.4
4	ProLiant BL460c G6	System ROM	I24 05/20/2010
		iLO2	iLO2 2.00 Jun 21 2010
		Power Management Controller	3.4

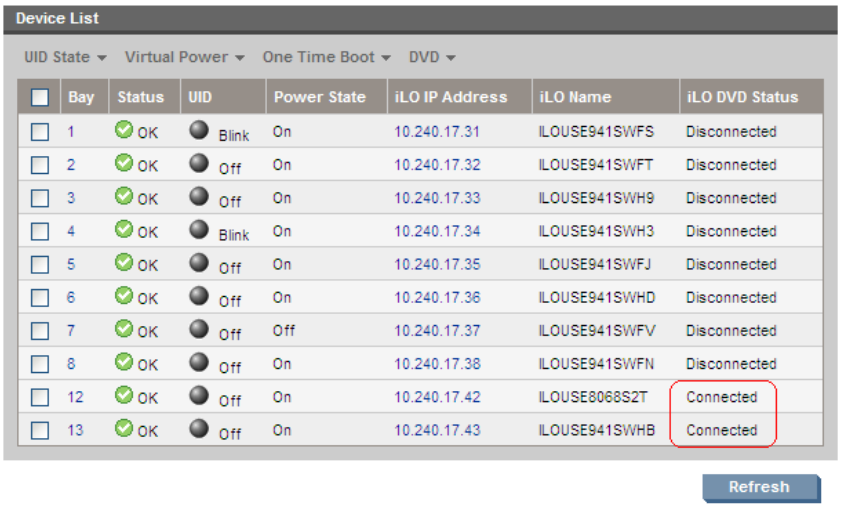
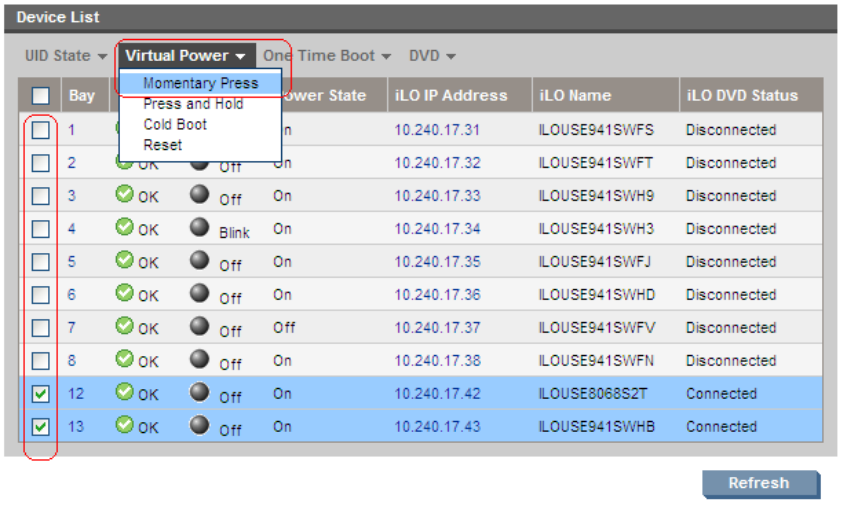
Procedure 18. Upgrade Blade server Firmware

2 ☐	**Local Workstation:** Import HP Firmware Maintenance CD	Insert the HP Smart Update Firmware DVD into the removable media drive of your local workstation. Use HP Solutions Firmware Upgrade Pack Release Notes [1] to select the proper part number. If your local workstation is a Linux machine, extract the iso image using the following commands, otherwise skip to the next step. Use the correct iso image part number from HP Solutions Firmware Upgrade Pack Release Notes [1]. # **getCDROM** # **dd if=/dev/scd0 of=/tmp/<image_part_number>.iso** Verify checksum of the extracted with the value listed in HP Solutions Firmware Upgrade Pack Release Notes [1]. # **/usr/bin/md5sum /tmp/<image_part_number>.iso** 422275a25353030fb5338876761ee1ca /tmp/872-XXXX-XXX-firmware.iso **Note**: The actual iso image in the output is for illustrative purposes only
3 ☐	**Local Workstation:** Create ISO file	If your local workstation is a windows machine, use an ISO creation tool such as "ImgBurn" to create an iso from the inserted disk. Use the correct iso image part number from HP Solutions Firmware Upgrade Pack Release Notes [1].
4 ☐	**Local Workstation:** Copy ISO to USB Media	Take the ISO you just mounted/created and copy it to USB media.
5 ☐	**c7000 Enclosure** Insert USB Flash Drive	Insert the USB Flash Drive with the *HP Smart Update Firmware* ISO into the USB port of the Active OA Module. 
6 ☐	**Local Workstation:** Access the Active OA	Access the Active OA Login Page from an Internet Explorer ® session using the following URL: **https://<OA_IP>/**
7 ☐	**OA Web GUI:** Log in to the Active OA Log in as an administrator user.	**User Name = <OA_admin_user>** **Password = <OA_admin_password>**

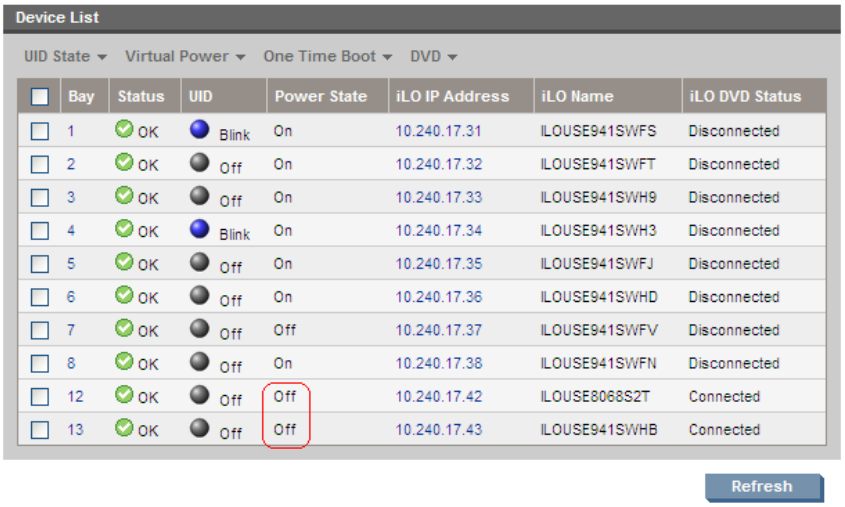
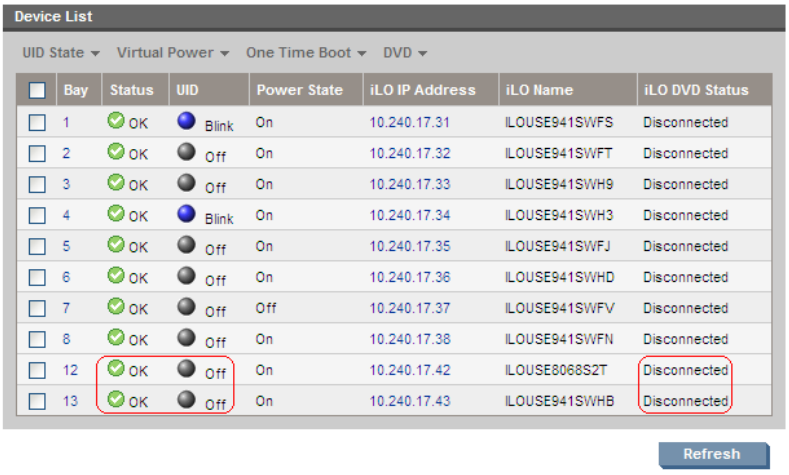
Procedure 18. Upgrade Blade server Firmware

8 ☐	**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 blades to be upgraded by clicking and enabling the corresponding UID checkbox.	 Note: **A maximum of 8 blades should be upgraded concurrently at one time. If the c7000 enclosure has more than 8 blades they will need to be upgraded to multiple sessions.**
9 ☐	**OA Web GUI:** Connect to USB Drive	Once the blades are selected, connect them to the ISO on the USB Drive, by selecting the **Connect to usb…** item from the **DVD** menu. 

Procedure 18. Upgrade Blade server Firmware

10 ☐	**OA Web GUI:** Verify Drive Connection	Once each blade has mounted the ISO media the **Device List** table should indicate an **iLO DVD Status** as *Connected* for each blade that was previously selected.  **Note**: The **Refresh** button may need to be clicked in order to see the current status of all blades.
11 ☐	**OA Web GUI:** Power Down Blades	If needed, reselect the UID checkbox for each blade to be upgraded and then select the **Momentary Press** option under the **Virtual Power** menu.  When prompted click the **OK** button to confirm the action.

Procedure 18. Upgrade Blade server Firmware

12 ☐	**OA Web GUI:** Verify Power Down	The power down sequence can take several minutes to complete. When it completes the **Device List** table will indicate the **Power State** of each select blade to be *Off*.  **Note**: The **Refresh** button may need to be clicked in order to see the current status of all blades.
13 ☐	**OA Web GUI:** Initiate Firmware Upgrade	To power the blades back on and begin the automated firmware upgrade process, repeat Steps 11 and 12 this time being sure the **Power State** indicates *On* for each selected blade.
14 ☐	**OA Web GUI:** Monitor Firmware Upgrade	From this point on each blade will boot into an automated firmware upgrade process that will last between *20 to 25 minutes*.  Upon a successful firmware upgrade, the **Device List** table will list each blade with a **Status** of *OK*, **UID** of *Off* and the **iLO DVD Status** as *Disconnected.* At this time the blades will automatically be rebooted. If the status does not update to disconnected, you can verify completion by opening an iLo window (via the OA) for each blade and watching the console for indication of firmware upgrade progress and successful completion If necessary, repeat Steps 8 through 14 for the remaining blades in the enclosure to be upgraded. Proceed to the next step.

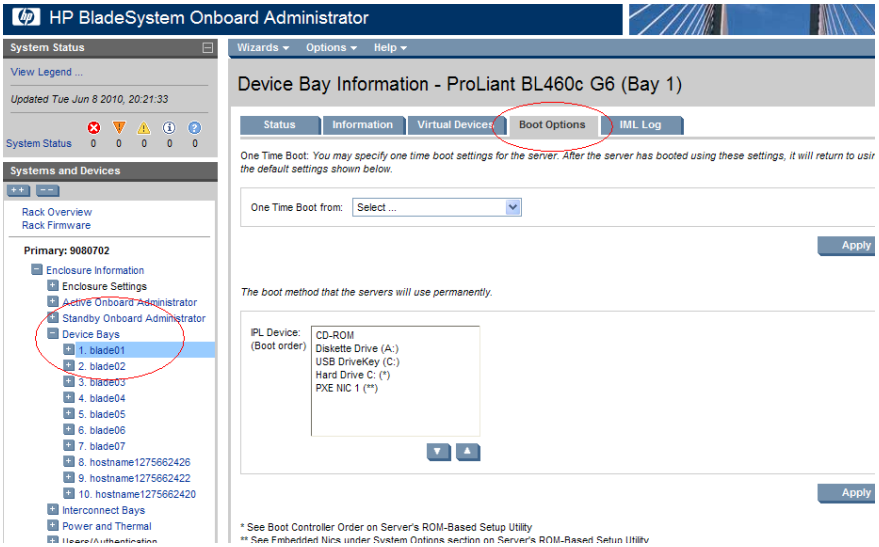
Procedure 18. Upgrade Blade server Firmware

15 ☐	**c7000 Enclosure** Remove USB Flash Drive	The USB flash drive may now safely be removed from the Active OA module.
16 ☐	Remove temporary file	After all blade servers have been upgraded, the file copied to laptop in Step 3 may be removed.

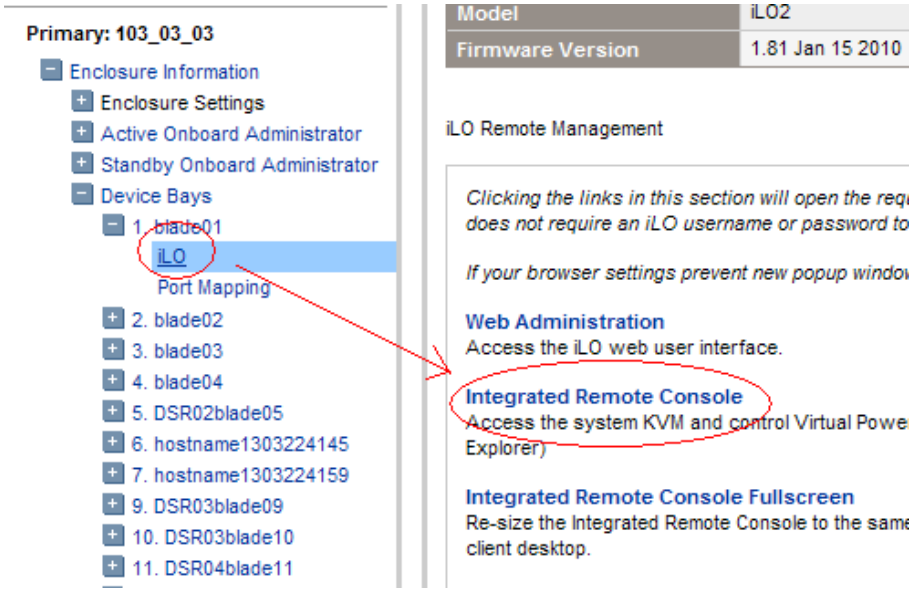
Procedure 19. Confirm/Update Blade server BIOS Settings

STEP #	This procedure will provide the steps to confirm and update the BIOS boot order on the Blade servers. **Prerequisite:** *Procedure 18. Upgrade Blade server Firmware* has been completed. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**OA GUI:** Login	Open your web browser and navigate to the OA IP address You will see following:  Login to HP OA as Administrator. Original password is on paper card attached to each OA.

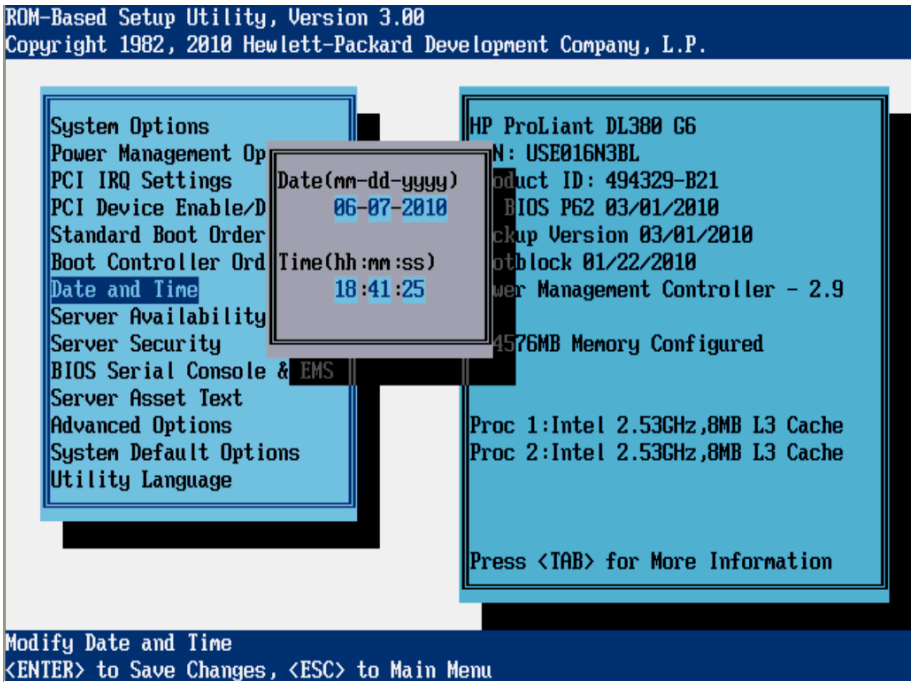
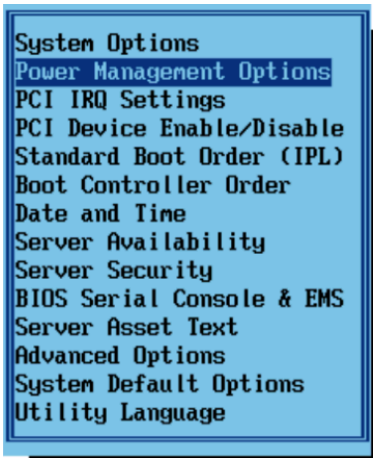
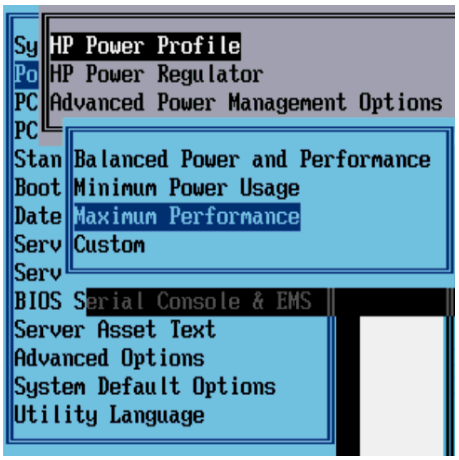
Procedure 19. Confirm/Update Blade server BIOS Settings

2 ☐	**OA:** Navigate to device Bay Settings	Navigate to **Enclosure Information** -> **Device Bays** -> **<Blade 1>** Click on **Boot Options** Tab 
3 ☐	**OA:** Verify/update Boot device Order	Verify that the Boot order is as follows. If it is not, use the up and down arrows to adjust the order to match the picture below, then click on **Apply** Note that for servers that do not have a CD-ROM, set USB to be on top. IPL Device: (Boot order) CD-ROM Diskette Drive (A:) USB DriveKey (C:) Hard Drive C: (*) PXE NIC 1 (**)

Procedure 19. Confirm/Update Blade server BIOS Settings

4 ☐	**OA:** Access the Blade iLO	Navigate to **Enclosure Information** -> **Device Bays** -> **<Blade 1>** -> **iLO** Click on **Integrated Remote Console**  This will launch the iLO interface for that blade. If this is the first time the iLO is being accessed, you will be prompted to install an addon to your web browser, follow the on screen instructions to do so.
5 ☐	**OA:** restart the blade and access the bios	You might be prompted with a certificate security warning, just press continue. Once a promt is displayed, login onto the blade using the “root” username. Once logged in, 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.

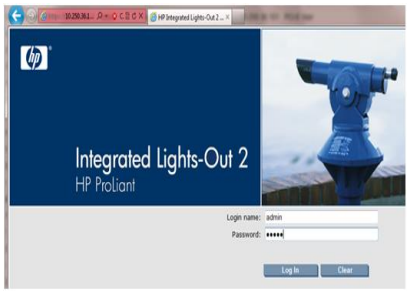
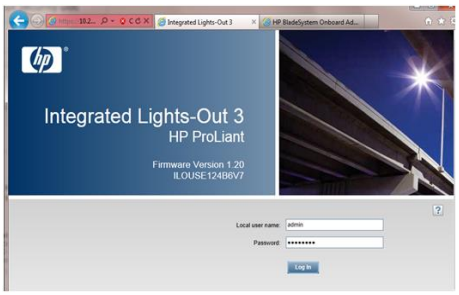
Procedure 19. Confirm/Update Blade server BIOS Settings

6 ☐	**OA:** Update bios settings	Scroll to *Date and Time* and press **Enter** Set current date, set current UTC time and press **Enter**.  Go back to the main menu by pressing **<Esc>** and scroll down to *Power Management Options* and press **Enter** Select *HP Power Profile* and press **Enter** Scroll down to *Maximum Performance* and press **Enter**   Press **<Esc>** twice to return to exit the BIOS setup screen and press **F10** to confirm Exiting the utility. The blade will reboot afterwards

Procedure 19. Confirm/Update Blade server BIOS Settings

7 ☐	**OA:** Repeat for the remaining blades	Repeat Steps 2 through 6 for the remaining blades. Once done, exit out of the OA GUI.

Procedure 20. Disable SNMP on iLO Interface

STEP #	This procedure will provide the steps to disable SNMP on the iLO interfaces of both rack mount servers and blades **Prerequisite:** *Procedure 18. Upgrade Blade server Firmware* has been completed. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**OA GUI:** Login	**This procedure needs to be repeated for every Rack Mount Server and blade in the system.** Open your web browser and navigate to the Blade iLO IP address You will see one of the following depending on the iLO Version   Login to the GUI using an Administrator account name and password.
2 ☐	**Blade iLO:** Navigate SNMP Management Page	If using iLO2, then select the **Administration** tab on the top navigation bar, then select the **Management** menu item on the left navigation bar to display the SNMP Settings page. If using iLO3 or iLO4, then **e**xpand the **Administration** menu item in the left hand navigation pane and select the **Management** sub-menu item to display the Management configuration page.
3 ☐	**Blade iLO:** Disable SNMP	Select option **Disabled** for each of the 3 SNMP settings as shown below, then click **Apply Settings** to save the change. The web page will refresh but no specific indication will be given that settings have been saved.

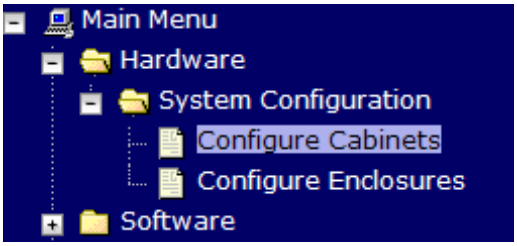
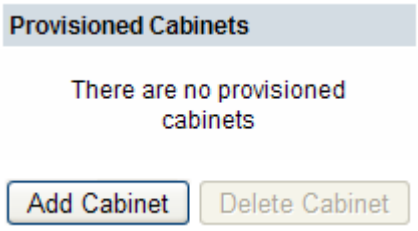
Procedure 20. Disable SNMP on iLO Interface

4 ☐	**Blade iLO:** Verify the Changes	To verify the setting change navigate away from the SNMP/Insight Manager Settings page and then go back to it to verify the SNMP settings are disabled. Click the **Log Out** link in upper right corner of page to log out of the iLO Web UI.
5 ☐	Complete for remaining iLO devices	Repeat this procedure all remaining iLO 2 Servers.

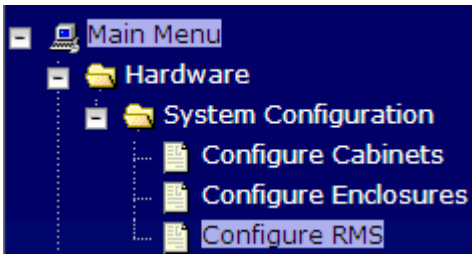
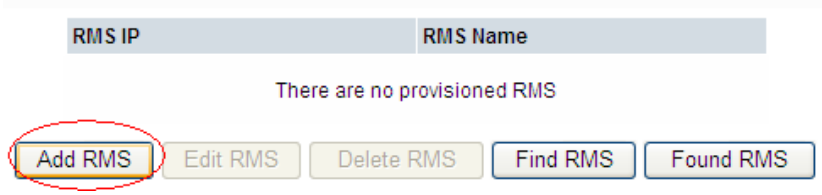
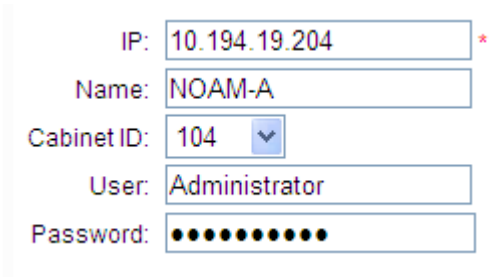
4.12 Install TVOE on Rack Mounted Servers

NOTE: IF THIS INSTALLATION DOES NOT HAVE NOAMP servers running on RMSes, then skip this entire section and continue with section 4.13

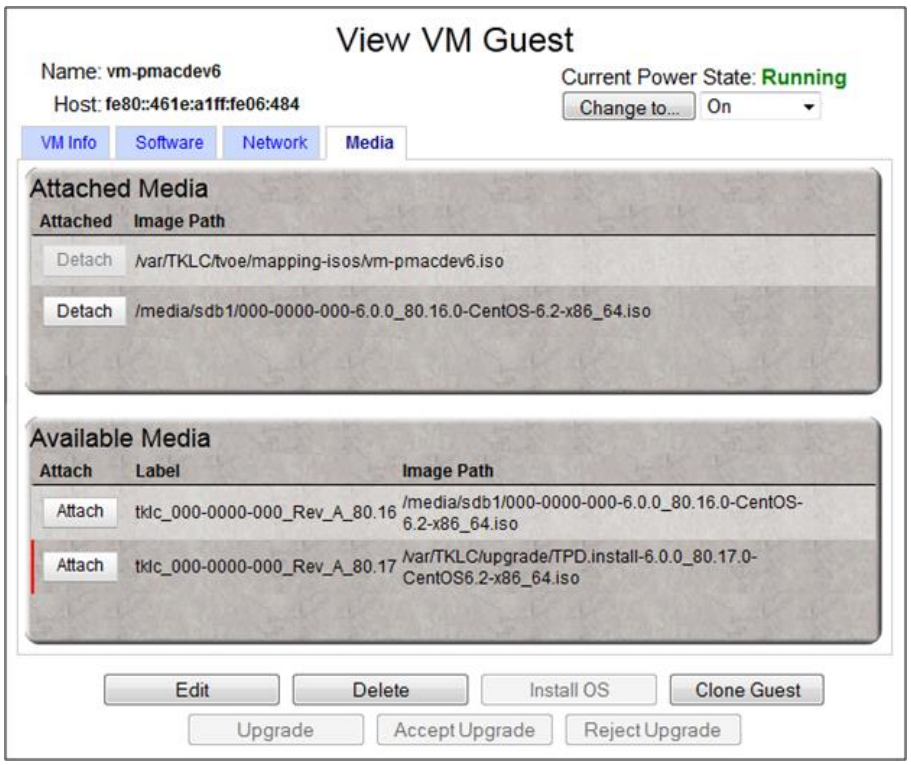
Procedure 21. Install TVOE on Additional RMS Server(s)

S T E P #		
	This procedure will install the TVOE operating system on the additional Rack Mounted Servers. Recall that TVOE has already been installed on the First RMS server which is running the PMAC software. **Prerequisite**: PMAC (virtualized) has been installed on the First RMS 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 TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**PM&C GUI:** Login	Open web browser and Login to PMAC GUI as pmacadmin user.
2 ☐	**PM&C GUI:** Configure Cabinets if Needed	Navigate to **Main Menu** -> **Hardware** -> **System Configuration** -> **Configure Cabinets**.  If you see this message:  Then press **Add Cabinet**, Enter a cabinet id for your RMS `systems`, then press **Add Cabinet** again. If there are already cabinets listed on this screen, then proceed ahead.

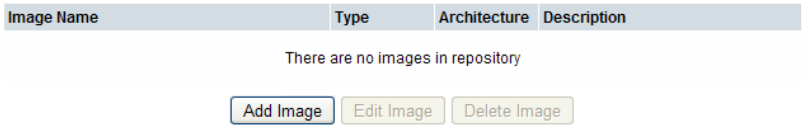
Procedure 21. Install TVOE on Additional RMS Server(s)

3 ☐	**PM&C GUI:** Configure RMS on PMAC Server	Navigate to **Main Menu -> Hardware -> System Configuration -> Configure RMS**.  Click **Add RMS**  Enter Information about the RMS server: It's iLO IP address, name, pick the cabinet ID, and finally enter the iLO username and password.  Click **Add RMS** The iLO IP address and name of the new RMS should now display: RMS IP: 10.194.19.204 RMS Name: NOAM-A **REPEAT THIS STEP FOR ANY ADDITIONAL RMSes YOU WISH THE PMAC TO CONFIGURE.**

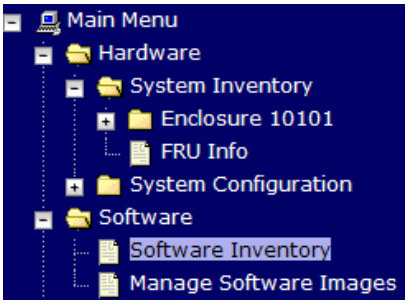
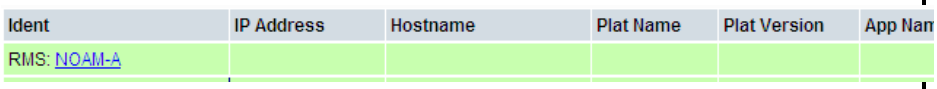
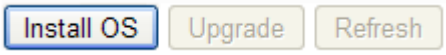
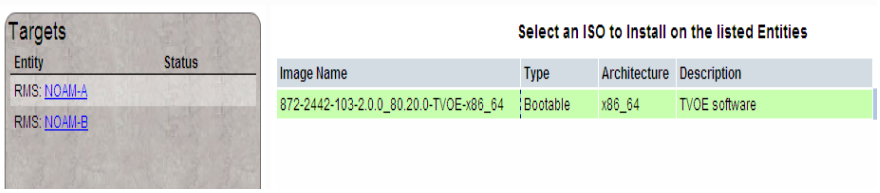
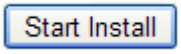
Procedure 21. Install TVOE on Additional RMS Server(s)

4 ☐	**TVOE Host:** Load TVOE 2.0 ISO	Add the TVOE ISO image to the PM&C, this can be done in one of three ways: 1. Insert the TVOE 2.0 **64 bit** CD required by the application into the removable media drive. 2. Attach the USB device containing the ISO image to a USB port. 3. Using a TVOE **64 bit** iso file cd into the directory where your ISO image is located on the **TVOE Host** (not on the PM&C server) Using scp, copy the ISO file to the PM&C `# scp <TVOE_image>.iso root@<pmac_management_network_ip>:/var/TKLC/smac/image/isoimages/home/smacftpusr/`
5 ☐	**PM&C GUI:** Attach the software Image to the PM&C Guest	If in Step 4 the ISO image was transferred directly to the PM&C guest via sftp, skip the rest of this step and continue with step 6. If the image is on a CD or USB device, continue with this step. In the PM&C GUI, nevigate to **Main Menu ➢ VM Managmenet.**. In the "**VM Entities**" list, select the PM&C guest. On the resulting "**View VM Guest**" page, 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 will appear in the "**Attached Media**" list. 

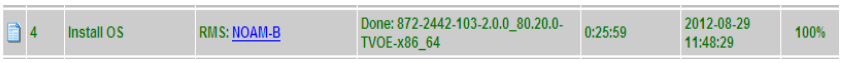
Procedure 21. Install TVOE on Additional RMS Server(s)

6 ☐	**PM&C GUI:** Add TVOE image	Navigate to **Main Menu -> Software -> Manage Software Images** Press **Add Image** button. Use the drop down to select the image.  If the image was supplied on a CD or a USB drive, it will appear as a virtual device ("device://…"). These devices are assigned in numerical order as CD and USB images become available on the Management Server. The first virtual device is reserved for internal use by TVOE and PM&C; therefore, the iso image of interest is normally present on the second device, "device://dev/sr1". If one or more CD or USB-based images were already present on the Management Server before you started this procedure, choose a correspondingly higher device number. If in Step 4 the image was transferred to PM&C via sftp it will appear in the list as a local file "/var/TKLC/...".  Select the appropriate path and Press **Add New Image** button. You may check the progress using the `Task Monitoring` link. Observe the green bar indicating success. Once the green bar is displayed, remove the TVOE 2.0 Media from the optical drive of the management server.

Procedure 21. Install TVOE on Additional RMS Server(s)

7 ☐	**PM&C GUI:** Select RMS Servers for TVPE OS install	Navigate to **Software -> Software Inventory**.  Select the RMS servers you want to IPM. If you want to install the same OS image to more than one server, you may select multiple servers by clicking multiple rows individually. Selected rows will be highlighted in green.  Click on **Install OS** 
8 ☐	**PM&C GUI:** Initiate OS Install on RMS Server(s)	The left side of this screen shows the servers to be affected by this OS installation. From the list of available bootable images on the right side of the screen, select one OS image to install to all of the selected servers.  Click on **Start Install**, a confirmation window will pop up, click on **Ok** to proceed with the install. 

Procedure 21. Install TVOE on Additional RMS Server(s)

9 ☐	**PM&C GUI:** Monitor OS Install	Navigate to **Main Menu** > **Task Monitoring** to monitor the progress of the TVOE Installation background task. A separate task will appear for each blade affected.  When the installation is complete, the task will change to green and the Progress bar will indicate "100%". 

	ID	Task	Target	Status	Running Time	Start Time	Progress
	14	Install OS	Enc:10101 Bay:15F	Boot install image	0:00:01	2011-09-20 11:12:02	50%
	13	Install OS	Enc:10101 Bay:8F	Boot install image	0:00:01	2011-09-20 11:12:02	50%
	12	Install OS	Enc:10101 Bay:7F	Boot install image	0:00:01	2011-09-20 11:12:02	50%
	11	Install OS	Enc:10101 Bay:2F	Boot install image	0:00:01	2011-09-20 11:12:02	50%
	10	Install OS	Enc:10101 Bay:1F	Boot install image	0:00:02	2011-09-20 11:12:01	50%
	9	Add Image		Done: TPD.install-5.0.0_72.20.0-CentOS5.6-x86_64	0:00:09	2011-09-20 11:01:50	100%

	4	Install OS	RMS: NOAM-B	Done: 872-2442-103-2.0.0_80.20.0-TVOE-x86_64	0:25:59	2012-08-29 11:48:29	100%

Procedure 22. Continue TVOE Configuration on First RMS Server

S T E P #	This procedure will extend the TVOE networking configuration on the First RMS server in preparation for the installation of the NOAMP VM on that RMS. **NOTE: If a NOAMP VM will NOT be co-located with the PMAC VM on the First RMS (for instance, this server will only run PMAC, but there are 2 additional RMS which will not), then skip this procedure and continue with the next procedure.** **Prerequisite**: TVOE and PMAC (virtualized) have been installed on the First RMS 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 TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.

Procedure 22. Continue TVOE Configuration on First RMS Server

<table>
<tr><td>1
☐</td><td>Determine Bridge names and interfaces for XMI and IMI, and Netbackup (if used) networks.</td><td>Determine the bridge names and physical bridge interfaces to be used on the TVOE server for the NOAMP XMI and IMI networks. Based on the site survey, you will need to determine if you are using vlan tagging or not, what bonds will be used, and also the actual Ethernet interfaces that will make up those bonds.

If the netbackup bridge and interface were not previously configured on this server when PMAC was installed, determine those values as well.

Fill in the appropriate values in the table below:

<table>
<tr><th>NOAM&P Guest Interface Name</th><th>TVOE Bridge Name</th><th>TVOE Bridge Interface</th></tr>
<tr><td>xmi</td><td>xmi</td><td>Interface Bond:

_____

<TVOE_XMI_Bridge_Interface_Bond>

Interface Name (will be same as interface bond if not using tagging):

_____

<TVOE_XMI_Bridge_Interface></td></tr>
<tr><td>imi</td><td>imi</td><td>Interface Bond:

_____

<TVOE_IMI_Bridge_Interface_Bond>

Interface Name (will be same as interface bond if not using tagging):

_____

<TVOE_IMI_Bridge_Interface></td></tr>
<tr><td>netbackup</td><td>netbackup</td><td>: Interface Name

_____

<TVOE_NetBackup_Bridge_Interface></td></tr>
</table>
</td></tr>
<tr><td>2
☐</td><td>First RMS Server:
Login</td><td>Log in to the TVOE prompt of the first RMS server (the one running the PMAC). Use either the iLO facility, or the TVOE’s IP address on the management network.</td></tr>
</table>

Procedure 22. Continue TVOE Configuration on First RMS Server

3 ☐	**First RMS Server:** Configure XMI Bridge Interface Bond	Verify the xmi bridge interface bond by running the following command:
		
		Note: The output below is for illustrative purposes only. The example output below shows the control bridge configured.
		
		`# netAdm query –device=<TVOE_XMI_Bridge_Bond>`
		
		`Protocol: none`
		`On Boot: yes`
		`Persistent: yes`
		`Bonded Mode: active-backup`
		`Enslaving: eth01 eth02`
		
		If the bond has already been configured you will see output similar to what you see above. If this is so, **skip to the next step**. Otherwise, continue with this step.
		
		Create bonding interface and associate subordinate interfaces with bond:
		
		`# netAdm add --device=<TVOE_XMI_Bridge_Bond>`
		`--onboot=yes --type=Bonding --mode=active-backup --miimon=100`
		`Interface <TVOE_XMI_Bridge_Bond> added`
		
		`# netAdm set --device=<TVOE_XMI_Bridge_Bond_Ethernet1> --`
		`type=Ethernet`
		`--master=<TVOE_XMI_Bridge_Bond> --slave=yes --onboot=yes`
		`Interface <TVOE_XMI_Bridge_Bond_Ethernet1> updated`
		
		`# netAdm set --device=<TVOE_XMI_Bridge_Bond_Ethernet2> --`
		`type=Ethernet`
		`--master=<TVOE_XMI_Bridge_Bond> --slave=yes --onboot=yes`
		`Interface <TVOE_XMI_Bridge_Bond_Ethernet2> updated`

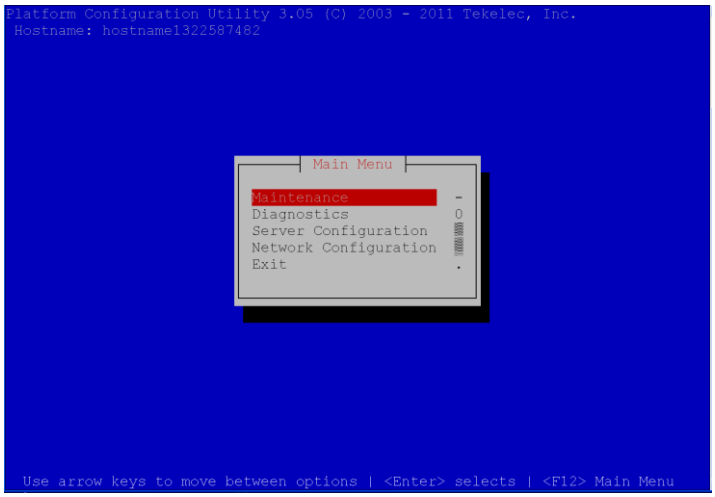
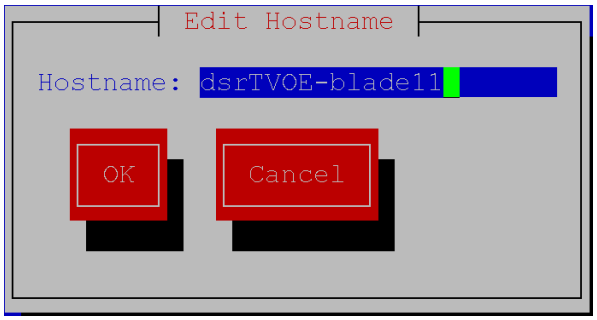
4 ☐	**First RMS Server:** Create XMI Bridge	Perform the following command if you are using VLAN tagging.
		If not, skip to the next com**mand:**
		
		`# netAdm add –device=<TVOE_XMI_Bridge_Interface> --onboot=yes`
		`Interface <TVOE_XMI_Bridge_Interface> created.`
		
		`# netAdm add --type=Bridge --name=xmi--onboot=yes`
		`--bridgeInterfaces=<TVOE_XMI_Bridge_Interface>`
		
		`Interface <TVOE_XMI_Bridge_Interface> updated.`
		`Bridge xmi created.`

Procedure 22. Continue TVOE Configuration on First RMS Server

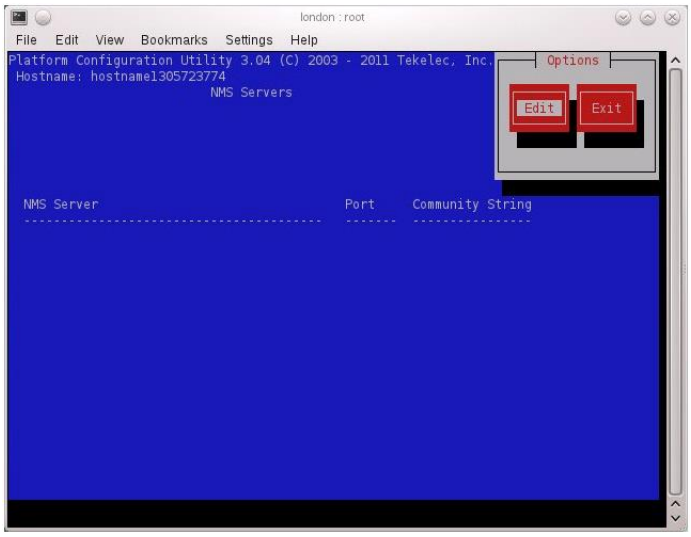
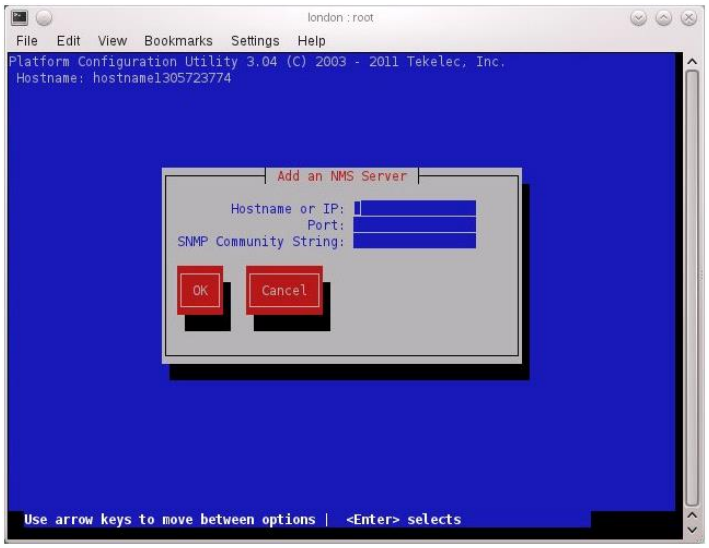
5 ☐	**First RMS Server:** Configure IMI Bridge Interface Bond	Verify the imi bridge interface bond by running the following command:
		
		Note: The output below is for illustrative purposes only. The example output below shows the control bridge configured.
		
		`# netAdm query –device=<TVOE_IMI_Bridge_Bond>`
		
		`Protocol: none`
		`On Boot: yes`
		`Persistent: yes`
		`Bonded Mode: active-backup`
		`Enslaving: eth01 eth02`
		
		If the bond has already been configured you will see output similar to what you see above. If this is so, **skip to the next step**. Otherwise, continue with this step.
		
		Create bonding interface and associate subordinate interfaces with bond:
		
		`# netAdm add --device=<TVOE_IMI_Bridge_Bond>`
		`--onboot=yes --type=Bonding --mode=active-backup --miimon=100`
		`Interface <TVOE_IMI_Bridge_Bond> added`
		
		`# netAdm set --device=<TVOE_IMI_Bridge_Bond_Ethernet1> --type=Ethernet`
		`--master=<TVOE_IMI_Bridge_Bond> --slave=yes --onboot=yes`
		`Interface <TVOE_IMI_Bridge_Bond_Ethernet1> updated`
		
		`# netAdm set --device=<TVOE_IMI_Bridge_Bond_Ethernet2> --type=Ethernet`
		`--master=<TVOE_IMI_Bridge_Bond> --slave=yes --onboot=yes`
		`Interface <TVOE_IMI_Bridge_Bond_Ethernet2> updated`

6 ☐	**First RMS Server:** Create IMI Bridge	Perform the following command if you are using VLAN tagging.
		If not, skip to the next command:
		
		`# netAdm add --device=<TVOE_IMI_Bridge_Interface> --onboot=yes`
		`Interface <TVOE_IMI_Bridge_Interface> created.`
		
		`# netAdm add --type=Bridge --name=imi--onboot=yes`
		`--bridgeInterfaces=<TVOE_IMI_Bridge_Interface>`
		
		`Interface <TVOE_IMI_Bridge_Interface> updated.`
		`Bridge imi created.`

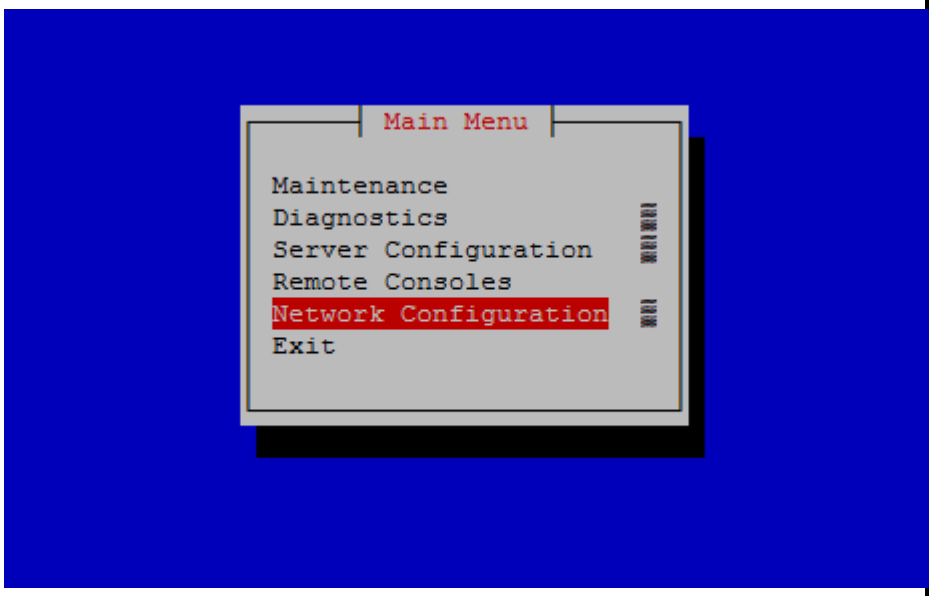
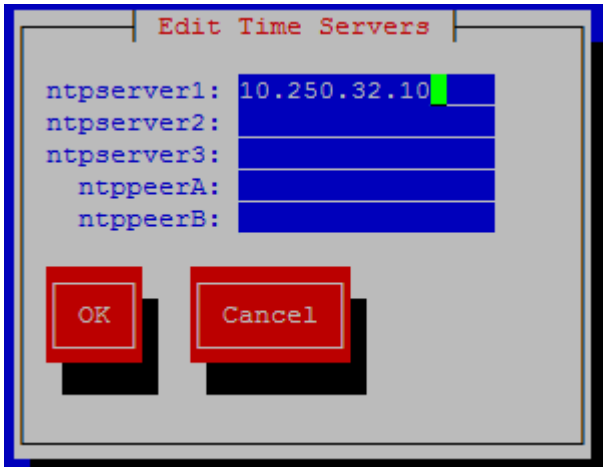
Procedure 22. Continue TVOE Configuration on First RMS Server

7 ☐	**RMS Server iLO:** Set Hostname	**# su - platcfg**  Navigate to **Sever Configuration->Hostname-> Edit** and enter a new hostname for your server.  Press **OK** and select and continue to press Exit until you are at the platcfg main menu again. NOTE: Although the new hostname has been properly configured and committed at this point, it will not appear on your command prompt unless you log out and log back in again

Procedure 22. Continue TVOE Configuration on First RMS Server

8 ☐	**RMS Server iLO:** Configure SNMP	From the platcfg main menu, navigate to **Network Configuration -> SNMP Configuration -> NMS Configuration**  Press **Edit**. Choose **Add a New NMS Server**  Enter the Hostname/IP of the Customer NMS Server, for port enter 162, and for Community String enter the community string provided in the customer NAPD Document. Press **Exit**. Select Yes when prompted to restart the Alarm Routing Service. Optionally, additional NMS Servers can be specified by repeating the steps above, such as NOAMP VIP, SOAM VIP, etc. Once Done, press **Exit** to quit to the platcfg main menu.

Procedure 22. Continue TVOE Configuration on First RMS Server

9 ☐	**RMS Server iLO:** Configure NTP	Navigate to **Network Configuration**  Navigate **to Configuration->NTP** Click **Edit**  Enter the customer provided NTP server IP address(es) Press **OK** **P**ress **Exit** to return to the platcfg menu.
10 ☐	**First RMS Server:** Create Netbackup bridge (Optional)	Perform the following command if you will have a dedicated Netbackup interface within your NOAMP guests (and if the Netbackup bridge was NOT configured when setting up the PMAC earlier) **# netAdm add --type=Bridge --name=<TVOE_NetBackup_Bridge> --onboot=yes --MTU=<NetBackup_MTU_size> --bridgeInterfaces=<TVOE_NetBackup_Bridge_Interface>**

Procedure 22. Continue TVOE Configuration on First RMS Server

11 ☐	**First RMS Server and Customer provided Backup Server:** Backup TVOE files	This step backs up the TVOE files to a customer provided backup server.
		
		<u>If NetBackup is being used, then this step should be skipped. Select 'Exit' to exit out of platcfg.</u>
		
		<u>If Netback</u> isn't used, execute the following:
		
		1. Select the following menu options sequentially:
		Maintenance ➢ Backup and Restore ➢ Backup Platform (CD/DVD).
		The 'Backup TekServer Menu' page will now be shown.
		
		2. Build the backup ISO image by selecting:
		Build ISO file only
		
		Note: Creating the ISO image may happen so quickly that this screen may only appear for an instant.
		
		After the ISO is created, platcfg will return to the Backup TekServer Menu. 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"
		
		3. Exit out of platcfg by selecting '**Exit'.**
		
		4. Login to the customer server and copy backup image to the customer server where it can be safely stored. If the customer system is a Linux system, please execute the following command to copy the backup image to the customer system.
		
		`# scp tvoexfer@<TVOE IP Address>:backup/* /path/to/destination/`
		
		5. 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`
		
		If the Customer System is a Windows system please refer to reference [4] *Platform 6.x Configuration Procedure Reference,* Appendix A Using WinSCP to copy the backup image to the customer system.
		
		The TVOE backup file has now been successfully placed on the Customer System.

Procedure 23. Configure TVOE on Additional RMS Server(s)

S T E P #	This procedure will configure TVOE networking on RMS Servers *other* than the first one which has already been installed and is running PMAC. NOTE: You will repeat this procedure for each additional RMS you wish to configure TVOE for. **Prerequisite**: RMS Server has been IPM'ed with TVOE 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 TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.

Procedure 23. Configure TVOE on Additional RMS Server(s)

<table>
<tr>
<td>1
☐</td>
<td>Determine Bridge names and interfaces for XMI and IMI, and Netbackup (if used) networks.</td>
<td>Determine the bridge names and physical bridge interfaces to be used on the TVOE server for the Management, XMI and IMI networks. Based on the site survey, you will need to determine if you are using vlan tagging or not, what bonds will be used, and also the actual Ethernet interfaces that will make up those bonds.

Fill in the appropriate values in the table below:

<table>
<tr><th>NOAM&P Guest Interface Name</th><th>TVOE Bridge Name</th><th>TVOE Bridge Interface</th></tr>
<tr><td>xmi</td><td>xmi</td><td>Interface Bond:

_____

<TVOE_XMI_Bridge_Interface_Bond>

Interface Name (will be same as interface name if not using tagging):

_____

<TVOE_XMI_Bridge_Interface></td></tr>
<tr><td>imi</td><td>imi</td><td>Interface Bond:

_____

<TVOE_IMI_Bridge_Interface_Bond>

Interface Name (will be same as interface name if not using tagging):

_____

<TVOE_IMI_Bridge_Interface></td></tr>
<tr><td>netbackup</td><td>netbackup</td><td>: Interface Name

_____

<TVOE_NetBackup_Bridge_Interface></td></tr>
<tr><td>management</td><td>management</td><td>Interface Name

_____

<TVOE_Management_Bridge_Interface></td></tr>
</table>
</td>
</tr>
</table>

Procedure 23. Configure TVOE on Additional RMS Server(s)

2 ☐	**RMS Server iLO:** Login	Log in to the TVOE prompt of the RMS Server using the iLO facility.

3 ☐	**RMS Server iLO:** Modify control bridge if using tagged control interface (Optional)	**If you are using VLAN tagging for your control interface, you must reconfigure the default control bridge configuration. Otherwise, skip this step and proceed to the next step.**
		
		`# netAdm set --type=Bridge –name=control --delBridgeInt=bond0`
		`Bridge control updated.`
		
		`# netAdm add --device=bond0.<control_VLAN_ID>`
		`--onboot=yes`
		`Interface bond0.X added`
		
		`# netAdm set --type=Bridge –name=control --`
		`addBridgeInt=bond0.<control_VLAN_ID>`
		`Bridge control updated.`

4 ☐	**RMS Server iLO:** Configure XMI Bridge Interface Bond	Verify the xmi bridge interface bond by running the following command:
		
		Note: The output below is for illustrative purposes only. The example output below shows the control bridge configured.
		
		`# netAdm query –device=<TVOE_XMI_Bridge_Bond>`
		
		`Protocol: none`
		`On Boot: yes`
		`Persistent: yes`
		`Bonded Mode: active-backup`
		`Enslaving: eth01 eth02`
		
		If the bond has already been configured you will see output similar to what you see above. If this is so, **skip to the next step**. Otherwise, continue with this step.
		
		Create bonding interface and associate subordinate interfaces with bond:
		
		`# netAdm add --device=<TVOE_XMI_Bridge_Bond>`
		`--onboot=yes --type=Bonding --mode=active-backup --miimon=100`
		`Interface <TVOE_XMI_Bridge_Bond> added`
		
		`# netAdm set --device=<TVOE_XMI_Bridge_Bond_Ethernet1> --`
		`type=Ethernet`
		`--master=<TVOE_XMI_Bridge_Bond> --slave=yes --onboot=yes`
		`Interface <TVOE_XMI_Bridge_Bond_Ethernet1> updated`
		
		`# netAdm set --device=<TVOE_XMI_Bridge_Bond_Ethernet2> --`
		`type=Ethernet`
		`--master=<TVOE_XMI_Bridge_Bond> --slave=yes --onboot=yes`
		`Interface <TVOE_XMI_Bridge_Bond_Ethernet2> updated`

Procedure 23. Configure TVOE on Additional RMS Server(s)

5 ☐	**RMS Server iLO:** Create XMI Bridge and add default route to XMI network	**Perform the following command if you are using VLAN tagging. If not, skip to the next command:** # **netAdm add –device=<TVOE_XMI_Bridge_Interface> --onboot=yes** Interface <TVOE_XMI_Bridge_Interface> created. # **netAdm add --type=Bridge --name=xmi--onboot=yes --bridgeInterfaces=<TVOE_XMI_Bridge_Interface>** Interface <TVOE_XMI_Bridge_Interface> updated. Bridge xmi created.
6 ☐	**RMS Server iLO:** Configure IMI Bridge Interface Bond	Verify the imi bridge interface bond by running the following command: **Note:** The output below is for illustrative purposes only. The example output below shows the control bridge configured. # **netAdm query –device=<TVOE_IMI_Bridge_Bond>** Protocol: dhcp On Boot: yes Persistent: yes Bonded Mode: active-backup Enslaving: eth01 eth02 If the bond has already been configured you will see output similar to what you see above. If this is so, **skip to the next step**. Otherwise, continue with this step. Create bonding interface and associate subordinate interfaces with bond: # **netAdm add --device=<TVOE_IMI_Bridge_Bond> --onboot=yes --type=Bonding --mode=active-backup --miimon=100** Interface <TVOE_IMI_Bridge_Bond> added # **netAdm set --device=<TVOE_IMI_Bridge_Bond_Ethernet1> --type=Ethernet --master=<TVOE_IMI_Bridge_Bond> --slave=yes --onboot=yes** Interface <TVOE_IMI_Bridge_Bond_Ethernet1> updated # **netAdm set --device=<TVOE_IMI_Bridge_Bond_Ethernet2> --type=Ethernet --master=<TVOE_IMI_Bridge_Bond> --slave=yes --onboot=yes** Interface <TVOE_IMI_Bridge_Bond_Ethernet2> updated

Procedure 23. Configure TVOE on Additional RMS Server(s)

7 ☐	**RMS Server iLO:** Create IMI Bridge	**Perform the following command if you are using VLAN tagging. If not, skip to the next command:** # **netAdm add --device=<TVOE_IMI_Bridge_Interface> --onboot=yes** Interface <TVOE_IMI_Bridge_Interface> created. # **netAdm add --type=Bridge --name=imi--onboot=yes --bridgeInterfaces=<TVOE_IMI_Bridge_Interface>** Interface <TVOE_IMI_Bridge_Interface> updated. Bridge imi created.

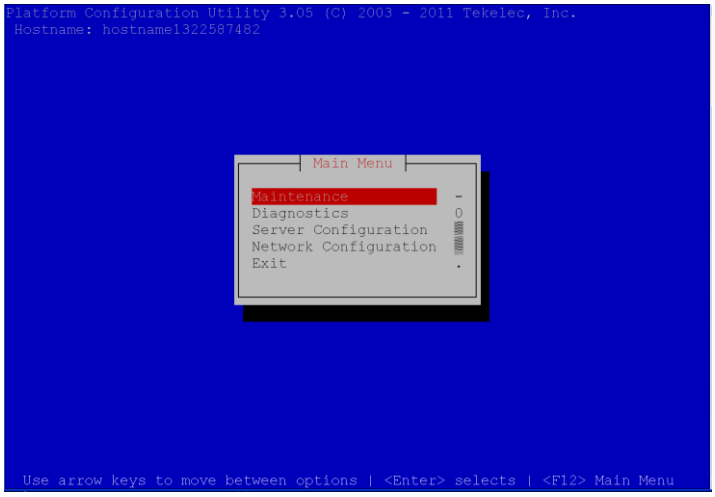
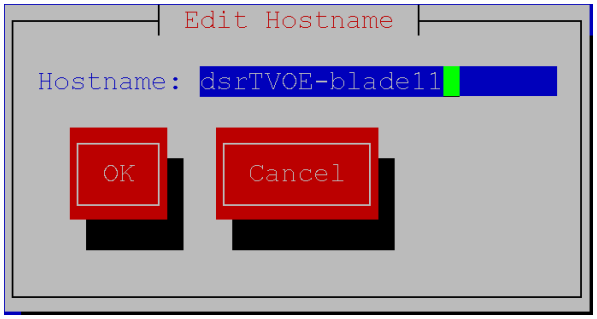
Procedure 23. Configure TVOE on Additional RMS Server(s)

8 ☐	**Management server iLO:** Create management bridge and assign TVOE Management IP and default route	**Note:** The output below is for illustrative purposes only. The site information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure. If <TVOE_Management_Bridge_Interface> or the bond it is based on (if using tagged interface) has not yet been created, then execute the nex 3 commands. Otherwise, skip to the "EXAMPLE…" section: **# netAdm add --device=<TVOE_Management_Bridge_Interface_Bond> --onboot=yes --type=Bonding --mode=active-backup --miimon=100** Interface <TVOE_Management_Bridge_Interface> added **# netAdm set --device=<mgmt_ethernet_interface1> --type=Ethernet --master=<TVOE_Management_Bridge_Interface_Bond> --slave=yes --onboot=yes** Interface <mgmt_ethernet_interface1> updated **# netAdm set --device=<mgmt_ethernet_interface2> --type=Ethernet --master-<TVOE_Management_Bridge_Interface_Bond> --slave=yes --onboot=yes** Interface <mgmt_ethernet_interface2> updated EXAMPLE 1: Create Management bridge using untagged interfaces (<TVOE_Management_Bridge>). **# netAdm add --type=Bridge --name=management --bootproto=none --onboot=yes --address=<TVOE_RMSX_Mgmt_IP_Address> --netmask=<TVOE_RMS_Mgmt_Netmask> --bridgeInterfaces=<TVOE_Management_Bridge_Interface>** EXAMPLE 2: Create Management bridge using tagged interfaces **# netAdm add --device=<TVOE_Management_Bridge_Interface>** **# netAdm add --type=Bridge --name=management --address=<TVOE_RMSX_Mgmt_IP_Address > --netmask=<TVOE_RMS_Mgmt_Netmask> --onboot=yes --bridgeInterfaces=<TVOE_Management_Bridge_Interface>** Cretate default route (execute regardless of which example is chosen): **# netAdm add --route=default -gateway=<mgmt_gateway_address> --device=management** Route to management created.

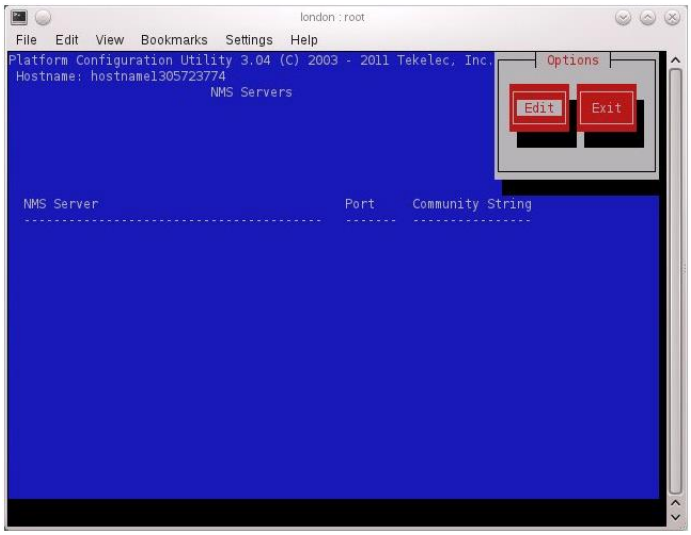
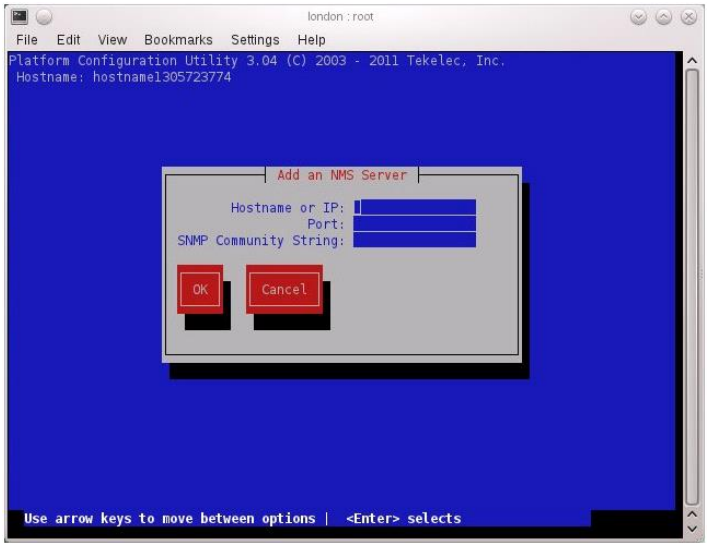
Procedure 23. Configure TVOE on Additional RMS Server(s)

9 ☐	**RMS Server iLO:** Create Netbackup bridge (Optional)	**Perform the following command if you will have a dedicated Netbackup interface within your NOAMP guests (and if the Netbackup bridge was NOT configured when setting up the PMAC earlier)** # **netAdm add --type=Bridge --name=<TVOE_NetBackup_Bridge> --onboot=yes --MTU=<NetBackup_MTU_size> --bridgeInterfaces=<TVOE_NetBackup_Bridge_Interface>**

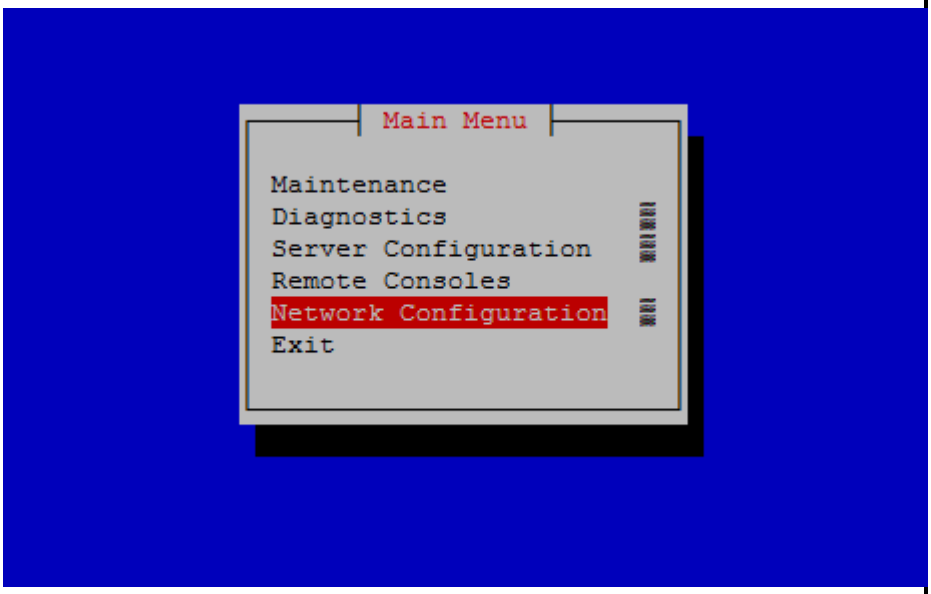
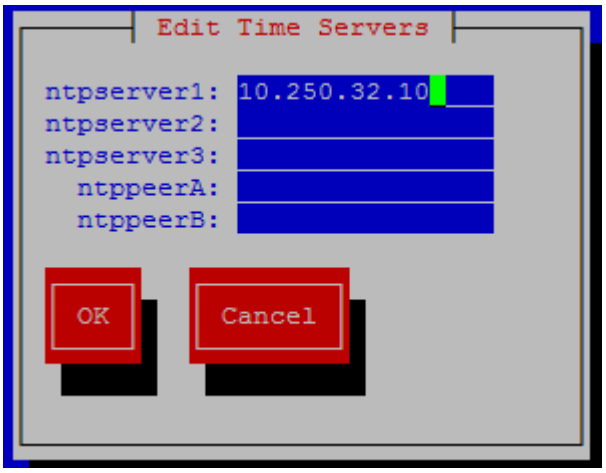
Procedure 23. Configure TVOE on Additional RMS Server(s)

10 ☐	**RMS Server iLO:** Set Hostname	# **su - platcfg**  Navigate to **Sever Configuration->Hostname-> Edit** and enter a new hostname for your server.  Press **OK** and select and continue to press **Exit** until you are at the platcfg main menu again. Continue To Press **Exit** until you are back at the platcfg main menu **NOTE:** Although the new hostname has been properly configured and committed at this point, it will not appear on your command prompt unless you log out and log back in again

Procedure 23. Configure TVOE on Additional RMS Server(s)

11 ☐	**RMS Server iLO:** Configure SNMP	From the platcfg main menu, navigate to **Network Configuration -> SNMP Configuration -> NMS Configuration**  Press **Edit.** Choose **Add a New NMS Server**  Enter the *Hostname/IP* of the NO VIP, for *port* enter 162, and for *Community String* enter the value provided by the customer in the NAPD document. Press **Exit.** Select **Yes** when prompted to restart the Alarm Routing Service. Optionally, add any customer provided NMS Servers by repeating the step above. Once Done, press **Exit** to quit to the platcfg main menu.

Procedure 23. Configure TVOE on Additional RMS Server(s)

12 ☐	**RMS Server iLO:** Configure NTP	Navigate to Network Configuration  Navigate to **Configuration->NTP** Click **Edit**  Enter the customer provided NTP server IP address(es) Press **OK** Continue to press Exit until you are out of the platcfg menu.

13 ☐	**RMS Server:** Create Netbackup bridge (Optional)	Perform the following command if you will have a dedicated Netbackup interface within your NOAMP guests (and if the Netbackup bridge was NOT configured when setting up the PMAC earlier) `# netAdm add --type=Bridge --name=<TVOE_NetBackup_Bridge> --onboot=yes --MTU=<NetBackup_MTU_size> --bridgeInterfaces=<TVOE_NetBackup_Bridge_Interface>`

14 ☐	**RMS Server and Customer provided Backup Server:** Backup TVOE files	This step backs up the TVOE files to a customer provided backup server.
		
		If NetBackup is being used, then this step should be skipped. Select 'Exit' to exit out of platcfg.
		
		If Netback isn't used, execute the following:
		
		1. Select the following menu options sequentially:
		Maintenance ➢ Backup and Restore ➢ Backup Platform (CD/DVD).
		The 'Backup TekServer Menu' page will now be shown.
		
		2. Build the backup ISO image by selecting **Build ISO file only**
		
		Note: Creating the ISO image may happen so quickly that this screen may only appear for an instant.
		
		After the ISO is created, platcfg will return to the Backup TekServer Menu. 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"
		
		3. Exit out of platcfg by selecting '**Exit'.**
		
		4. Login to the customer server and copy backup image to the customer server where it can be safely stored. If the customer system is a Linux system, please execute the following command to copy the backup image to the customer system.
		
		`# scp tvoexfer@<TVOE IP Address>:backup/* /path/to/destination/`
		
		5. 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`
		
		If the Customer System is a Windows system please refer to reference [4] *Platform 6.x Configuration Procedure Reference,* Appendix A Using WinSCP to copy the backup image to the customer system.
		
		The TVOE backup file has now been successfully placed on the Customer System.

15 ☐	**RMS Server iLO:** Repeate Procedure for other RMS Servers	TVOE Configuration of this RMS server is complete. Repeat this procedure from the beginning for other RMSs that need to be configured.

4.13 Install TVOE On Server Blades

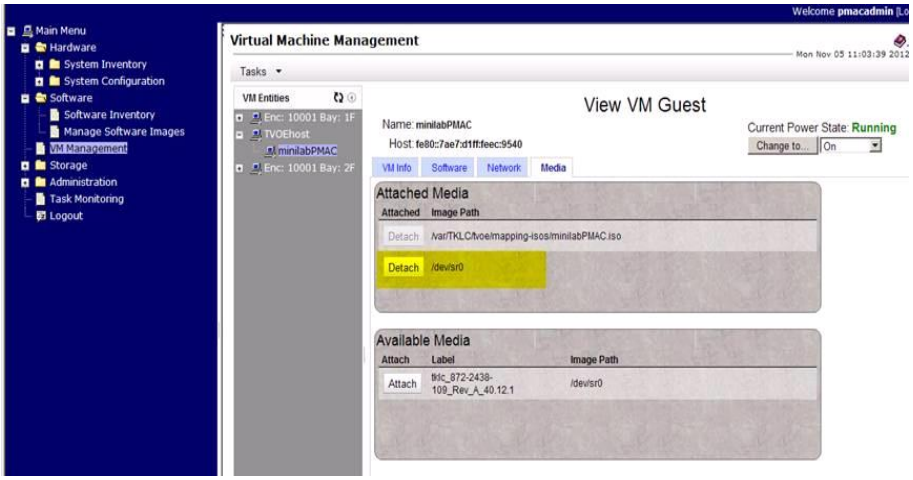
Procedure 24. Install TVOE on Server Blades

S T E P #		
	This procedure will provide the steps to install TVOE on the Blade servers which will host DSR SOAM Applications and if applicable at this site, DSR NOAMP Applications. **NOTE:** TVOE should only be installed on Blade servers that will run either as DSR SOAMs or DSR NOAMPs. They should NOT be installed on Blade servers intended to run as DSR MPs. **Prerequisite**: Enclosures containing the blade servers targeted for IPM that have been configured. **Needed material:** - TVOE Media (64-bits) Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	

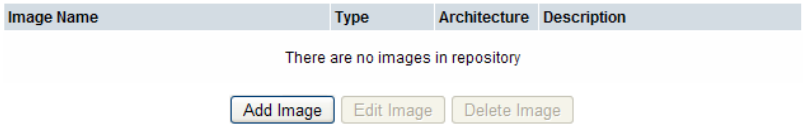
1
☐
	TVOE Host: Load TVOE ISO	If the TVOE ISO has already been loaded on the PM&C server in a previous procedure, skip to step 5, otherwise Add the TVOE ISO image to the PM&C, this can be done in one of three ways:
		
		1. Insert the TVOE 2.0 **64 bit** CD required by the application into the removable media drive.
		2. Attach the USB device containing the ISO image to a USB port.
		3. Copy the TVOE **64 bit** iso file to the management server into the "/var/TKLC/smac/image/isoimages/home/smacftpusr/" directory as pmacftpusr user:
		
		cd into the directory where your ISO image is located on the **TVOE Host** (not on the PM&C server)
		
		Using sftp, connect to the PM&C management server
		
		`# sftp pmacftpusr@<pmac_management_network_ip>`
		`# put <image>.iso`
		
		After the image transfer is 100% complete, close the connection
		`# quit`

2 ☐	**PM&C GUI:** Login	Open web browser and enter: `http://<management_server_ip>` Login as pmacadmin user.

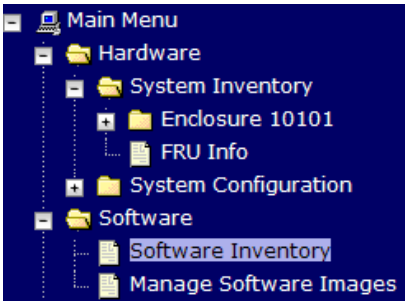
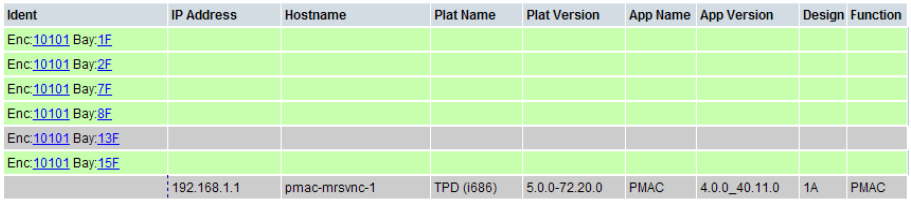
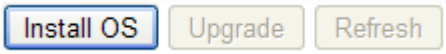
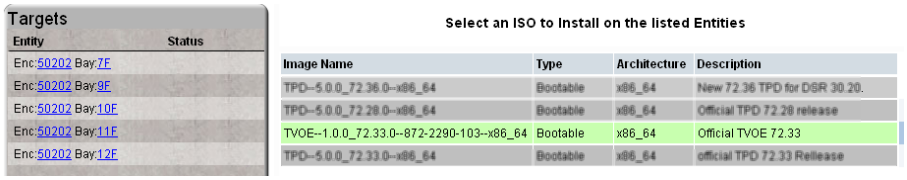
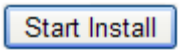
Procedure 24. Install TVOE on Server Blades

3 ☐	**PM&C GUI:** Attach the software Image to the PM&C Guest	If in Step 1 the ISO image was transferred directly to the PM&C guest via sftp, skip the rest of this step and continue with step 4. If the image is on a CD or USB device, continue with this step. In the PM&C GUI, nevigate to **Main Menu ➢ VM Managmenet.**. In the "**VM Entities**" list, select the PM&C guest. On the resulting "**View VM Guest**" page, 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 will appear in the "**Attached Media**" list. 

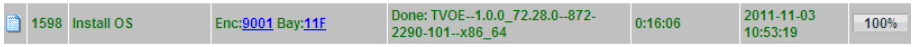
Procedure 24. Install TVOE on Server Blades

4 ☐	**PM&C GUI:** Add TVOE image	Navigate to **Main Menu -> Software -> Manage Software Images** Press **Add Image** button. Use the drop down to select the image.  If the image was supplied on a CD or a USB drive, it will appear as a virtual device ("device://…"). These devices are assigned in numerical order as CD and USB images become available on the Management Server. **The first virtual device is reserved for internal use by TVOE and PM&C; therefore, the iso image of interest is normally present on the second device, "device://dev/sr1" (even though it was mounted as "device://dev/sr0" in the previous step.**. If one or more CD or USB-based images were already present on the Management Server before you started this procedure, choose a correspondingly higher device number. If in Step 1 the image was transferred to PM&C via sftp it will appear in the list as a local file "/var/TKLC/...".  Select the appropriate path and Press **Add New Image** button. You may check the progress using the `Task Monitoring` link. Observe the green bar indicating success. Once the green bar is displayed, remove the TVOE 2.0 Media from the optical drive of the management server.

Procedure 24. Install TVOE on Server Blades

5 ☐	**PM&C GUI:** SelectServers for TVOE install	If you are not logged into the PM&C GUI, Open web browser and enter: http://<pmac_mgmt_ip> and login as pmacadmin user. Otherwise, Navigate to **Software -> Software Inventory**.  Select the servers you want to IPM. If you want to install the same TVOE image to more than one server, you may select multiple servers by clicking multiple rows individually. Selected rows will be highlighted in green.  Click on **Install OS** 
6 ☐	**PM&C GUI:** Initiate OS Install	The left side of this screen shows the servers to be affected by this OS installation. From the list of available bootable images on the right side of the screen, select one OS image to install to all of the selected servers.  Click on **Start Install**, a confirmation window will pop up, click on **Ok** to proceed with the install. 

Procedure 24. Install TVOE on Server Blades

7 ☐	**PM&C GUI:** Monitor OS Install and wait until complete	Navigate to **Main Menu**-> **Task Monitoring** to monitor the progress of the OS Installation background task. A separate task will appear for each blade affected.  When the installation is complete, the task will change to green and the Progress bar will indicate "100%".  Wait until all TVOE OS Installs are 100% complete and the procedure is finished.

Procedure 25. Configure TVOE on Server Blades

S T E P #	This procedure will configure TVOE on the server blades that will host DSR NOAMP VMs. It details the configuration for a single server blade and should be repeated for every TVOE blade that was IPM-ed in the previous procedure. **Prerequisite**: TVOE OS has been installed on the target server blade, and configuration files created. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**PMAC Server:** Exchange SSH keys between PMAC and TVOE server	Use the PMAC GUI to determine the Control Network IP address of TVOE server. From the PMAC GUI, navigate to `Main Menu` → `Software` →`Software Inventory`. Note the IP address TVOE server. From a terminal window connection on the PMAC, exchange SSH keys between the PMAC and the TVOE server using the keyexchange utility, using the Control network IP address for the TVOE blade server. When prompted for the password, enter the password for the TVOE server. # **keyexchange root@<TVOE blade Control Net IP addr>** Note: If the key exchange fails, remove blank lines from "/root/.ssh/known_hosts"
2 ☐	**TVOE Server:** Login and Copy Configuration Scripts from PMAC	Login as root on the TVOE server using the ILO facility. Execute the following commands: # **scp root@<Management_Server Control_IP_ addr>:/usr/TKLC/smac/etc/TVOE* /root/** # **chmod 777 /root/TVOE***

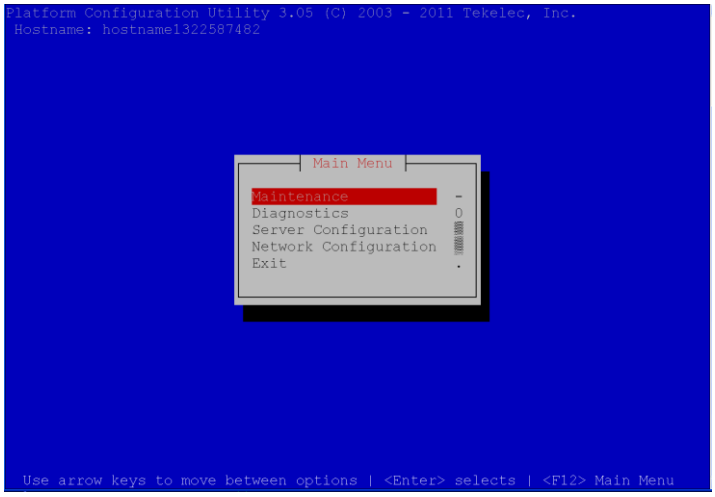
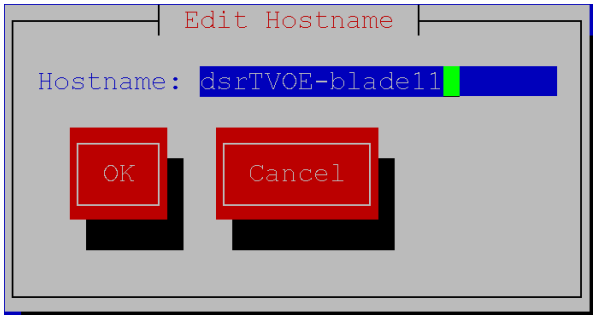
Procedure 25. Configure TVOE on Server Blades

3 ☐	**TVOE Server:** Run Configuration Script Based on Server Blade NIC Configuration	**Next, you will execute ONLY ONE of the following commands. Read carefully to determine which command you should run.**
		
		If your TVOE server blade DOES have mezzanine cards (Typical deployments, applicable in most cases), execute the following command:
		
		`# /root/TVOEcfg.sh --xmivlan=<XMI_VLAN_ID> --imivlan=<IMI_VLAN_ID> mezz`
		
		If your TVOE server blade DOES NOT have mezzanine cards, execute the following command (Very uncommon, applicable only in certain lab deployments):
		
		`# /root/TVOEcfg.sh --xmivlan=<XMI_VLAN_ID> --imivlan=<IMI_VLAN_ID>`
		
		In both cases: *XMI_VLAN_ID* is the VLAN ID for the XMI network in this installation, and *IMI_VLAN_ID* is the VLAN ID for the IMI network in this installation. For deployments with aggregation switches, the IMI and XMI VLAN IDs will be the values of the "INTERNAL-IMI" and "INTERNAL-XMI" vlan ids, respectively. For layer-2 only deployments, the IMI and XMI vlan ids will be obtained from the customer.
		
		Upon executing the proper version of the TVOEcfg.sh script, you should see an output similar to the following (example shows output without the "mezz" parameter):
		
		`Using onboard NICs ...`
		`Interface bond0.3 added`
		`Interface bond0.4 added`
		`Setting up the bridge and unsetting network info`
		`Interface bond0.3 was updated.`
		`Bridge xmi added!`
		`Setting up the bridge and unsetting network info`
		`Interface bond0.4 was updated.`
		`Bridge imi added!`
		
		The prompt will return.
		
		NOTE: If for any reason, you ran the wrong version of the TVOEcfg.sh command, you can execute: `/root/TVOEclean.sh` to reset the networking configuration so you can repeat this step.

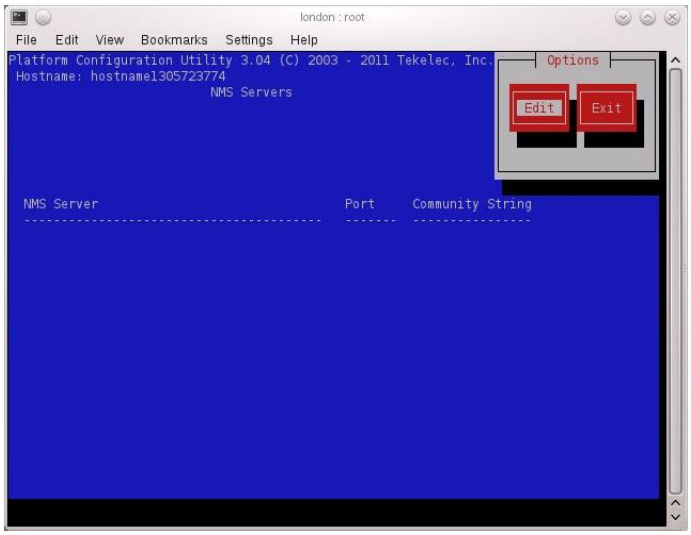
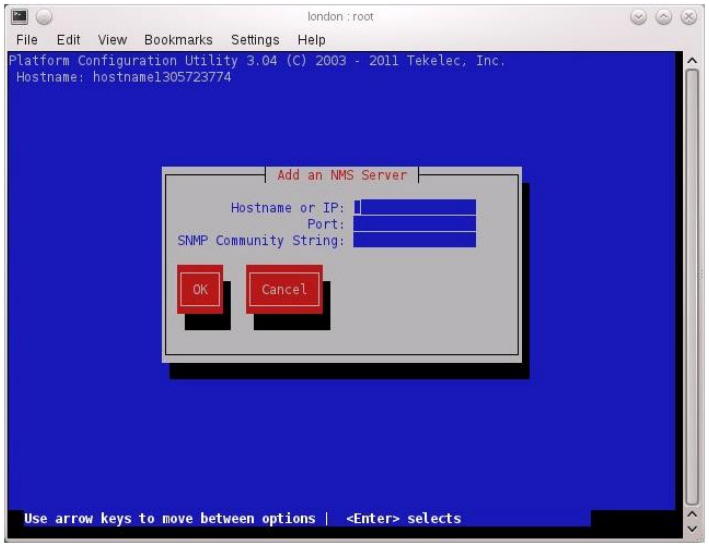
Procedure 25. Configure TVOE on Server Blades

4 ☐	**TVOE Server:** Configure XMI IP and Default Route	**Configure IP address on the XMI network.:** **# netAdm set --type=Bridge --name=xmi --address=<TVOE_XMI_IP_ADDRESS> --netmask=<XMI_NETMASK>** Interface xmi was updated. **Restart network services:** **# service network restart** [wait for the prompt to return] **Set the default route:** **# netAdm add --route=default --device=xmi --gateway=<XMI_NETWORK_GATEWAY>** ERROR: xmi is of type Bridge (Ignore this message) Route to xmi added. **If this installation does not require NetBackup to use a dedicated ethernet interface, then skip the next step and proceed to step 6.**
5 ☐	**(Optional)** **TVOE Server:** Configure NetBackup Dedicated Interface and Bridge	In these examples, <*interface*> should be replaced with the actual ethernet interface that will be used as the dedicated NetBackup port. For instance, "eth01", or "eth22". **Unbond Ethernet Interface:** **# netAdm set --device=<interface> --slave=no --onboot=yes** **[OPTIONAL] If this installation is using jumbo frames, set the ethernet interface MTU to the desired jumbo frame size:** **# netAdm set --device=<interface> --MTU=<NetBackup_MTU_size>** **Create NetBackup VM Bridge Interface:** **# netAdm add --type=Bridge --name=netbackup --bridgeInterfaces=<interface> --onboot=yes**

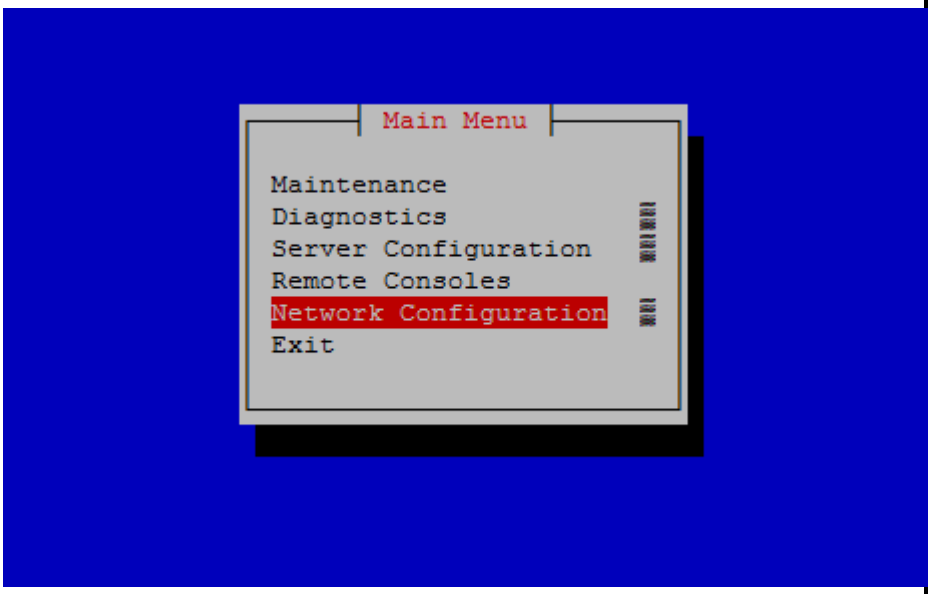
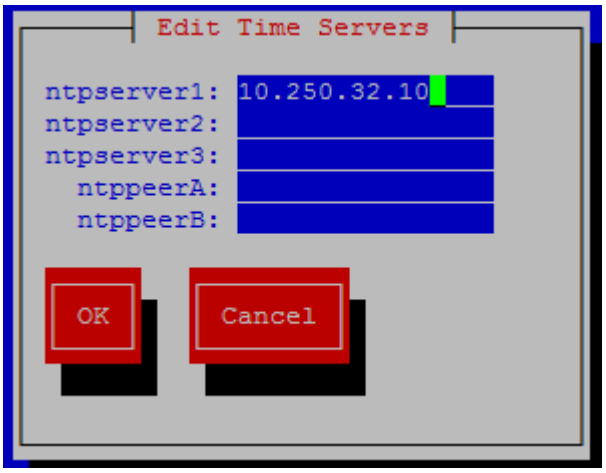
Procedure 25. Configure TVOE on Server Blades

6 ☐	**TVOE Server:** Set Hostname	# **su - platcfg**  Navigate to **Sever Configuration->Hostname-> Edit** and enter a new hostname for your server.  Press **OK** and select and continue to press **Exit** until you are at the platcfg main menu again. Continue To Press **Exit** until you are back at the platcfg main menu **NOTE:** Although the new hostname has been properly configured and committed at this point, it will not appear on your command prompt unless you log out and log back in again

Procedure 25. Configure TVOE on Server Blades

7 ☐	**TVOE server:** Configure SNMP	From the platcfg main menu, navigate to **Network Configuration -> SNMP Configuration -> NMS Configuration**  Press **Edit.** Choose **Add a New NMS Server**  Enter the *Hostname/IP* of the NO VIP, for *port* enter 162, and for *Community String* enter the value provided by the customer in the NAPD document. Press **Exit.** Select **Yes** when prompted to restart the Alarm Routing Service. Optionally, add any customer provided NMS Servers by repeating the step above. Once Done, press **Exit** to quit to the platcfg main menu.

Procedure 25. Configure TVOE on Server Blades

8 ☐	**TVOE server:** Configure NTP	Navigate to Network Configuration  Navigate to **Configuration->NTP** Click **Edit**  Enter the customer provided NTP server IP address(es) Press **OK** Continue to press Exit until you are out of the platcfg menu.
9 ☐	**TVOE server:** Repeate Procedure for other TVOE blades.	**Configuration of this TVOE server blade is complete. Repeat this procedure from the beginning for other TVOE hosts that need to be configured.**

4.14 Create Virtual Machines for Applications

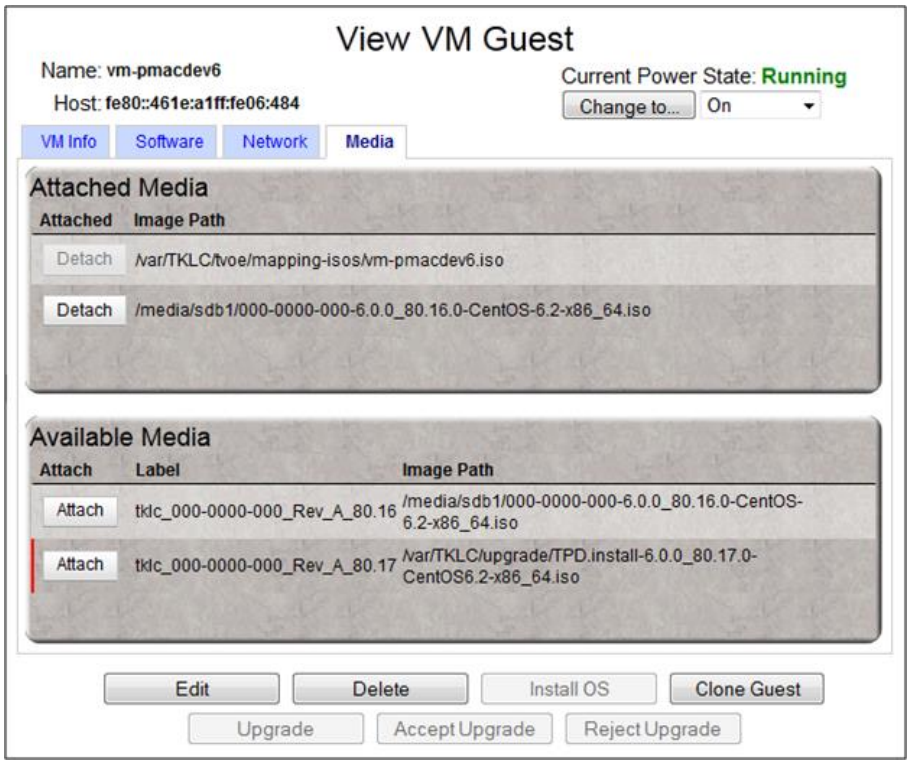
Procedure 26. Load Application ISO onto PM&C Server

S T E P #	This procedure will load the DSR Application ISO into the PM&C Server **Needed material:** - 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 TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	

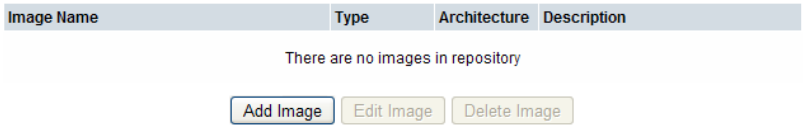
1
☐
	TVOE Host: Load Application ISO	Add the Application ISO image to the PM&C, this can be done in one of three ways:
		1. Insert the Application CD required by the application into the removable media drive.
		2. Attach the USB device containing the ISO image to a USB port.
		3. Copy the Application iso file to the management server into the "/var/TKLC/smac/image/isoimages/home/smacftpusr/" directory as pmacftpusr user:
		
		cd into the directory where your ISO image is located on the **TVOE Host** (not on the PM&C server)
		
		Using sftp, connect to the PM&C management server
		
		`# sftp pmacftpusr@<pmac_management_network_ip>`
		`# put <image>.iso`
		
		After the image transfer is 100% complete, close the connection
		`# quit`

2 ☐	**PM&C GUI:** Login	Open web browser and enter: `http://<management_server_ip>` Login as pmacadmin user.

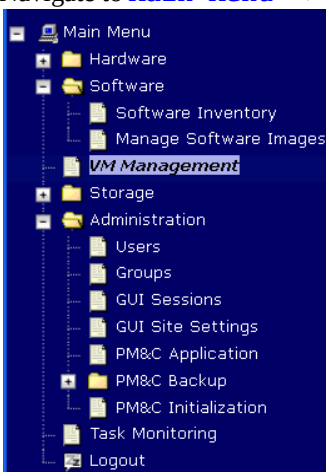
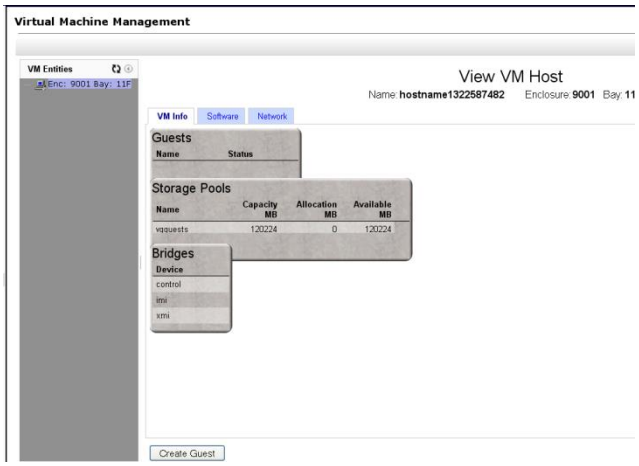
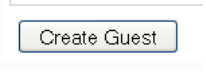
Procedure 26. Load Application ISO onto PM&C Server

3 ☐	**PM&C GUI:** Attach the software Image to the PM&C Guest	If in Step 1 the ISO image was transferred directly to the PM&C guest via sftp, skip the rest of this step and continue with step 4. If the image is on a CD or USB device, continue with this step. In the PM&C GUI, nevigate to **Main Menu ➢ VM Managmenet.**. In the "**VM Entities**" list, select the PM&C guest. On the resulting "**View VM Guest**" page, 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 will appear in the "**Attached Media**" list. 

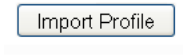
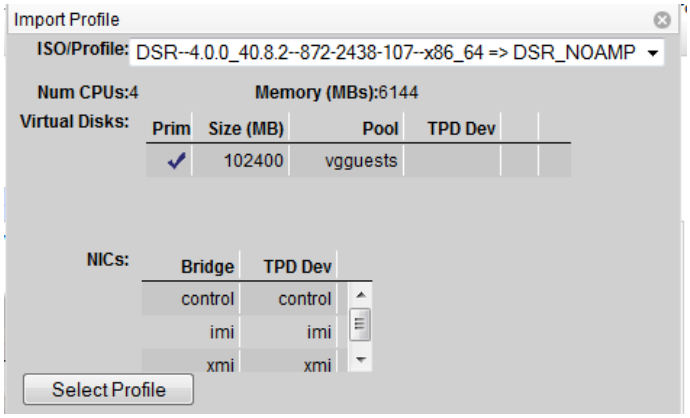
Procedure 26. Load Application ISO onto PM&C Server

4 ☐	**PM&C GUI:** Add Application image	Navigate to **Main Menu -> Software -> Manage Software Images** Press **Add Image** button. Use the drop down to select the image.  If the image was supplied on a CD or a USB drive, it will appear as a virtual device ("device://…"). These devices are assigned in numerical order as CD and USB images become available on the Management Server. The first virtual device is reserved for internal use by TVOE and PM&C; therefore, the iso image of interest is normally present on the second device, "device://dev/sr1". If one or more CD or USB-based images were already present on the Management Server before you started this procedure, choose a correspondingly higher device number. If in Step 1 the image was transferred to PM&C via sftp it will appear in the list as a local file "/var/TKLC/...".  Select the appropriate path and Press **Add New Image** button. You may check the progress using the `Task Monitoring` link. Observe the green bar indicating success. Once the green bar is displayed, remove the TVOE 2.0 Media from the optical drive of the management server.

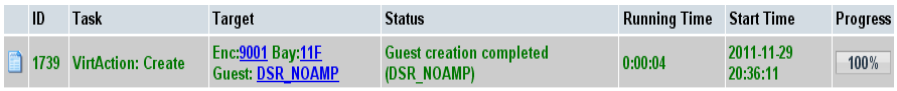
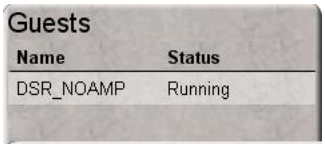
Procedure 27. Create NOAMP Guest VMs

STEP #		
	This procedure will provide the steps needed to create a DSR NOAMP virtual machine (refered to as a "guest") on a TVOE server blade or TVOE RMS. It must be repeated for every NOAMP server you wish to install. **Prerequisite**: TVOE has been installed and configured on the target blade server or RMS Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**PM&C GUI:** Login	Open web browser and enter: **`http://<management_server_ip>`** Login as pmacadmin user.
2 ☐	**PM&C GUI:** Navigate to VM Management of the Target Server Blade	Navigate to **`Main Menu -> VM Management`**  Select the TVOE server blade or rack mounted server from the "VM Entities" listing on the left side of the screen. The selected server's guest machine configuration will then be displayed in the remaining area of the window.   Click **`Create Guest`**

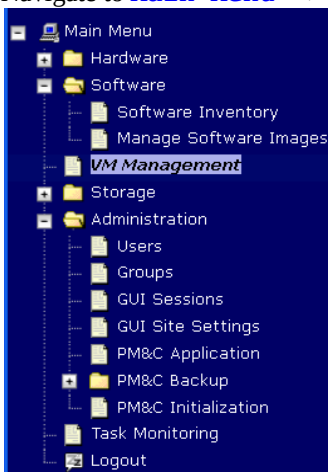
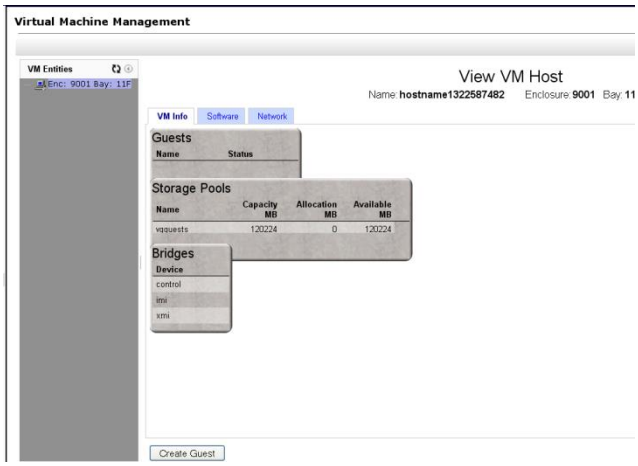
Procedure 27. Create NOAMP Guest VMs

3 ☐	**PM&C GUI:** Configure VM Guest Parameters	Press **Import Profile**   From the "ISO/Profile" drop-down box, select the entry that matches: • <Application ISO NAME>➔DSR_NOAMP - If your NOAMP **DOES NOT** require a dedicated ethernet port for NetBackup • <Application ISO NAME>➔DSR_NOAMP_NBD - If your NOAMP **DOES** require a dedicated ethernet port for NetBackup Where Application_ISO_NAME is the name of the DSR Appilcation ISO to be installed on this NOAMP. Press **Select Profile**. Values from the profile should now populate the VM configuration screen Disk Size, Number of CPUs, Memory, and NICs: should all change fom their default values to the profile values You can edit the name, if you wish. For instance: "DSR_NOAMP-A," or DSRNOAMP-B". (**This will not become the ultimate hostname. It is just an internal tag for the VM host manager.)** Press **Create** 

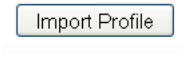
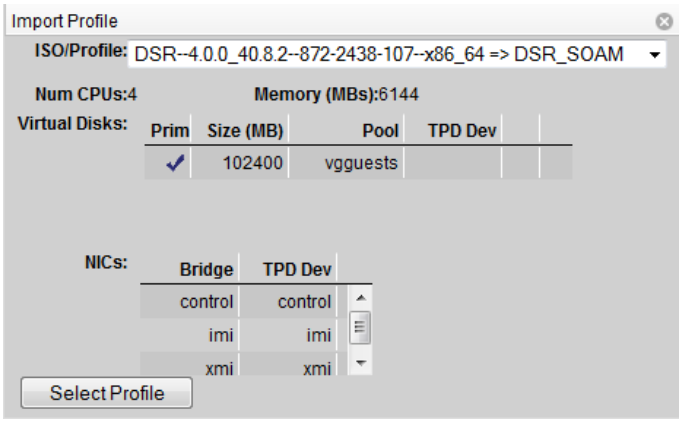
Procedure 27. Create NOAMP Guest VMs

4 ☐	**PM&C GUI:** Wait for Guest Creation to Complete	Navigate to **Main Menu** > **Task Monitoring** to monitor the progress of the guest creation task.. A separate task will appear for each guest creation that you have launched. Wait or referesh the screen until you see that the guest creation task has completed successfully. 
5 ☐	**PM&C GUI:** Verify Guest Machine is Running	Navigate to **Main Menu -> VM Management** Select the TVOE server blade on which the guest machine was just created. Look at the list of guests present on the blade and verify that you see a guest that mataches the name you configured and that its status is “Running”.  **VM Creation for this guest is complete. Repeat from Step 2 for any remaining NOAMP VMs (for instance, the standby NOAMP) that must be created.**

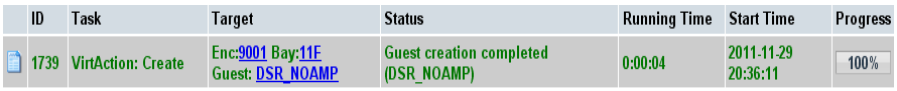
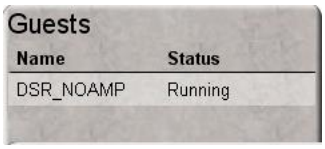
Procedure 28. Create SOAMP Guest VMs

S T E P #		
	This procedure will provide the steps needed to create a DSR SOAMP virtual machine (refered to as a "guest") on a TVOE server blade. It must be repeated for every SOAMP server you wish to install. **Prerequisite**: TVOE has been installed and configured on the target blade 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 TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**PM&C GUI:** Login	Open web browser and enter: **`http://<management_server_ip>`** Login as pmacadmin user.
2 ☐	**PM&C GUI:** Navigate to VM Management of the Target Server Blade	Navigate to **`Main Menu -> VM Management`**  Select the TVOE server blade from the "VM Entities" listing on the left side of the screen. This blade's guest machine configuration will then be displayed in the remaining area of the window.   Click **`Create Guest`**

Procedure 28. Create SOAMP Guest VMs

3 ☐	**PM&C GUI:** Configure VM Guest Parameters	Press **Import Profile**   From the "ISO/Profile" drop-down box, select the entry that matches <Application ISO NAME>➔DSR_SOAM Where Application_ISO_NAME is the name of the DSR Appilcation ISO to be installed on this SOAMP. Press **Select Profile**. Values from the profile should now populate the VM configuration screen Disk Size, Number of CPUs, Memory, and NICs: should all change fom their default values to the profile values You can edit the name, if you wish. For instance: "DSR_SOAM_A," or DSR_SOAM_B". (**This will not become the ultimate hostname. It is just an internal tag for the VM host manager.)** Press **Create** 

Procedure 28. Create SOAMP Guest VMs

4 ☐	**PM&C GUI:** Wait for Guest Creation to Complete	Navigate to **Main Menu** > **Task Monitoring** to monitor the progress of the guest creation task.. A separate task will appear for each guest creation that you have launched. Wait or referesh the screen until you see that the guest creation task has completed successfully. 
5 ☐	**PM&C GUI:** Verify Guest Machine is Running	Navigate to **Main Menu -> VM Management** Select the TVOE server blade on which the guest machine was just created. Look at the list of guests present on the blade and verify that you see a guest that mataches the name you configured and that its status is “Running”.  **VM Creation for this guest is complete. Repeat from Step 2 for any remaining SOAMP VMs (for instance, the standby SOAMP) that must be created.**

4.15 Install Application Software on Servers

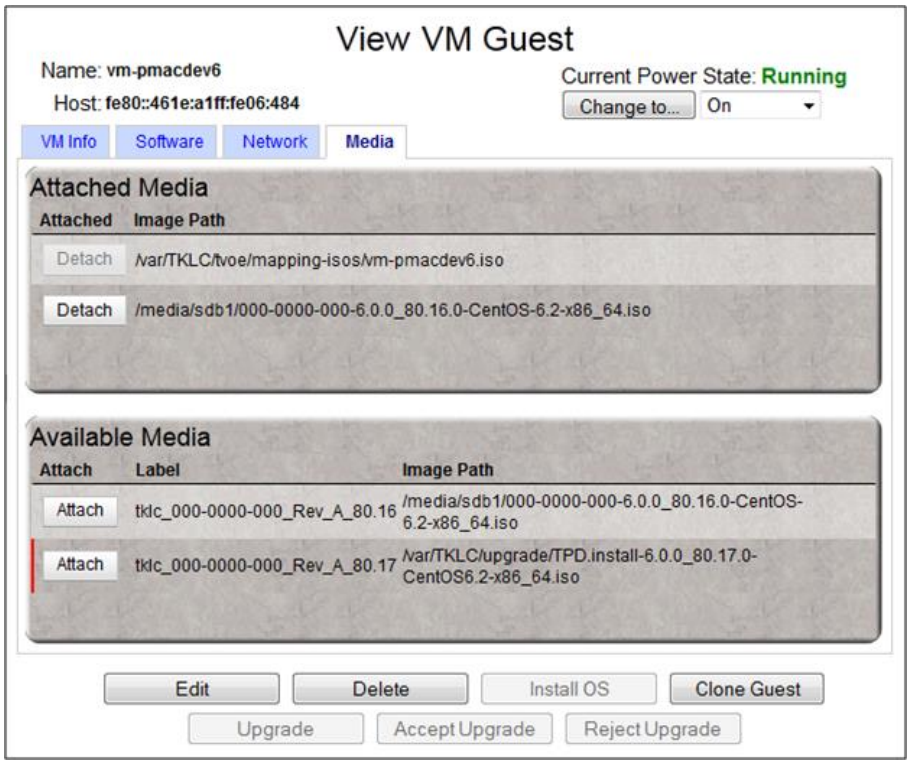
Procedure 29. IPM Blades and VMs

S T E P #	This procedure will provide the steps to install TPD on Blade servers and Blade server guest VMs **Prerequisite**: Enclosures containing the blade servers targeted for IPM that have been configured. **Prerequisite**: TVOE has been installed and configured on Blade servers that will host DSR NOAMP VMs. **Prerequisite**: DSR NOAMP and SOAM Guest VMs have been created successfully. **Needed material:** - TPD Media (64-bits) Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	

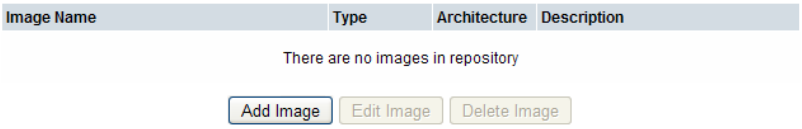
1 ☐	**TVOE Host:** Load Application ISO	Add the TPD ISO image to the PM&C, this can be done in one of three ways:
		1. Insert the TPD CD required by the application into the removable media drive.
		2. Attach the USB device containing the ISO image to a USB port.
		3. Copy the TPD iso file to the management server into the "/var/TKLC/smac/image/isoimages/home/smacftpusr/" directory as pmacftpusr user:
		
		cd into the directory where your ISO image is located on the **TVOE Host** (not on the PM&C server)
		
		Using sftp, connect to the PM&C management server
		
		`# sftp pmacftpusr@<pmac_management_network_ip>`
		`# put <image>.iso`
		
		After the image transfer is 100% complete, close the connection
		`# quit`

2 ☐	**PM&C GUI:** Login	Open web browser and enter: `http://<management_server_ip>` Login as pmacadmin user.

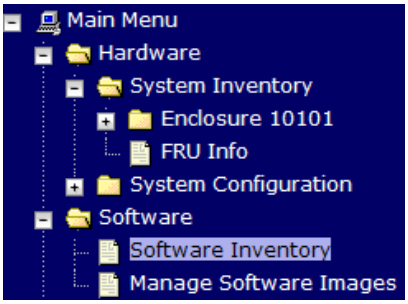
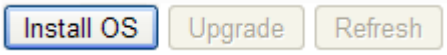
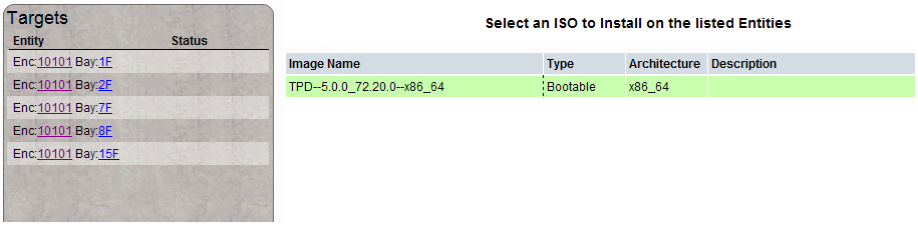
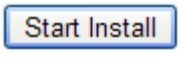
Procedure 29. IPM Blades and VMs

3 ☐	**PM&C GUI:** Attach the software Image to the PM&C Guest	If in Step 1 the ISO image was transferred directly to the PM&C guest via sftp, skip the rest of this step and continue with step 4. If the image is on a CD or USB device, continue with this step. In the PM&C GUI, nevigate to **Main Menu ➢ VM Managmenet.**. In the "**VM Entities**" list, select the PM&C guest. On the resulting "**View VM Guest**" page, 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 will appear in the "**Attached Media**" list. 

Procedure 29. IPM Blades and VMs

4 ☐	**PM&C GUI:** Add Application image	Navigate to **Main Menu -> Software -> Manage Software Images** Press **Add Image** button. Use the drop down to select the image.  If the image was supplied on a CD or a USB drive, it will appear as a virtual device ("device://…"). These devices are assigned in numerical order as CD and USB images become available on the Management Server. The first virtual device is reserved for internal use by TVOE and PM&C; therefore, the iso image of interest is normally present on the second device, "device://dev/sr1". If one or more CD or USB-based images were already present on the Management Server before you started this procedure, choose a correspondingly higher device number. If in Step 4 the image was transferred to PM&C via sftp it will appear in the list as a local file "/var/TKLC/...".  Select the appropriate path and Press **Add New Image** button. You may check the progress using the `Task Monitoring` link. Observe the green bar indicating success. Once the green bar is displayed, remove the TVOE 2.0 Media from the optical drive of the management server.

Procedure 29. IPM Blades and VMs

5 ☐	**PM&C GUI:** Select Servers for OS install	Navigate to **Software -> Software Inventory**.  Select the servers you want to IPM. If you want to install the same OS image to more than one server, you may select multiple servers by clicking multiple rows individually. Selected rows will be highlighted in green. Note: VM's will have the text "Guest: <VM_GUEST_NAME>" underneath the physical blade or RMS that hosts them. Ident / IP Address / Hostname / Plat Name / Plat Version / App Name / App Version / Design / Function Enc:10101 Bay:1F Enc:10101 Bay:2F Enc:10101 Bay:7F Enc:10101 Bay:8F Enc:10101 Bay:13F Enc:10101 Bay:15F 192.168.1.1 / pmac-mrsvnc-1 / TPD (i686) / 5.0.0-72.20.0 / PMAC / 4.0.0_40.11.0 / 1A / PMAC Click on **Install OS** 
6 ☐	**PM&C GUI:** Initiate OS Install	The left side of this screen shows the servers to be affected by this OS installation. From the list of available bootable images on the right side of the screen, select one OS image to install to all of the selected servers.  Click on **Start Install**, a confirmation window will pop up, click on **Ok** to proceed with the install. 

Procedure 29. IPM Blades and VMs

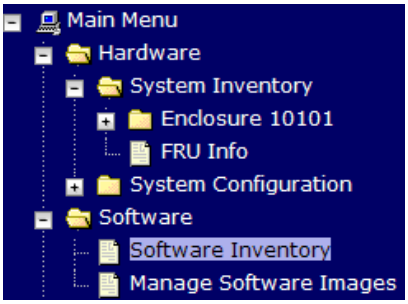
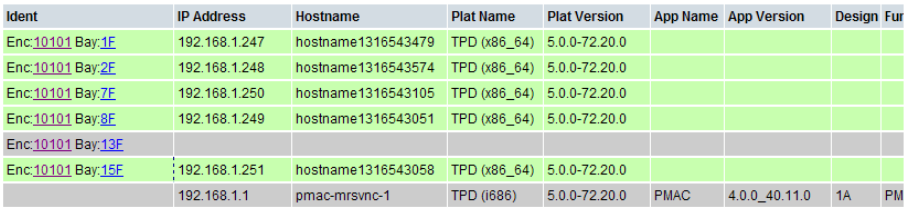
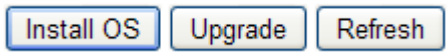
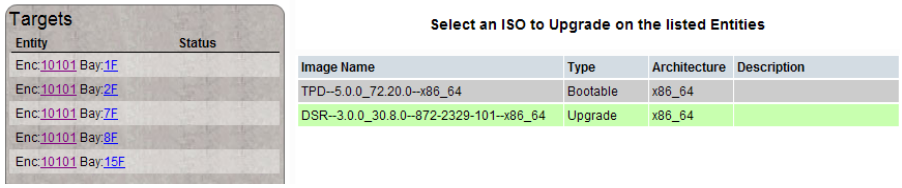
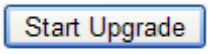
7 ☐	**PM&C GUI:** Monitor OS Install	Navigate to **Main Menu** > **Task Monitoring** to monitor the progress of the OS Installation background task. A separate task will appear for each blade affected.  When the installation is complete, the task will change to green and the Progress bar will indicate "100%".

	ID	Task	Target	Status	Running Time	Start Time	Progress
	14	Install OS	Enc:10101 Bay:15F	Boot install image	0:00:01	2011-09-20 11:12:02	50%
	13	Install OS	Enc:10101 Bay:8F	Boot install image	0:00:01	2011-09-20 11:12:02	50%
	12	Install OS	Enc:10101 Bay:7F	Boot install image	0:00:01	2011-09-20 11:12:02	50%
	11	Install OS	Enc:10101 Bay:2F	Boot install image	0:00:01	2011-09-20 11:12:02	50%
	10	Install OS	Enc:10101 Bay:1F	Boot install image	0:00:02	2011-09-20 11:12:01	50%
	9	Add Image		Done: TPD.install-5.0.0_72.20.0-CentOS5.6-x86_64	0:00:09	2011-09-20 11:01:50	100%

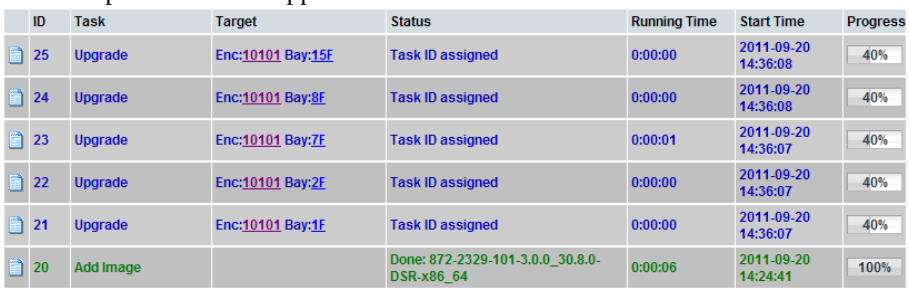
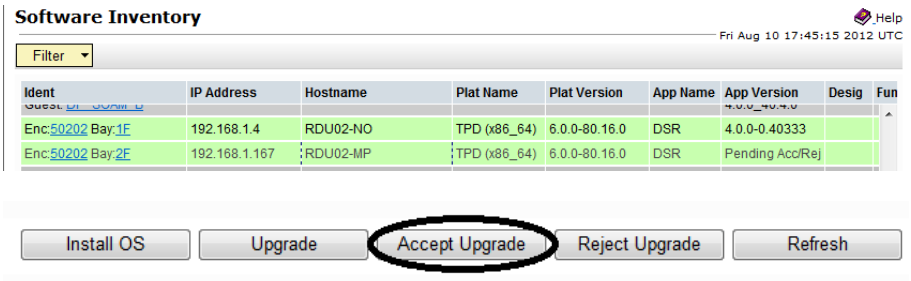
Procedure 30. Install the Application Software on Blades

S T E P #	This procedure will provide the steps to install Diameter Signaling Router 4.X on the Blade servers. **Prerequisite**: *Procedure 29. IPM Blades* has been completed. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**PM&C GUI:** Login	Open web browser and enter: **http://<management_network_ip>** Login as pmacadmin user.

Procedure 30. Install the Application Software on Blades

2 ☐	**PM&C GUI:** Select Servers for Application install	Navigate to **Software -> Software Inventory**.  Select the servers on which the application is to be installed. If you want to install the same application image to more than one server, you may select multiple servers by clicking multiple rows individually. Selected rows will be highlighted in green. Note: VM's will have the text "Guest: <VM_GUEST_NAME>" underneath the physical blade that hosts them.  Click on **Upgrade** 
3 ☐	**PM&C GUI:** Initiate Application Install	The left side of this screen shows the servers to be affected by this OS installation. From the list of available bootable images on the right side of the screen, select one OS image to install to all of the selected servers.  Click on **Start Upgrade**, a confirmation window will pop up, click on **Ok** to proceed with the install. 

Procedure 30. Install the Application Software on Blades

4 ☐	**PM&C GUI:** Monitor the installation status	Navigate to **Main Menu** > **Task Monitoring** to monitor the progress of the Application Installation. task. A separate task will appear for each blade affected.  When the installation is complete, the task will change to green and the Progress bar will indicate "100%".
5 ☐	**PM&C GUI:** Accpet Upgrade	Navigate to **Software** > **Software Inventory** to accept the software installation. Select all the servers on which the application has been installed in the previous steps and click on "**Accept Upgrade**" as shown below. Note that on some RMS and Blade servers, the GUI may not provide the option to accept/reject upgrade. So first verify in task monitoring that the upgrade is not in progress, then manually accept or reject the upgrade by ssh'ing into the server and execute: 1. To accept: */var/TKLC/backout/accept* 2. To reject: */var/TKLC/backout/reject*  Note that once the upgrade has been accepted, the App version will change from "Pending Acc/Rej" to the version number of the application.

4.16 Application Configuration

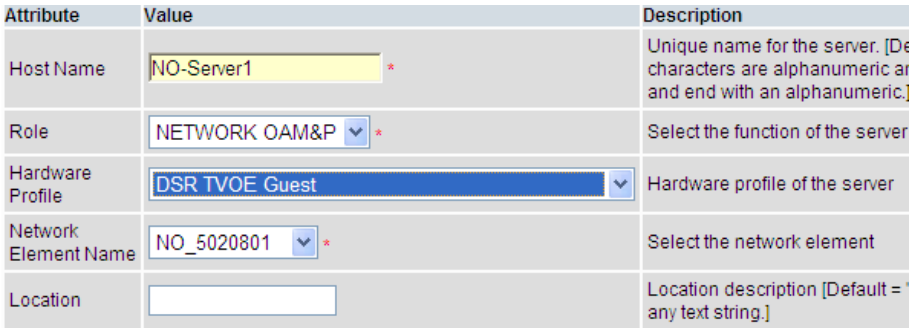
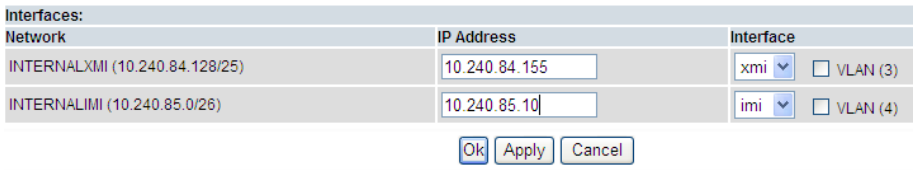
Procedure 31. Configure the First NOAMP NE and Server

S T E P	This procedure will provide the steps to configure the First NOAMP blade 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 TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**Save the NOAMP Network Data to an XML file**	Using a text editor, create a NOAMP Network Element file that describes the networking of the target install environment of your first NOAMP server. Select an appropriate file name and save the file to a known location on your computer. A suggested filename format is "Appname_NEname_NetworkElement.XML", so for example an DSR2 NOAMP network element XML file would have a filename "DSR2_NOAMP_NetworkElement.xml". Alternatively, you can update the sample DSR 4.0 Network Element file be found on the management server at: **`/usr/TKLC/smac/etc/SAMPLE-NetworkElement.xml`** A sample XML file can also be found in Appendix A. Note that the following limitations apply when specifying a Network Element name: "A 1-32-character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit".
2 ☐	**Exchange SSH keys between PMAC and first NOAMP server**	Use the PMAC GUI to determine the Control Network IP address of the blade server that is to be the first NOAMP server. From the PMAC GUI, navigate to **`Main Menu → Software →Software Inventory`**. Note the IP address for the first NOAMP server. From a terminal window connection on the PMAC, exchange SSH keys between the PMAC and the 1st NOAMP blade server using the keyexchange utility, using the Control network IP address for the NOAMP blade server. When prompted for the password, enter the password for the NOAMP server. # **`keyexchange root@<NOAMP blade Control Net IP addr>`** Note: if keyexchange fails, edit "/root/.ssh/known_hosts" and remove blank lines, and retry the keyexchange commands.
3 ☐	**Connect a Web Browser to the NOAMP GUI**	Plug a laptop ethernet cable onto an unused, unconfigured port on the 4948 switch (if available in your installation) or use SSH Tunneling through the PMAC to connect the laptop to the NOAMP server blade. **If you are using tunneling, then you can skip the rest of this step and instead complete the instructions in 4.18Appendix G. (for using Putty) or 4.18Appendix H (for using OpenSSH). Openssh is recommended if you are using a Windows 7 PC.** From the PMAC, enable the switch port that the laptop is plugged into. Enable that laptop Ethernet port to acquire a DHCP address and then access the NOAMP-"A" GUI via its control IP address.
4 ☐	**NOAMP GUI:** Login	Login to the NOAMP GUI as the guiadmin user.

Procedure 31. Configure the First NOAMP NE and Server

5 ☐	**Create the NOAMP Network Element using the XML File**	Navigate to **Main Menu->Configuration->Network Elements** Select the "Browse" button, and enter the pathname of the NOAMP network XML file. Select the "Upload File" button to upload the XML file and configure the NOAMP Network Element. Once the data has been uploaded, you should see a folder appear with the name of your network element. Click on this folder and you will get a drop-down which describes the individual networks that are now configured: Network Element: NO_9006005 Network Name / Network Address / Netmask / VLAN ID / Gateway IP Address INTERNALXMI / 10.240.10.32 / 255.255.255.224 / 3 / 10.240.10.35 INTERNALIMI / 10.240.10.0 / 255.255.255.224 / 4 / 10.240.10.3
6 ☐	**Map Services to Networks**	Navigate to **Main Menu → Configuration → Services**. Select the "Edit" button and set the Services as shown in the table below: **Name** / **Intra-NE Network** / **Inter-NE Network** OAM / *<IMI Network>* / *<XMI Network>* Replication / *<IMI Network>* / *<XMI Network>* Signaling / Unspecified / Unspecified HA_Secondary / Unspecified / Unspecified HA_MP_Secondary / Unspecified / Unspecified Replication_MP / *<IMI Network>* / Unspecified ComAgent / *<IMI Network>* / Unspecified For example, if your IMI network is named "IMI" and your XMI network is named "XMI", then your services should config should look like the following: Name / Intra-NE Network / Inter-NE Network OAM / IMI / XMI Replication / IMI / XMI Signaling / Unspecified / Unspecified HA_Secondary / Unspecified / Unspecified HA_MP_Secondary / Unspecified / Unspecified Replication_MP / IMI / Unspecified ComAgent / IMI / Unspecified Select the "Ok" button to apply the Service-to-Network selections.

Procedure 31. Configure the First NOAMP NE and Server

7 ☐	**Insert the 1st NOAMP server**	Navigate to **Main Menu → Configuration → Servers**. Select the "Insert" button to insert the new NOAMP server into servers table (the first or "A" server).  Fill in the fields as follows: **Hostname:** **<Hostname>** **Role:** **NETWORK OAM&P** **Hardware Profile:** **DSR TVOE Guest** **Network Element Name:** **[Choose NE from Drop Down Box]** The network interface fields will now become available with selection choices based on the chosen hardware profile and network element  Fill in the server IP addresses for the XMI network. Select "xmi" for the interface. **Leave the "VLAN" checkbox unchecked**. Fill in the server IP addresses for the IMI network. Select "imi" for the interface. **Leave the "VLAN" checkbox unchecked**. For **DSR 4.1.X installations ONLY:** add the following NTP servers: | NTP Server | Preferred? | | ***<NO1-TVOE-XMI-IP-Address>*** | Yes | Select the "Ok" button when you have completed entering the server data.
8 ☐	**Export the Initial Configuration**	Navigate to **Main Menu → Configuration → Servers.** From the GUI screen, select the NOAMP server and then select "Export" action button to generate the initial configuration data for that server.

Procedure 31. Configure the First NOAMP NE and Server

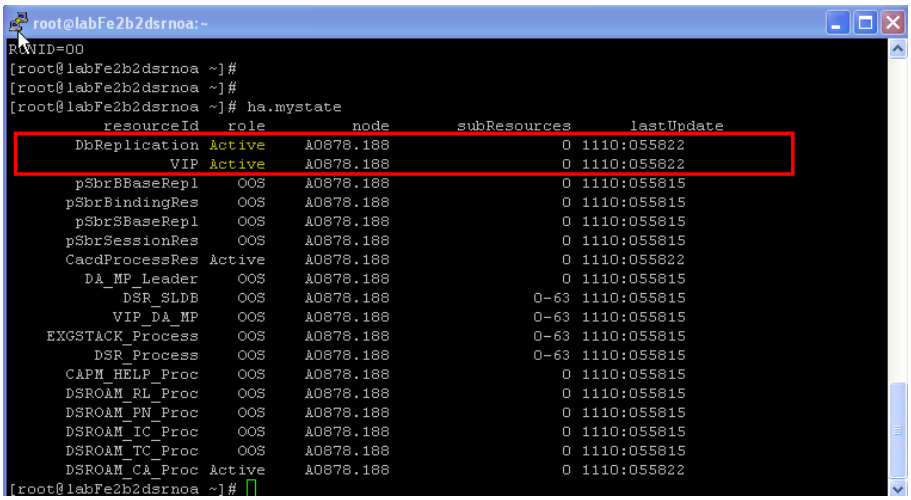
9 ☐	**Copy Configuration File to 1st NOAMP Server**	From a terminal window connection on the 1st NOAMP VM (see 4.18Appendix F for instructions on how to access the NOAMP from iLO) , copy the configuration file created in the previous step from the `/var/TKLC/db/filemgmt` directory on the 1st NOAMP to the /var/tmp directory. The configuration file will have a filename like `TKLCConfigData.<hostname>.sh`. The following is an example: `# cp /var/TKLC/db/filemgmt/TKLCConfigData.blade01.sh /var/tmp/TKLCConfigData.sh`
10 ☐	**Wait for Configuration to Complete**	The automatic configuration daemon will look for the file named "TKLCConfigData.sh" in the /var/tmp directory, implement the configuration in the file, and then prompt the user to reboot the server. Wait to be prompted to reboot the server, but **DO NOT** reboot the server, it will be rebooted later on in this procedure. **NOTE**: Ignore the warning about removing the USB key, since no USB key is present. .
11 ☐	**Configure Time Zone**	From the command line prompt, execute *set_ini_tz.pl*. This will set the system time zone The following command example uses the America/New_York time zone. Replace as appropriate with the time zone you have selected for this installation. For UTC, use "Etc/UTC", for a full list of valid timezones, see 4.18Appendix K. `# /usr/TKLC/appworks/bin/set_ini_tz.pl "Etc/UTC" >/dev/null 2>&1`
12 ☐	**Reboot the Server**	`# init 6`

13 ☐	**(Optional) Configure Networking for Dedicated NetBackup Interface**	**NOTE: You will only execute this step if your NO is using a dedicated Ethernet interface for NetBackup.**
		
		From a root login session on the first NO, execute the following commands:
		`# netAdm set --device=netbackup --type=Ethernet --onboot=yes --address=<NO1_NetBackup_IP> --netmask=<NetBackup_NetMask>`
		
		`# netAdm add --route=net --device=netbackup --address=<NetBackup_Network_ID> --netmask=<NetBackup_Network_NetMask> --gateway=<NetBackup_Network_Gateway_IP>`

Procedure 32. Configure the NOAMP Server Group

S T E P	This procedure will provide the steps to configure the NOAMP server group. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**NOAMP GUI:** Login	Establish a GUI session on the first NOAMP server by using the XMI IP address of the first NOAMP server. Open the web browser and enter a URL of: `http://<first noamp XMI IP address>` Login as the guiadmin user. If prompted by a security warming, select "Continue to this Website" to proceed.
2 ☐	**Enter NOAMP Server Group Data**	Using the GUI session on the first NOAMP server, go to the GUI **Main Menu→Configuration→Server Groups**, select Insert and fill the following fields: • Server Group Name → **[Enter Server Group Name]** • Level → **A** • Parent : **None** • Function: **DSR (Active/Standby Pair)** Select "OK" when all fields are filled in.
3 ☐	**Edit the NOAMP Server Group**	From the GUI Main Menu→Configuration→Server Groups, select the new server group, and then select "Edit". Select the Network Element that represents the NOAMP. NO_900060103 Server | SG Inclusion | Preferred HA Role HPC6NO | ☑ Include in SG | ☐ Preferred Spare In the portion of the screen that lists the servers for the server group, find the NOAMP server being configured. Click the "Include in SG" checkbox. Leave other boxes blank. Press OK

Procedure 32. Configure the NOAMP Server Group

4 ☐	**Verify NOAMP blade server role**	From terminal window to the iLO of the first NOAMP blade server, execute the **`ha.mystate`** command to verify that the "DbReplication" and VIP item under the "resourceId" column has a value of "Active" under the "role" column. You might have to wait a few minutes for it to become in that state. Press Ctrl+C to exit Example: 
5 ☐	**Restart 1st NOAMP blade server**	From the NOAMP GUI, select the **Main menu→Status & Manage→Server** menu. Select the first NOAMP server. Select the **`Restart`** button. Answer OK to the confirmation popup. Wait for restart to complete.

Procedure 33. Configure the Second NOAMP Server

<table>
<tr><th>S
T
E
P</th><td colspan="2">This procedure will provide the steps to configure the Second NOAMP 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 TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.</td></tr>
<tr><td>1
☐</td><td>Exchange SSH keys between PMAC and second NOAMP server</td><td>Use the PMAC GUI to determine the Control Network IP address of the blade server that is to be the second NOAMP server. From the PMAC GUI, navigate to Main Menu → Software-→Software Inventory. Note the IP address for the second NOAMP server, usually the second blade in the first enclosure.

From a terminal window connection on the PMAC, exchange SSH keys between the PMAC and the second NOAMP blade server using the keyexchange utility, using the Control network IP address for the NOAMP blade server. When prompted for the password, enter the password for the NOAMP server.

keyexchange root@<NOAMP blade Control Net IP addr></td></tr>
<tr><td>2
☐</td><td>NOAMP GUI:
Login</td><td>If not already done, establish a GUI session on the first NOAMP server by using the XMI IP address of the first NOAMP server. Open the web browser and enter a URL of: http://<first noamp XMI IP address>

Login as the guiadmin user.</td></tr>
<tr><td>3
☐</td><td>Insert the 2nd NOAMP server</td><td>Navigate to Main Menu → Configuration → Servers.

Click on Insert to insert the new second NOAMP server into servers table (“B” server).
This server role should be the “NETWORK OAM&P”.
Select the Network Element Name (should be the same used when configuring the first NOAMP).
Choose "DSR TVOE Guest" for the hardware profile.

Fill in the server IP addresses for the XMI network. Select "xmi" for the interface. Leave the "VLAN" checkbox unchecked.

Fill in the server IP addresses for the IMI network. Select "imi" for the interface. Leave the "VLAN" checkbox unchecked.

For DSR 4.1.X installations ONLY: add the following NTP servers:

<table><tr><th>NTP Server</th><th>Preferred?</th></tr><tr><td><NO2-TVOE-XMI-IP-Address></td><td>Yes</td></tr></table>
Select the Ok button when you have completed entering the server data.</td></tr>
<tr><td>4
☐</td><td>Export the initial configuration</td><td>From the GUI screen, select the second server and then select Export action button to generate the initial configuration data for that server.</td></tr>
</table>

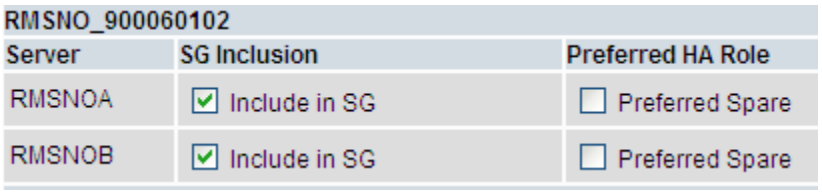
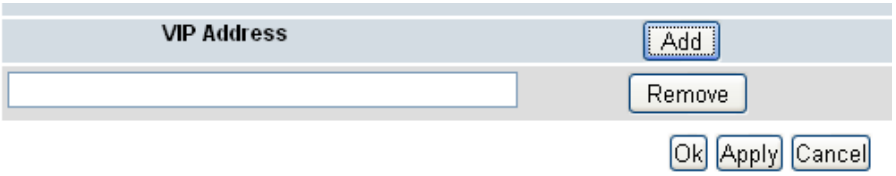
Procedure 33. Configure the Second NOAMP Server

5 ☐	**Copy Configuration File to 2nd NOAMP Server**	From a terminal window connection on the 1st NOAMP iLO, use the `awpushcfg` utility to copy the configuration file created in the previous step from the `/var/TKLC/db/filemgmt` directory on the 1st NOAMP to the 2nd NOAMP blade server, using the Control network IP address for the 2nd NOAMP blade server. The configuration file will have a filename like `TKLCConfigData.<hostname>.sh`. `# awpushcfg` The awpushcfg utility is interactive, so the user will be - prompted for the IP address of the local PMAC server. Use the local control network address from the PMAC. - the blade inventory will be presented, - prompted for the Control network IP address for the target server (In this case, the standby NOAMP server). - prompted for the hostname of the target server,

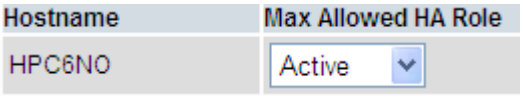
6 ☐	**Set the timezone and Reboot the Server**	Obtain a terminal window connection on the 2nd NOAMP iLO from the OA (Use the procedure in 4.18Appendix F).
		The automatic configuration daemon will look for the file named "TKLCConfigData.sh" in the /var/tmp directory, implement the configuration in the file, and then prompt the user to reboot the server.
		
		Verify awpushcfg was called by checking the following file
		`# cat /var/TKLC/appw/logs/Process/install.log`
		Set the timezone using the following command. The following command example uses the America/New_York time zone. Replace as appropriate with the time zone you have selected for this installation. For UTC, use "Etc/UTC", for a full list of valid timezones, see 4.18Appendix K.
		`# /usr/TKLC/appworks/bin/set_ini_tz.pl "Etc/UTC" >/dev/null 2>&1`
		Now Reboot the Server:
		`# init 6`
		Wait for the server to reboot

7 ☐	**(Optional) Configure Networking for Dedicated NetBackup Interface**	**NOTE: You will only execute this step if your NO is using a dedicated Ethernet interface for NetBackup.**
		
		From a root login session on the 2nd NO, execute the following commands:
		`# netAdm set --device=netbackup --type=Ethernet --onboot=yes --address=<NO2_NetBackup_IP> --netmask=<NetBackup_NetMask>`
		
		`# netAdm add --route=net --device=netbackup --address=<NetBackup_Network_ID> --netmask=<NetBackup_Network_NetMask> --gateway=<NetBackup_Network_Gateway_IP>`

Procedure 34. Complete Configuring the NOAMP Server Group

S T E P #	This procedure will provide the steps to finish configuring th NOAMP Server Group. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**Edit the NOAMP Server Group Data**	From the GUI session on the first NOAMP server, go to the GUI **Main Menu->Configuration->Server Groups.** Select the NOAMP Server group and click on **Edit** and add the second NOAMP server to the Server Group by clicking the "Include in SG" checkbox for the second NOAMP server. Click **Apply.**  Add a NOAMP VIP by click on **Add**. Fill in the `VIP Address` and press **Ok** as shown below 
2 ☐	**Wait for Replication**	After replication, which will initially take up to 5 minutes, the HA status should be active (**Main menu->Status & Manage->HA**). Note: This may take up to 5 minutes while the NOAMP servers figure out master/slave relationship. Log out of GUI from the first NOAMP XMI address.
3 ☐	**Establish GUI Session on the NOAMP VIP**	Establish a GUI session on the NOAMP by using the XMI VIP address. Login as user "guiadmin".
4 ☐	**Wait for Remote Database Alarm to Clear**	Wait for the alarm "Remote Database re-initialization in progress" to be cleared before proceeding. (**Main menu->Alarms & Events->View Active**)

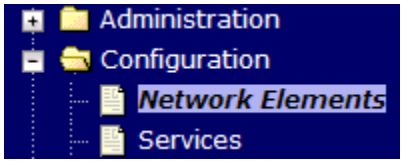
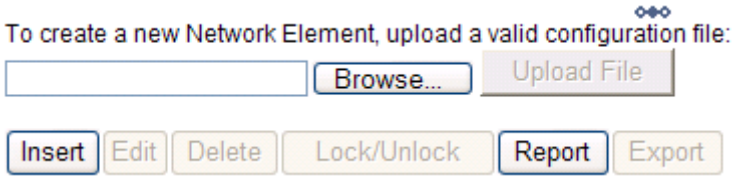
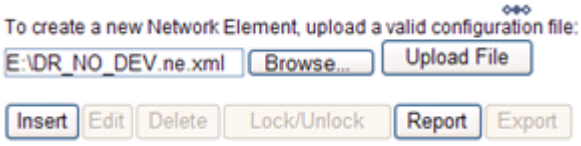
Procedure 34. Complete Configuring the NOAMP Server Group

5 ☐	**Verify HA Role for 2nd NOAMP server**	In the **Main menu->Status & Manage->HA** menu, verify that the "Max Allowed HA Role" for the 2nd NOAMP server is "Active". If it is **not**, press the **Edit** button and in the resulting screen, change the 2nd NOAMPs server's "Max Allowed HA Role" to "Active" using the dropdown box.  Press **OK**.
6 ☐	**Restart 2nd NOAMP blade server**	In the **Main menu->Status & Manage->Server** menu, select the second NOAMP server. Select the "Restart" button. Answer OK to the confirmation popup. Wait approximately 3-5 minutes before proceeding to allow the system to stabilize indicated by having the "Appl State" as "Enabled".
7 ☐	**SDS can now be installed (Optional)**	If this deployement contains SDS, SDS can now be installed.

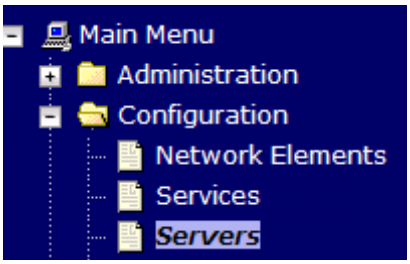
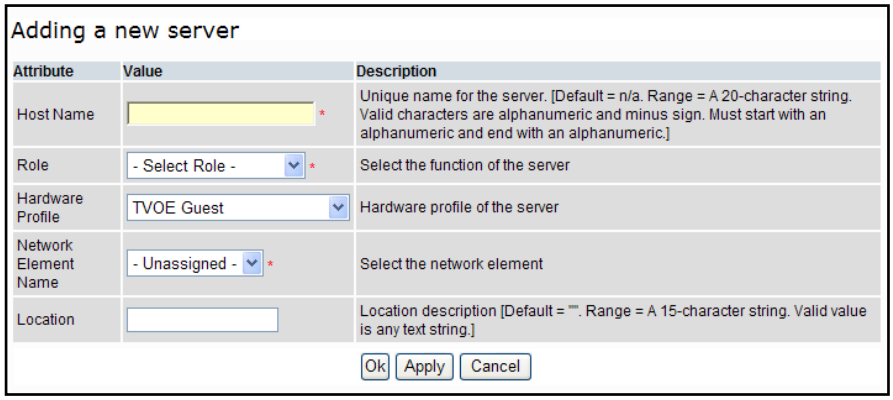
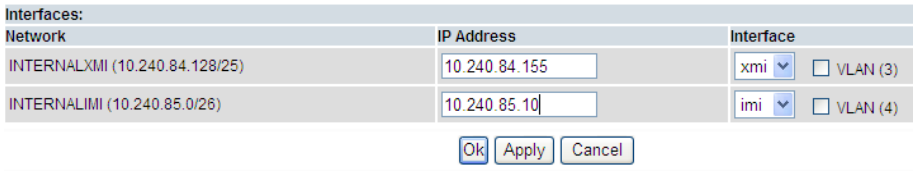
Procedure 35. Install NetBackup Client (Optional)

STEP #	This procedure will download and install NetBackup Client software on the server. Location of the bpstart_notify and bpend_notify scripts is required for the execution of this procedure. For Appworks based applications the scripts are located as follows: /usr/TKLC/appworks/sbin/bpstart_notify /usr/TKLC/appworks/sbin/bpend_notify Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**Install Netbackup Client Software**	If a customer has a way of transferring and installing the netbackup client without the aid of TPD tools (push configuration) then use *Appendix J.2 Netbackup Client Install with nbAutoInstall*. **This is not common. If the answer to the previous question is not known** then use *Appendix J.1 Netbackup Client Install with platcfg*.
2 ☐	**Install Netbackup Client Software**	Choose the same method used in step 1 to install NetBackup on the 2nd NO.

Procedure 36. NO Configuration for DR Site (Optional)

S T E P #	This procedure will provide the steps to configure the First DR NOAMP blade server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. **Prerequisite**: Application software already installed. **Needed material:** - DR Site installed with its PM&C Configured - DSR NO DR Site Network Element File IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**Primary NOAMP VIP GUI :** Login	Using a web browser, navigate to the **XMI Virtual IP Address (VIP)** of the **Primary NO Site.** Login using the guiadmin user.
2 ☐	**Primary NOAMP VIP GUI:** Insert Network Element for DR Site	Refer to appendix A for a sample network element xml file (contains direction on setting the NTP servers). Using the GUI menu, Navigate to **Configuration -> Network Elements** as shown below  The "**Network** Elements" screen will display, select the **"Browse"** dialogue button (scroll to bottom left corner of screen).  A dialogue will pop up, browse to the location of the DSR DR NO Site Element XML File and click the **"Open"** button. Then click "**Upload File**" as shown below  If the values in the .xml file pass validation rules, the user will receive a banner information message showing that the data has been successfully validated and committed to the DB.

Procedure 36. NO Configuration for DR Site (Optional)

3 ☐	**Primary NOAMP VIP GUI:** Insert Servers	Using the GUI menu, Navigate to **Configuration -> Servers** as shown below  Click the "**Insert**" button (bottom left corner of screen). An "**Adding a new server**" screen will be displayed up as shown below  Fill in the following Values: Host Name: Name of **DSR DR NO Server A** Role: Select the **NETWORK OAM&P** Hardware Profile: Select **DSR TVOE Guest** Network element Name: Select the network Element Name for the **DSR DR** Site (the one inserted in step 2 above). Location: Fill in the server geographical location (optional). The network interface fields will now become available with selection choices based on the chosen hardware profile and network element  Fill in the server IP addresses for the XMI network. Select "xmi" for the interface. **Leave the "VLAN" checkbox unchecked**. Fill in the server IP addresses for the IMI network. Select "imi" for the interface. **Leave the "VLAN" checkbox unchecked**. (Continued in the next step …)

Procedure 36. NO Configuration for DR Site (Optional)

<table>
<tr>
<td>4
☐</td>
<td>Primary NOAMP VIP GUI: Insert Servers - Cont.</td>
<td>For DSR 4.1.X installations ONLY: add the following NTP servers:
If inserting the DR-NO “A” Server:
<table>
<tr><th>NTP Server</th><th>Preferred?</th></tr>
<tr><td><DR-NO1-TVOE-XMI-IP-Address></td><td>Yes</td></tr>
</table>
If inserting the DR-NO “B” Server:
<table>
<tr><th>NTP Server</th><th>Preferred?</th></tr>
<tr><td><DR-NO2-TVOE-XMI-IP-Address></td><td>Yes</td></tr>
</table>
Select the “Ok” button when you have completed entering the server data.</td>
</tr>
<tr>
<td>5
☐</td>
<td>Primary NOAMP VIP GUI: Export the Initial Configuration</td>
<td>Navigate to <tt>Main Menu -> Configuration -> Servers</tt>

From the GUI screen, select the DR NO server added in the previous step and click the “Export” button to generate the initial configuration data for that server.

The user will receive a banner information message as shown below.
 
</td>
</tr>
<tr>
<td>6
☐</td>
<td>Exchange SSH keys between NOAMP and PMAC at the DR site</td>
<td>From a terminal window connection on the NOAMP VIP, exchange SSH keys between the NOAMP and the DR NO’s PMAC using the keyexchange utility.
When prompted for the password, enter the root password for the PMAC server.
<tt>keyexchange root@<DR_NO_SITE_PMAC_Management_IP></tt></td>
</tr>
<tr>
<td>7
☐</td>
<td>Copy Configuration File to 1st DR NO Server</td>
<td>SSH to the NOAMP VIP and use the <tt>awpushcfg</tt> utility to copy the configuration file created in the previous step from the <tt>/var/TKLC/db/filemgmt</tt> directory on the Primary Active to the first DR NOAMP server, using the Control network IP address for the first DR NOAMP serrver. The configuration file will have a filename like <tt>TKLCConfigData.hostname.sh</tt>.
<tt>awpushcfg</tt>

The awpushcfg utility is interactive, so the user will be
- prompted for the IP address of the PMAC server (make sure you enter the Management IP address of the PM&C on the DR Site),
- the blade inventory will be presented,
- prompted for the Control network IP address for the target server (in this case, the first DR NOAMP server).
- prompted for the hostname of the target server,</td>
</tr>
</table>

Procedure 36. NO Configuration for DR Site (Optional)

8 ☐	**DR NO Server A:** Verify awpushcfg was successful	• Access the machine hosting the **DR NO Server A** using the **iLO** Connection and log in as root.
		• Access the **DR NO Server A VM** console by running the following commands
		`# virsh list --all`
		`Id Name State`
		`----------`
		`6 vm-pmac running`
		`7 DSR-NO running`
		The connect to **DR NO Server A VM** using the following command, and login as root.
		`# virsh console DSR-NO`
		`Connected to domain vm-DSR-NO`
		`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`
		`DSR-NO login: root`
		`Password:`
		`Last login: Fri May 25 16:39:04 on ttyS4`
		• Verify awpushcfg was called by checking the following file
		`# cat /var/TKLC/appw/logs/Process/install.log`

9 ☐	**DR NO Server A VM:** Wait for Configuration to Complete	The automatic configuration daemon will look for the file named "TKLCConfigData.sh" in the /var/tmp directory, implement the configuration in the file, and then prompt the user to reboot the server. Wait to be prompted to reboot the server, but **DO NOT** reboot the server, it will be rebooted later on in this procedure. **NOTE**: Ignore the warning about removing the USB key, since no USB key is present. .
10 ☐	**DR NO Server A VM:** Configure Time Zone	From the command line prompt, execute *set_ini_tz.pl*. This will set the system time zone The following command example uses the America/New_York time zone. Replace as appropriate with the time zone you have selected for this installation. For UTC, use "Etc/UTC", for a full list of valid timezones, see 4.18Appendix K. `# /usr/TKLC/appworks/bin/set_ini_tz.pl "Etc/UTC" >/dev/null 2>&1`
11 ☐	**DR NO Server A VM:** Reboot the VM	Reboot the server using the following command: `# init 6` Then wait for the server to reboot (takes between 5 and 10 minutes)

Procedure 36. NO Configuration for DR Site (Optional)

12 ☐	**DR NO Server A VM:** Configure Networking for Dedicated NetBackup Interface (Optional)	**NOTE: You will only execute this step if your NO is using a dedicated Ethernet interface for NetBackup.**
		
		From a root login session on the first NO, execute the following commands:
		`# netAdm set --device=netbackup --type=Ethernet --onboot=yes --address=<NO1_NetBackup_IP> --netmask=<NetBackup_NetMask>`
		
		`# netAdm add --route=net --device=netbackup --address=<NetBackup_Network_ID> --netmask=<NetBackup_Network_NetMask> --gateway=<NetBackup_Network_Gateway_IP>`

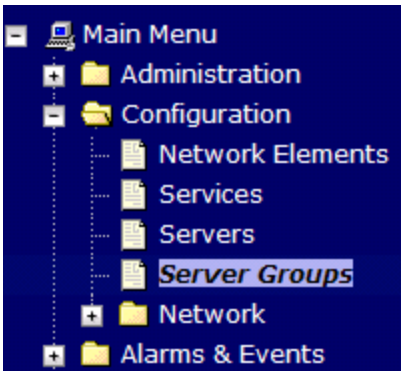
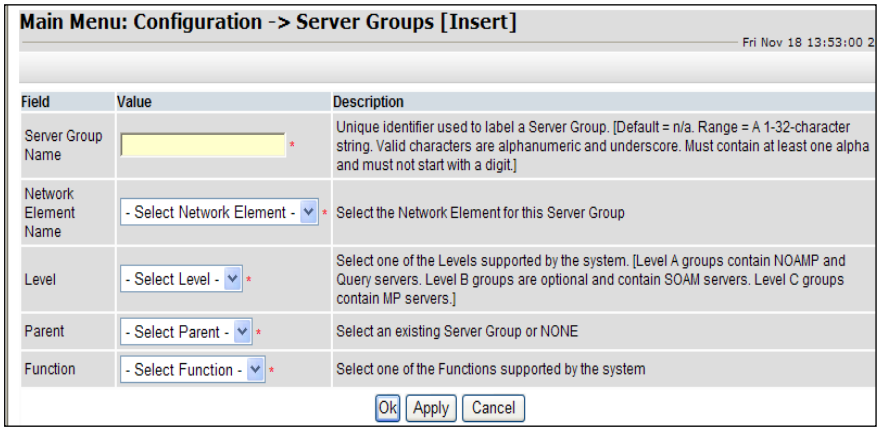
13 ☐	**DR NO Server A VM:** Verify Server Health	Execute the following command and make sure that no errors are returned:
		`# syscheck`
		`Running modules in class hardware... OK`
		`Running modules in class disk... OK`
		`Running modules in class net... OK`
		`Running modules in class system... OK`
		`Running modules in class proc... OK`
		`LOG LOCATION: /var/TKLC/log/syscheck/fail_log`

14 ☐	**Repeat for DR NO Server B**	Repeat Steps 3 through 13 to configure DR NO Server B.

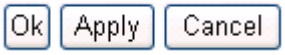
Procedure 37. NO Pairing for DSR NO DR Site (Optional)

S T E P #	This procedure will provide the steps to configure the First DR NOAMP blade server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. **Prerequisite**: Procedure 36. NO Installation for DR Site complete IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**Primary NOAMP VIP GUI:** Login	Using a web browser, navigate to the **XMI Virtual IP Address (VIP)** of the **Primary NO Site.** Login using the guiadmin user.

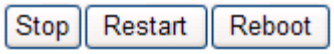
Procedure 37. NO Pairing for DSR NO DR Site (Optional)

2 ☐	**Primary NOAMP GUI:** Navigate to Server Group	Using the GUI menu, Navigate to **Configuration -> Server Groups** as shown below 
3 ☐	**Primary NOAMP GUI:** Insert Server Group	The **Server Groups** screen will display, click on **Insert** to add a new Server Group  The following will be displayed  Fill in the following values: Server Group Name: Name of **DSR DR NO** Site Network Element Name: Select the **DSR DR Site** Level: Select **A** Parent: Select **None** Function: Select **DSR** Then press "**Apply**", make sure the validation is successful

Procedure 37. NO Pairing for DSR NO DR Site (Optional)

4 ☐	**Primary NOAMP GUI:** Update Server Group	Select the **Server Group** that was created in the previous step, and click on "**Edit**".  The user will be presented with the **"Server Groups [Edit]"** screen Check the checkbox labeled "**Include in SG**" for the "**A**" and "**B**" DR Servers as shown below and click on "**Apply**" 
5 ☐	**Primary NOAMP GUI:** Add VIP	Click the "**Add**" dialogue button for the VIP Address and enter an IP Address for the VIP as shown below  Then click the "**Apply**" dialogue button. Verify that the banner information message states **"Data committed"**. 
6 ☐	**Primary NOAMP GUI:** Wait for 5 minutes	Now that the server(s) have been paired within a Server Group they must establish a master/slave relationship for High Availability (HA). It may take several minutes for this process to be completed. Allow a minimum of **5 minutes** before continuing to the next Step.
7 ☐	**Primary NOAMP GUI:** Verify/Change HA Status	Using the GUI main menu, Navigate to **Status & Manage -> HA** Verify that the "**Max Allowed HA Role"** for **DR NO Servers A** and **B** shows **"Active"**. If the "**Max Allowed HA Role**" is set to standby for **Server A** or **Server B**, then click on "**Edit**" and set the "**Max Allowed HA Role**" to be "**Active**" for both DR Servers then press "**OK**". You will be returned to the previous screen, verify that the "**Max Allowed HA Role"** for **DR NO Servers A** and **B** now shows **"Active"**.

Procedure 37. NO Pairing for DSR NO DR Site (Optional)

8 ☐	**Primary NOAMP GUI:** Verify Server Status	Using the GUI main menu, Navigate to **Status & Manage** -> **Server** The **"A"** and **"B"** DR NO servers should now appear in the right panel. Verify that the **"DB"** status shows **"Norm"** and the **"Proc"** status shows **"Man"** for both servers before proceeding to the next Step. 
9 ☐	**Primary NOAMP GUI:** Restart Application on DR NO A	Using the mouse, select **DR NO Server A**. The line entry should now be highlighted in **GREEN**. Click the **"Restart"** button from the bottom left corner of the screen.  Click the **"OK"** button on the confirmation dialogue box. The user should be presented with a confirmation message (in the banner area) for **DR NO Server A** stating: **"Successfully restarted application"**.
10 ☐	**Primary NOAMP GUI:** Verify Application State on DR NO Server A	Using the GUI main menu, Navigate to **Status & Manage** -> **Server** Verify that the **"Appl State"** now shows **"Enabled"** and that the **"Alm, Repl, Coll, DB, HA & Proc"** status columns all show **"Norm"** for **DR NO Server A** before proceeding to the next Step.  **NOTE:** *If user chooses to refresh the Server status screen in advance of the default setting (15-30 sec.). This may be done by simply reselecting the* ***"Status & Manage → Server"*** *option from the Main menu on the left.*
11 ☐	**Primary NOAMP GUI:** Restart the application on DR NO Server B	Repeat Steps 8 – 10, but this time selecting DR NO Server B instead of A

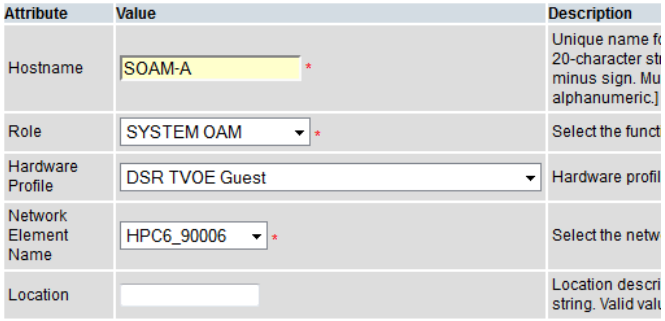
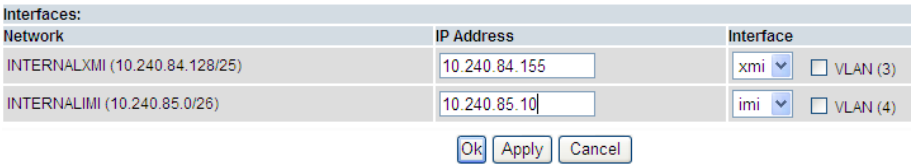
Procedure 38. Configure the SOAM NE

S T E P #	This procedure will provide the steps to configure the SOAM Network Element Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**Establish GUI Session on the NOAMP VIP**	If needed, establish a GUI session on the NOAMP by using the OAM VIP address. Login as user "guiadmin".
2 ☐	**Create the SOAM Network Element using an XML File**	Make sure to have an SOAM Network Element XML file available on the PC that is running the web browser. The SOAM Network Element XML file is similar to what was created and used in Procedure 31, but defines the SOAM "Network Element". Refer to Appendix A for a sample Network Element xml file (and instructions on what NTP server to choose) Navigate to **Main Menu->Configuration->Network Elements** Select the "Browse" button, and enter the path and name of the SOAM network XML file. Select the "Upload File" button to upload the XML file and configure the SOAM Network Element.

Procedure 39. Configure the SOAM Servers

S T E P #	This procedure will provide the steps to configure the SOAM 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 TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**Exchange SSH keys between SOAM site's local PMAC and the SOAM server**	Use the **SOAM site's** PMAC GUI to determine the Control Network IP address of the server that is to be the SOAM server. From that site's PMAC GUI, navigate to **Main Menu → Software→Software Inventory**. Note the IP address for the SOAM server. From a terminal window connection on the **SOAM site's** PMAC, exchange SSH keys between the PMAC and the SOAM server using the keyexchange utility, using the Control network IP address for the SOAM server. When prompted for the password, enter the password for the SOAM server. # **keyexchange root@<SOAM blade Control Net IP addr>**
2 ☐	**Exchange SSH keys between NOAMP and PMAC at the SOAM site (If necessary)**	**NOTE: If this SOAM shares the same PMAC as the NOAM, then you can skip this step.** From a terminal window connection on the **NOAMP VIP**, exchange SSH keys between the NOAMP and the PMAC for this SOAM site using the keyexchange utility.

Procedure 39. Configure the SOAM Servers

		When prompted for the password, enter the root password for the PMAC server. # **keyexchange root@<SOAM_SITE_PMAC_Management_IP>**
3 ☐	**Establish GUI Session on the NOAMP VIP**	If needed, establish a GUI session on the NOAMP by using the OAM VIP address. Login as user "guiadmin".
4 ☐	**Insert the SOAM "A" server**	Navigate to **Main Menu->Configuration->Servers** Select the "Insert" button to insert the new SOAM "A" server into servers table.  Fill in the fields as follows: **Hostname:** **<Hostname>** **Role:** **SYSTEM OAM** **Hardware Profile:** **DSR TVOE Guest** **Network Element Name:** **[Choose NE from Drop Down Box]** The network interface fields will now become available with selection choices based on the chosen hardware profile and network element  Fill in the server IP addresses for the XMI network. Select "xmi" for the interface. **Leave the "VLAN" checkbox unchecked**. Fill in the server IP addresses for the IMI network. Select "imi" for the interface. **Leave the "VLAN" checkbox unchecked**. For **DSR 4.1.X installations ONLY:** add the following NTP servers: **NTP Server** | **Preferred?** ***<SO1-TVOE-XMI-IP-Address>*** | Yes Select the "Ok" button when you have completed entering the server data.

Procedure 39. Configure the SOAM Servers

5 ☐	**Export the initial configuration**	From the GUI screen, select the desired server and then select "Export" action button to generate the initial configuration data for that server.
6 ☐	**Copy Configuration File to SOAM "A" server**	From a terminal window connection on the Active NOAMP, use the `awpushcfg` utility to copy the configuration file created in the previous step from the `/var/TKLC/db/filemgmt` directory on the 1st NOAMP to the SOAM server, using the Control network IP address for the SOAM server. The configuration file will have a filename like `TKLCConfigData.<hostname>.sh`. Verify that the server is in the "ProvideSvc" role and the availability is "Available", then proceed with... # **awpushcfg** The awpushcfg utility is interactive, so the user will be - prompted for the management IP address of the PMAC server at the site where the target blade is located. - prompted for the hostname of the target server, - prompted for the Control network IP address for the target server (in this case, the SOAM server). Use the SOAM IP address from step 1. The configuration success message can also be found in the /var/log/messages file.
7 ☐	**Wait for the reboot prompt and boot the Configured Server**	Obtain a terminal window connection on the SOAM "A" server console. The automatic configuration daemon will look for the file named "TKLCConfigData.sh" in the /var/tmp directory, implement the configuration in the file, and then prompt the user to reboot the server. Wait to be prompted to reboot the server. NOTE: Ignore the warning about removing the USB key, since no USB key is present. Use "init 6" in the terminal window to reboot the server as shown below. Verify awpushcfg was called by checking the following file # **cat /var/TKLC/appw/logs/Process/install.log** Set the timezone using the following command. The following command example uses the America/New_York time zone. Replace as appropriate with the time zone you have selected for this installation. For UTC, use "Etc/UTC", for a full list of valid timezones, see 4.18Appendix K. **# /usr/TKLC/appworks/bin/set_ini_tz.pl "Etc/UTC" >/dev/null 2>&1** Now reboot the server using the following command: # **init 6**

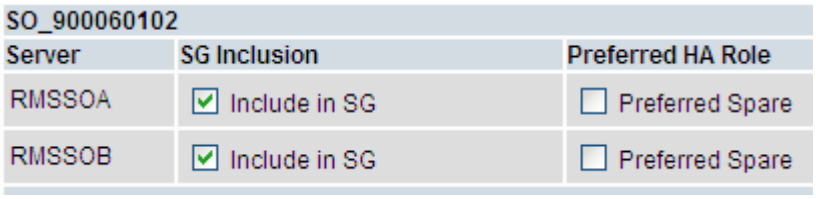
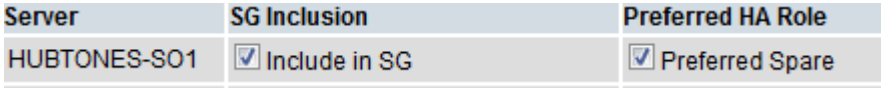
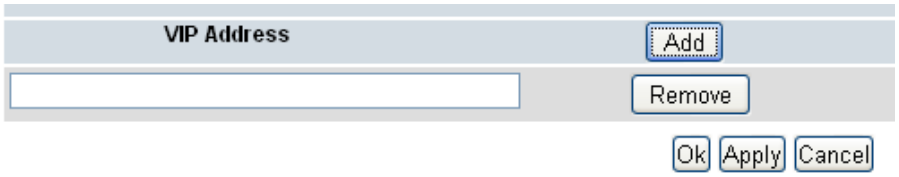
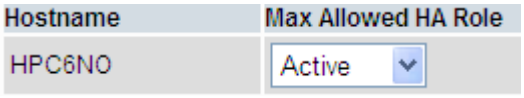
Procedure 39. Configure the SOAM Servers

8 ☐	**Insert and Configure the SOAM "B" server**	Repeat this procedure to insert and configure the SOAM "B" server. Instead of data for the "A" Server, insert the network data for the "B" server. For **DSR 4.1.X installations ONLY:** add the following NTP servers: **NTP Server** | **Preferred?** ***<SO2-TVOE-XMI-IP-Address>*** | Yes Transfer the TKLCConfigData file to the "B" server, and reboot the "B" server when prompted at a terminal window. Make sure to set the timezone as well.
9 ☐	**(OPTIONAL) Insert and Configure the SOAM Spare server**	If your site has SOs in Active/Standby/Spare configuration such as PDRA, then repeat this procedure to insert and configure the SOAM spare server. Instead of data for the "A" Server, insert the network data for the spare server, transfer the TKLCConfigData file to the spare server, and reboot the spare server when prompted at a terminal window. Make sure to set the timezone as well.
10 ☐	**(OPTIONAL) Install Netbackup Client Software on SOAMs**	If you are using Netbackup at this site, then execute **Procedure 35** again to install the Netbackup Client on all SOAM servers.

Procedure 40. Configure the SOAM Server Group

STEP #	This procedure will provide the steps to configure the SOAM Server Group Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**Enter SOAM Server Group Data**	After a approximately 5 minutes for the SOAM "B" server to reboot, from the GUI session on the NOAMP VIP address, go to the GUI Main Menu->Configuration->Server Groups, select Insert and add the SOAM Server Group name along with the values for the following fields: • Name → **[Enter Server Group Name]** • Level → **B** • Parent **[Select the NOAMP Server Group]** • Function: **DSR (Active/Standby Pair)** Select "OK" when all fields are filled.

Procedure 40. Configure the SOAM Server Group

2 ☐	**Edit the SOAM Server Group and add VIP**	From the GUI **Main Menu->Configuration->Server Groups**, select the new SOAM server group, and then select "Edit".  SO_900060102 Server / SG Inclusion / Preferred HA Role RMSSOA — Include in SG — Preferred Spare RMSSOB — Include in SG — Preferred Spare Select the SOAM Server group and click on **Edit** Add both SOAM servers to the Server Group by clicking the "Include in SG" checkbox If you are adding a SOAM spare sever to this server group, then click the "Include in SG" checkbox next to the spare server and also check the "Preferred Spare" checkbox.  Server / SG Inclusion / Preferred HA Role HUBTONES-SO1 — Include in SG — Preferred Spare Click **Apply.** Add a SOAM VIP by click on **Add**. Fill in the VIP Address and press **Ok** as shown below  VIP Address Add Remove Ok Apply Cancel
3 ☐	**Wait for Replication**	After replication, which will initially take up to 5 minutes, the server status should be active (Main menu->Status & Manage->Replication). Note: This may take up to 5 minutes while the servers figure out master/slave relationship. Look for the alarm "Remote Database re-initialization in progress" to be cleared before proceeding. (Main menu->Alarms->View Active)
4 ☐	**Verify HA Role for 2nd SOAMP server**	In the **Main menu->Status & Manage->HA** menu, verify that the "Max Allowed HA Role" for the 2nd SOAMP server is "Active". If it is **not**, press the **Edit** button and in the resulting screen, change the 2nd NOAMPs server's "Max Allowed HA Role" to "Active" using the dropdown box.  Hostname / Max Allowed HA Role HPC6NO — Active Press **OK**.
5 ☐	**Restart 1st SOAM server**	From the NOAMP GUI, select the Main menu->Status & Manage->Server menu. Select the "A" SOAM server. Select the "Restart" button. Answer OK to the confirmation popup. Wait for restart to complete.

Procedure 40. Configure the SOAM Server Group

6 ☐	**Restart 2nd SOAM server**	Continuing in the Main menu->Status & Manage->Server menu, now select the "B" SOAM server. Select the "Restart" button. Answer OK to the confirmation popup.

Procedure 41. Post NOAMP & SOAM Setup Operations

STEP #	This procedure will provide the steps to optimize the NO and SO databases and run other operations that should happen once the NOAMP and all SOAM sites have been 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 TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	

1 ☐	**Log into all NO and SO servers atall sites and run database optimization script**	Obtain a terminal window connection to the (NO/SO) server console via SSH or iLO. **If using SSH, use the actual IP of the server, not the VIP address.**
		
		Execute the following on the command line. Wait until the script completes and you are returned to the command line:
		
		`# /usr/TKLC/dsr/bin/optimizeComcolIdbRamUsage`
		`# sleep 20`
		`# prod.start`
		`# pm.sanity`
		`Sanity check OK: 01/23/13 11:42:20 within 15 secs`
		
		Verify that the script finished successfully by checking the exit status:
		
		`# echo $?`
		
		If anything other than "0" is printed out,. halt this procedure and contact Tekelec Support..
		
		Repeat this step for the **standby NO, D.R. NO (if applicable) servers, and every SO server at every site.**

2 ☐	**(PDRA Only) Activate PDRA Feature**	If you are installing PDRA, execute the instructions in [9] to activate PDRA. **NOTE: If not all SOAM sites are ready at this point, then you should repeat activation for each *new* SOAM site that comes online.**

Procedure 41. Post NOAMP & SOAM Setup Operations

<table>
<tr>
<td>3
☐</td>
<td>(PDRA Only) Perform Additional Services to Networks Mapping</td>
<td>Log Into Active NO GUI.

Navigate to Main Menu → Configuration → Services.

Select the “Edit” button and set the Services as shown in the table below:

<table>
<tr><th>Name</th><th>Intra-NE Network</th><th>Inter-NE Network</th></tr>
<tr><td>Replication_MP</td><td><IMI Network></td><td><PSBR DB Replication Network>*</td></tr>
<tr><td>ComAgent</td><td><IMI Network></td><td><PSBR DB Replication Network>*</td></tr>
</table>

(*) It is recommended that dual-path HA heartbeats be enabled in support of geo-diverse PSBRs. This requires participating servers to be attached to at least two routable networks.

.

Select the “Ok” button to apply the Service-to-Network selections.</td>
</tr>
</table>

Procedure 42. Configure the MP Blade Servers

S T E P #	This procedure will provide the steps to configure an MP Blade 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 TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**Exchange SSH keys between MP site's local PMAC and the MP server**	Use the MP site's PMAC GUI to determine the Control Network IP address of the blade server that is to be an MP server. From the MP site's PMAC GUI, navigate to **Main Menu → Software-→Software Inventory**. Note the IP address for an MP server. From a terminal window connection on the MP site's local PMAC, exchange SSH keys between the PMAC and the MP blade server using the keyexchange utility, using the Control network IP address for the MP blade server. When prompted for the password, enter the password for the MP server. # **keyexchange root@<MP blade Control Net IP addr>**
2 ☐	**Establish GUI Session on the NOAMP VIP**	If needed, establish a GUI session on the NOAMP by using the XMI VIP address. Login as user "guiadmin".

Procedure 42. Configure the MP Blade Servers

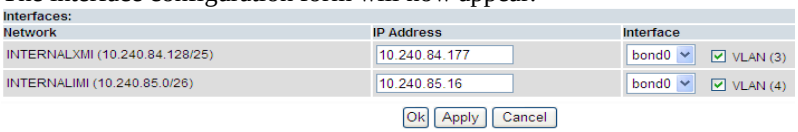
3 ☐	**Insert the MP server**	Navigate to **Main Menu->Configuration->Servers** Select the "Insert" button to insert the new MP server into servers table. Fill out the following values: **Hostname**: `<Hostname of the MP>` **Role**: `MP` **Network Element**: `[Choose Network Element]` **Hardware Profile**: Select the profile that matches your MP physical hardware and enclosure networking environment. Note that you must go through the process of identifying the enclosure switches, mezzannine cards and Ethernet interfaces of the network prior and blade(s) used before selecting the profile.

Profile Name	*Blade Size*	*Multiple Pairs of Enc. Switches?*	*Bonded Signaling Interfaces?*
BL460 HP c-Class Blade	Half	No	Yes
BL620 HP c-Class Blade	Full	No	Yes
L2D3 BL460 HP c-Class Blade	Half	Yes	Yes
L2D3 BL620 HP c-Class Blade	Full	Yes	Yes
L2D3 BL620 HP c-Class blade (Unbonded Sig)	Full	Yes	No
DSR TVOE Guest	N/A (Virtual)	N/A	N/A

NOTE: If none of the above profiles properly describe your MP server blade, then you will have to create your own in a text editor (See 4.18Appendix A) and copy it into the *`/var/TKLC/appworks/profiles/`* directory of the active NOAMP server. Then come back and repeat this step.

Location: <enter an optional location description>

The interface configuration form will now appear.



For the XMI network, enter the MP's XMI IP address. (**Note: an XMI address is mandatory for MP servers in DSR 4.0)** Select the correct bond or interface. If your XMI network uses VLAN tagging, then select the VLAN checkbox. If your XMI network does **NOT** use VLAN tagging, then do **NOT** select the vlan checkbox.

For the IMI network, enter the MP's IMI IP address. Select the proper bond or interface, and **select the VLAN checkbox.**

Continue to the next step for MP NTP server configuration …

Procedure 42. Configure the MP Blade Servers

<table>
<tr><td>4
☐</td><td>Insert the MP server - Part 2</td><td>For DSR 4.1.X installations ONLY: add the following NTP servers:
<table><tr><th>NTP Server</th><th>Preferred?</th></tr><tr><td><SO1-TVOE-XMI-IP-Address></td><td>Yes</td></tr><tr><td><SO2-TVOE-XMI-IP-Address></td><td>No</td></tr></table>
Select “OK” when all fields are filled in to finish MP server insertion.</td></tr>
<tr><td>5
☐</td><td>Export the initial configuration</td><td>From the GUI screen, select the server that was just inserted and then select “Export” action button to generate the initial configuration data for that server.</td></tr>
<tr><td>6
☐</td><td>Log onto the MP iLO</td><td>Obtain a terminal window connection on the MP server iLO from the OA.</td></tr>
<tr><td>7
☐</td><td>Copy Configuration File to MP server</td><td>From a terminal window connection on the active NOAMP, use the <code>awpushcfg</code> utility to copy the configuration file created in the previous step from the <code>/var/TKLC/db/filemgmt</code> directory on the active NOAMP to the MP blade server, using the Control network IP address for the MP blade server. The configuration file will have a filename like <code>TKLCConfigData.<<i>hostname</i>>.sh</code>.

<code># awpushcfg</code>

The awpushcfg utility is interactive, so the user will be
- prompted for the management IP address of the PMAC server at the site where the target blade is located.
- the blade inventory will be presented,
- prompted for the Control network IP address for the target server (in this case, the MP server).
- prompted for the hostname of the target server,

The automatic configuration daemon will look for the file named “TKLCConfigData.sh” in the /var/tmp directory, implement the configuration in the file, and then prompt the user to reboot the server.</td></tr>
</table>

Procedure 42. Configure the MP Blade Servers

8 ☐	**Set the Timezone and Reboot the Configured Server**	From the MP server iLO terminal, wait for the message ro reboot the server. Verify awpushcfg was called by checking the following file # **cat /var/TKLC/appw/logs/Process/install.log** Set the timezone using the following command. The following command example uses the America/New_York time zone. Replace as appropriate with the time zone you have selected for this installation. For UTC, use "Etc/UTC", for a full list of valid timezones, see 4.18Appendix K. **# /usr/TKLC/appworks/bin/set_ini_tz.pl "Etc/UTC" >/dev/null 2>&1** Use "init 6" in the terminal window to reboot the server. # **init 6** Proceed to the next step once the Server finished rebooting, The server is done rebooting once the login prompt is displayed.

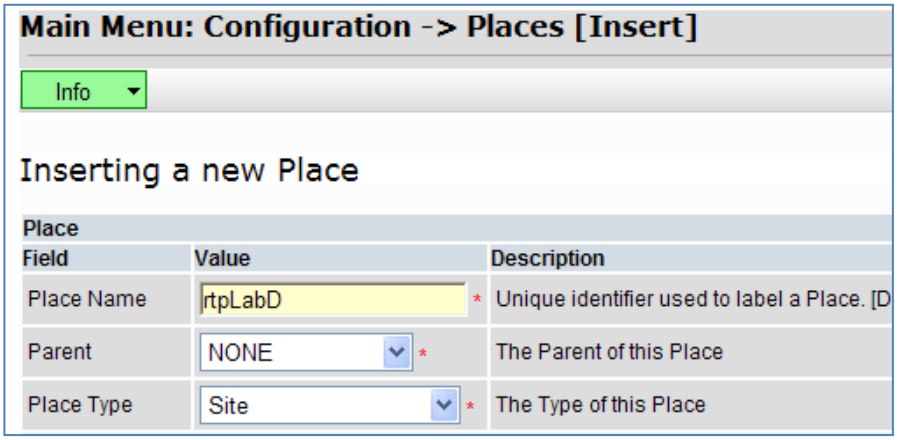
Procedure 42. Configure the MP Blade Servers

9 ☐	**(OPTIONAL) Delete Auto-Configured Default Route on MP and Replace it with a Network Route via the XMI Network**	*****NOTE: THIS STEP IS OPTIONAL AND SHOULD ONLY BE EXECTUED IF YOU PLAN TO CONFIGURE A DEFAULT ROUTE ON YOUR MP THAT USES A SIGNALING (XSI) NETWORK INSTEAD OF THE XMI NETWORK. (Not executing this step will mean that a default route will not be configurable on this MP and you will have to create separate network routes for each signaling network destination.) *****
		
		Log in to the **active NO** as the "root" user. Execute the following commands on the active NO:
		
		`# /usr/TKLC/appworks/sbin/deleteDefaultRoute <MP-Hostname>`
		`change status to Delete Pending for RouteId 6`
		`=== changed 1 records ===`
		
		`# syncApplConfig <MP-Hostname>`
		`NOTE: performing sync for IPFE1`
		`NOTE: Network configuration sync for IPFE1 is complete.`
		
		Now, using the iLO facility, **log into the MP** as the "root" user. The remaining commands in this step will be executed on the MP.
		
		Verify that the default route has been removed by executing the following command on the MP. There should be no output returned:
		
		`# netstat -r | grep default`
		`#`
		
		Note: If your NO XMI network is exactly the same as your MP XMI network, then you can skip this command and go right to the ping test afterwards.
		
		Determine <XMI_Gateway_IP> from your SO site network element info and <NO_XMI_Network_Address>,<NO_XMI_Network_Netmask> from your NO site network element info. You can either consult the XML files you imported earlier, or go to the NO GUI and view these values from the *Main Menu>Configuration>Network Elements* screen.
		
		[MP console] Create network route to the NO's XMI(OAM) network:
		
		`# netAdm add --route=net --address=<NO_XMI_Network_Address> --netmask=<NO_XMI_Network_Netmask> --gateway=<XMI_Gateway_IP> --device=<MP_XMI_Interface>`
		
		`Route to <MP_XMI_Interface> added.`
		
		[MP Console] Ping active NO XMI IP address to verify connectivity:
		
		`# ping <ACTIVE_NO_XMI_IP_Address>`
		
		`PING 10.240.108.6 (10.240.108.6) 56(84) bytes of data.`
		`64 bytes from 10.240.108.6: icmp_seq=1 ttl=64 time=0.342 ms`
		`64 bytes from 10.240.108.6: icmp_seq=2 ttl=64 time=0.247 ms`
		
		If you do not get a response, then verify your network configuration. If you continue to get failures then halt the installation and contact Tekelec customer support.

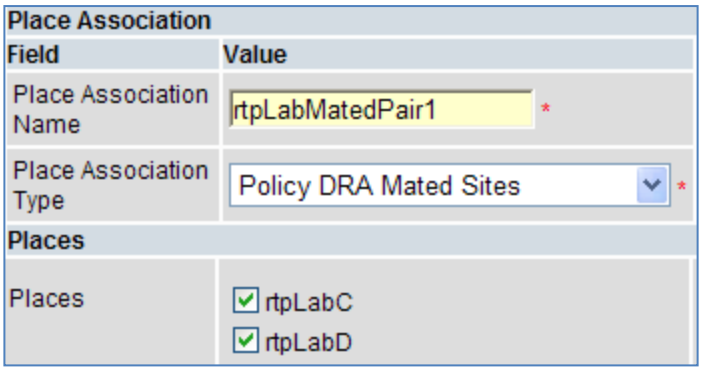
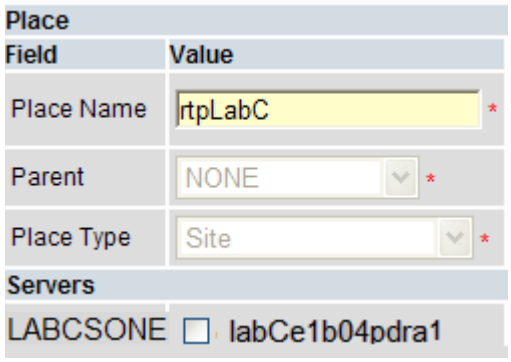
Procedure 42. Configure the MP Blade Servers

10 ☐	**Repeat for remaining MP at all sites**	Repeat this entire procedure for all remaining MP blades at all sites.

Procedure 43. Configure Places and Assign MP Servers to Places (PDRA Installations ONLY)

STEP #	This procedure will provide the steps/reference to add "Places" in the PDRA 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 TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**(PDRA Only) NOAMP VIP:** **Configure Places**	Establish a GUI session on the NOAMP by using the XMI VIP address. Login as user "guiadmin". Navigate to **Main Menu -> Configuration -> Places** Screen.  Place Name: Choose the site NAME Parent: Choose "NONE" Place Type: Choose "Site" **Repeat this step for all Places you wish to define.**

Procedure 43. Configure Places and Assign MP Servers to Places (PDRA Installations ONLY)

2 ☐	**(PDRA Only)** **NOAMP VIP:** **Configure Place Associations**	Click on **Insert** in the lower left corner and enter the information to create the place association for mated pairs, click Ok.  NOTE: . Place Association Name: .**Enter Association Name** Place Association Type: . **Policy DRA Mated Sites** Places: .Click on the list of Places you wish to define under this Place Association. **Repeat this step for all place associations you wish to define.**
3 ☐	**(PDRA Only)** **NOAMP VIP:** **Assign MP Servers To Places**	For each place you have defined, choose the set of MP servers that will be assigned to those places.  Check all the check boxes for PDRA and pSBR servers that will be assigned to this place. **Repeat this step for all other PDRA or pSBR servers you wish to assign to places.**

Procedure 44. Configure the MP Server Group(s) and Profiles

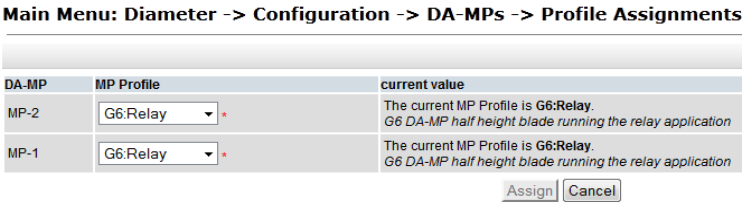
S T E P #	This procedure will provide the steps to configure MP Server Groups Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**Enter MP Server Group Data**	From the GUI session on the NOAMP VIP address, go to the GUI **Main Menu→Configuration→Server Groups**, select **Insert** and fill out the following fields: Server Group Name**: [Server Group Name]** Level: **C** Parent: **[Select the SOAMP Server Group That is Parent To this MP]** Function**: Select the Proper Function for this MP Server Group:** Select **OK** when all fields are filled in.
2 ☐	**Repeat For Addional Server Groups**	**Repeat Step 1** for any remaining MP server groups you wish to create. For instance,if you are installing *IPFE*, you will need to create an IP Load Balancer server group. If you are installing the CPA, you will need a Session Binding Repository server group. For PDRA, you will need at least one Policy SBR server group.

Server Group Function	MPs Will Run	Redundancy Model
DSR (multi-active cluster)	Diameter Relay and Application Services	Multiple MPs active
DSR (active-standby pair)	Diameter Relay and Application Services	1 Active MP and 1 Standby MP
Session Binding Repository	Session Binding Repository Function	1 Active MP and 1 Standby MP
IP Load Balancer	IPFE application	1 Active MP
Policy SBR	Policy Session and/or Policy Binding Application	1 Active MP

Procedure 44. Configure the MP Server Group(s) and Profiles

6 ☐	**Edit the MP Server Groups to include MP blades.**	From the GUI **Main Menu->Configuration->Server Groups**, select a server group that you just created and then select **Edit**. Select the Network Element that represents the MP server group you wish to edit. Click the "Include in SG" box for every MP server that you wish to include in *this* server group. Leave other checkboxes blank. HPC6_90006 Server / SG Inclusion / Preferred HA Role MP-1 ☑ Include in SG ☐ Preferred Spare MP-2 ☑ Include in SG ☐ Preferred Spare Select **Ok**. **Repeat for any remaining MP server groups untili all MPs have been assigned to a server group.**
7 ☐	**Wait for Replication to complete on all MP blades**	Browse to **Main menu->Status&Manage->Server.** Identify all the MP servers in the *Server Hostname* column . Now, wait for the corresponding *DB* and *Reporting Status* columns of those MPs to say "Norm". This may take up to 5 or 10 minutes. Server Hostname / Appl State / Alm / DB / Reporting Status HPC6-NO Enabled Norm Norm Norm HPC6-SO Enabled Warn Norm Norm HPC6-MP2 Enabled Warn Norm Norm HPC6-MP1 Enabled Warn Norm Norm
8 ☐	**Wait for Remote Database Alarm to Clear**	Wait for the alarm "10200: Remote Database re-initialization in progress" to be cleared. (**Main menu->Alarms & Events->Active Alarms**) This should happen shortly after you have verified the "Norm" DB status in the previous step.

Procedure 44. Configure the MP Server Group(s) and Profiles

<table>
<tr>
<td>9
☐</td>
<td>Assign Profiles to MPs from SOAM GUI.</td>
<td>Log onto the GUI of the active SOAM server.
From the SO GUI, select MainMenu->Diameter->Configuration->DA-MPs->Profiles Assignments
 

For each MP, select the proper profile assignment based on the MP’s hardware type and the function it will serve:
<table>
<tr><th>Profile Name</th><th>Description</th></tr>
<tr><td>G6:Relay</td><td>G6 DA-MP half height blade running relay application</td></tr>
<tr><td>G6:Database</td><td>G6 DA-MP half height blade running a database application (e.g. - FABR, RBAR)</td></tr>
<tr><td>G6:Session</td><td>G6 DA-MP half height blade running a session application (e.g. - CPA, PDRA)</td></tr>
<tr><td>G8:Relay</td><td>G8 DA-MP half height blade running the relay application</td></tr>
<tr><td>G8:Database</td><td>G8 DA-MP half height blade running a database application (e.g. FABR, RBAR)</td></tr>
<tr><td>G8:Session</td><td>G8 DA-MP half height blade running a session application (e.g. CPA, PDRA)</td></tr>
<tr><td>G7:Relay</td><td>G7 DA-MP Full height blade running the relay application</td></tr>
<tr><td>G7:Database</td><td>G7 DA-MP Full height blade running a database application (e.g. FABR, RBAR)</td></tr>
<tr><td>G7:Session</td><td>G7 DA-MP Full height blade running a session application (e.g. CPA, PDRA)</td></tr>
</table>

When finished, press the Assign button</td>
</tr>
<tr>
<td>10
☐</td>
<td>Update DpiOption table from the active SOAM</td>
<td>Log on to the active SOAM console via the XMI address or iLO.
Execute the following command (advise cut and paste to prevent errors):

```
# iset -fvalue="50" DpiOption where
"name='MpEngIngressMpsPercentile'"
```


=== changed 1 records ===</td>
</tr>
</table>

Procedure 44. Configure the MP Server Group(s) and Profiles

11 ☐	**Optimize Comcol memory usage**	SSH to each DA-MP and execute the following command. Note that this command **SHOULD NOT** be executed on SBR blades. **# /usr/TKLC/dsr/bin/optimizeComcolIdbRamUsage --force**
12 ☐	**Restart MP blade servers**	From the NOAMP GUI, select the **Main menu**->**Status & Manage**->**Server menu** *For each MP server:* • Select the MP server. • Select the **Restart** button. • Answer **OK** to the confirmation popup. Wait for the message which tells you that the restart was successful.

4.17 Signaling Network Configuration

Procedure 45. Configure the Signaling Networks

S T E P		
	This procedure will provide the steps to configure the Signaling Networks. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**Establish GUI Session on the NOAMP VIP**	Establish a GUI session on the NOAMP by using the XMI VIP address. Login as user "guiadmin".
2 ☐	**NOAMP VIP:** Navigate to Signaling Network Configuration Screen	Navigate to **Main Menu -> Configuration -> Network** Click on **Insert** in the lower left corner.
3 ☐	**NOAMP VIP:** Add First Signaling Network	You will see a screen similar to: Insert Network Field / Value / Description Network Name: XSI1 * — The name of this VLAN. [Default = n/a. Range = Alphanumeric string up to 31 chars, starting with a letter.] VLAN ID: 5 * — The VLAN ID to use for this VLAN. [Default = network dependent. Range = 4-4094 (VLAN 1-3 reserved for Management, XMI and IMI).] Network Address: 10.240.71.128 * — The network address of this VLAN. [Default = n/a. Range = Valid Network Address of the network in dotted decimal (IPv4) or colon hex (IPv6) format.] Netmask: 255.255.255.192 * — Subnetting to apply to servers within this VLAN. [Default = n/a. Range = Valid Netmask for the network in prefix length (IPv4 or IPv6) or dotted decimal (IPv4) format.] Ok Apply Cancel Enter the `Network Name, VLAN ID, Network Address and Netmask` that matches the first Internal Signaling network configuration at your site and press **Ok**.
4 ☐	**NOAMP VIP:** Add Second Signaling Network	Click on **Insert** in the lower left corner again and enter Enter the `Network Name, VLAN ID, Network Address and Netmask` that matches the second Internal Signaling network configuration at your site and press **Ok**. Repeat this step to configure any additional signaling networks.

Procedure 46. Configure the Signaling Devices

S T E P

This procedure will provide the steps to configure the Signaling Devices.

Note: The site specific HW configuration will affect which steps need to be executed

Questions:	How many pairs of switches are in the enclosure?	Will the MP use a bonded interface?
Possible Execution Scenarios:	Single	N/A
	Multiple	Yes
	Multiple	No

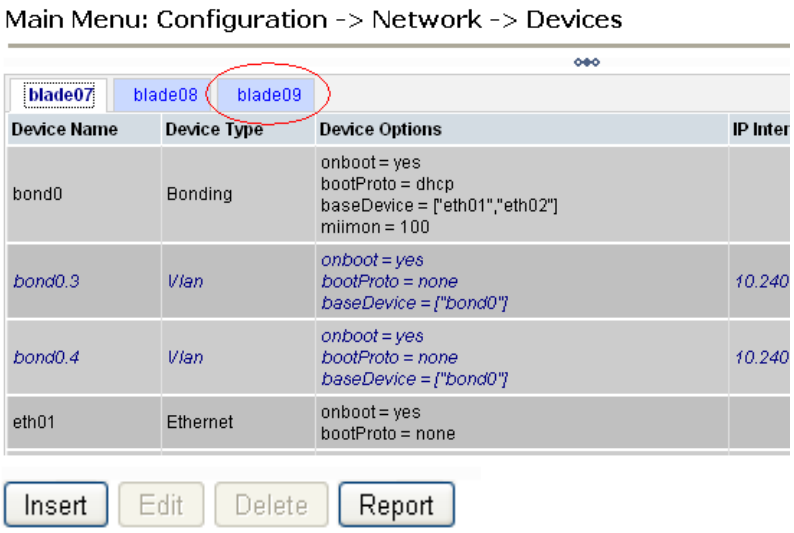
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.

1 ☐ **NOAMP VIP:** Configure the Signaling Interfaces of the first MP

Navigate to **Main Menu -> Configuration -> Network -> Devices**

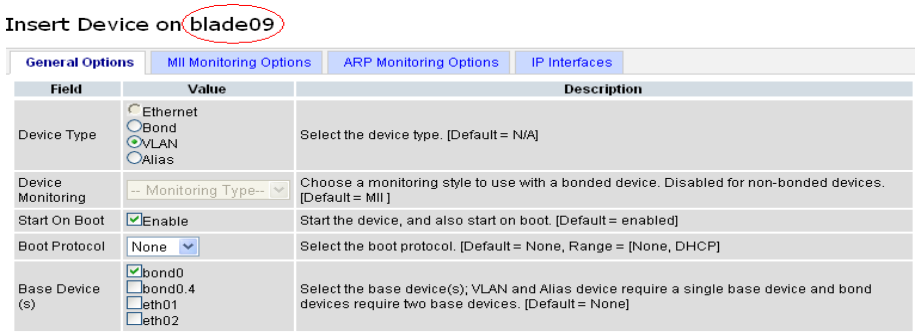
You should see several tabs each representing a blade in the system. Click on the tab representing the first MP Blade.



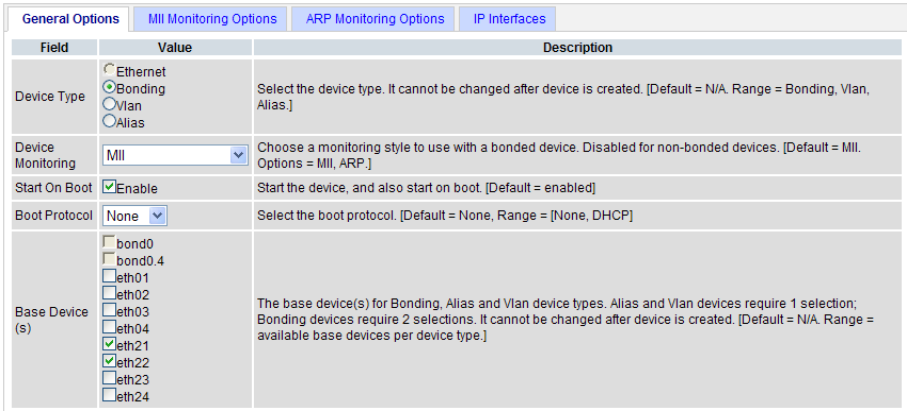
Refer to the following table to determine which steps to execute next based on the number of enclosure switch pairs and whether Bonded Interfaces are used

Nb of Enclosure Switch Pairs	Bonded Interface	Steps to Execute
1	N/A	2 and 5
2 or 3	Yes	3 and 5
2 or 3	No	4 and 5

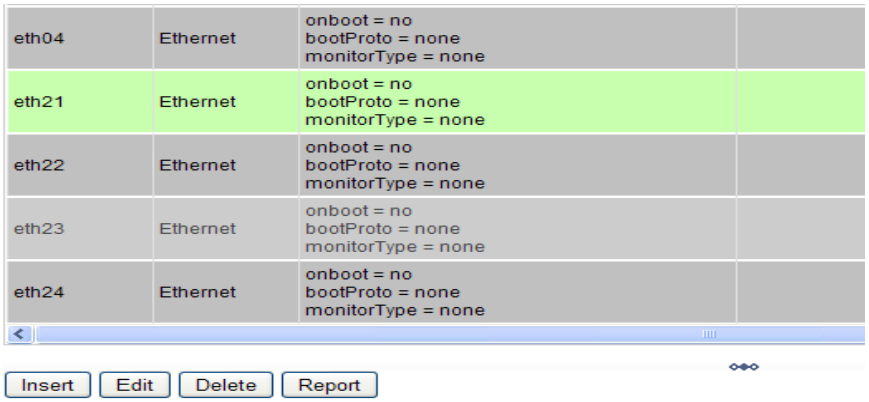
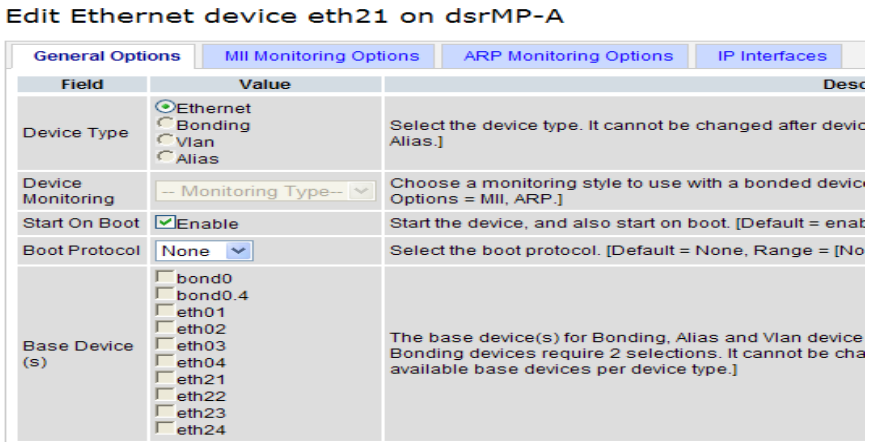
Procedure 46. Configure the Signaling Devices

2 ☐	**NOAMP VIP:** Configure the Signaling Interfaces of the MP (1 pair of enclosure switches)	Click on **Insert**. The following screen should be displayed. Verify that the blade name on the top corresponds to the MP.  For `Device Type`, select `VLAN`. For `Start on Boot`, verify that the checkbox is selected. For `Boot Protocol`, verify that it is set to None For `Base Device`, select `bond0`. Now Click on the **IP Interfaces** tab as shown below.  Now Click on **Add Row**, the following will be displayed  Select the first Signaling Network from the drop down menu. If configuring an IPv4, then enter the IPv4 address. If configuring an IPv6 address and IPv6 auto-configuration is enabled on your signaling network, and the MPs are in active/standby configuration, then there's no need to enter an IP address, it will be assigned automatically. If configuring an IPv6 address and IPv6 auto-configured is disabled, or the MPs are in multi-active mode: • If an IPv4 already exists, click on "Add Row" and enter the IPv6 address. • If an IPv4 doesn't exist, simply enter the IPv6 address. Click on **Ok** at the bottom of the screen.  To add additional Signaling Interfaces, click on Insert again and repeat this step, otherwise continue with the next step. Skip the next 2 steps and continue to step 5

Procedure 46. Configure the Signaling Devices

3 ☐	**NOAMP VIP:** Configure the Signaling Interfaces of the MP (multiple pairs of enclosure switches with bonded interfaces)	Click on **Insert**. The following screen should be displayed. Verify that the blade name on the top corresponds to the MP.  General Options | MII Monitoring Options | ARP Monitoring Options | IP Interfaces Field / Value / Description Device Type: Ethernet, Bonding, Vlan, Alias — Select the device type. It cannot be changed after device is created. [Default = N/A. Range = Bonding, Vlan, Alias.] Device Monitoring: MII — Choose a monitoring style to use with a bonded device. Disabled for non-bonded devices. [Default = MII. Options = MII, ARP.] Start On Boot: Enable — Start the device, and also start on boot. [Default = enabled] Boot Protocol: None — Select the boot protocol. [Default = None, Range = [None, DHCP] Base Device (s): bond0, bond0.4, eth01, eth02, eth03, eth04, eth21, eth22, eth23, eth24 — The base device(s) for Bonding, Alias and Vlan device types. Alias and Vlan devices require 1 selection; Bonding devices require 2 selections. It cannot be changed after device is created. [Default = N/A. Range = available base devices per device type.] For `Device Type`, select Bonding. For `Device Monitoring`, select `MII`. For `Start on Boot`, verify that the checkbox is selected. For `Boot Protocol`, verify that it is set to None For `Base Device`, select the ports that correspond to the signaling enclosure switches. (e.g. if the signaling switches are in Slots 3 and 4, you would select eth11 and eth12) Click on **Ok** at the bottom of the screen.  Ok Apply Cancel Next click **Insert** again. The same screen as above with appear, select the following: For `Device Type`, select `VLAN`. For `Start on Boot`, verify that the checkbox is selected. For `Boot Protocol`, verify that it is set to None For `Base Device`, select `bond1`. Now Click on the **IP Interfaces** tab as shown below.  Insert Device on blade09 General Options | MII Monitoring Options | ARP Monitoring Options | IP Interfaces IP Address List: Add Row Now Click on **Add Row**, the following will be displayed  IP Address List: Add Row XSI1 Remove Select the first Signaling Network from the drop down menu. Enter the IP address that corresponds to the IPv4 or IPv6 interface.

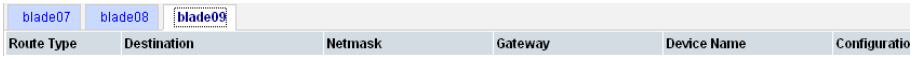
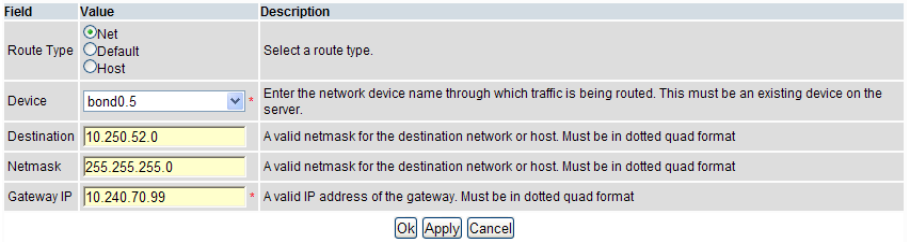
Procedure 46. Configure the Signaling Devices

		Click on **Ok** at the bottom of the screen.  To add additional Signaling Interfaces, click on Insert again and repeat this step, otherwise continue with the next step. Skip the next step and continue to step 5
4 ☐	**NOAMP VIP:** Configure the Signaling Interfaces of the MP (multiple pairs of enclosure switches without bonded interfaces)	Select `eth21` and click on **Edit**.  The following screen should be displayed. Verify that the blade name on the top corresponds to the MP. 

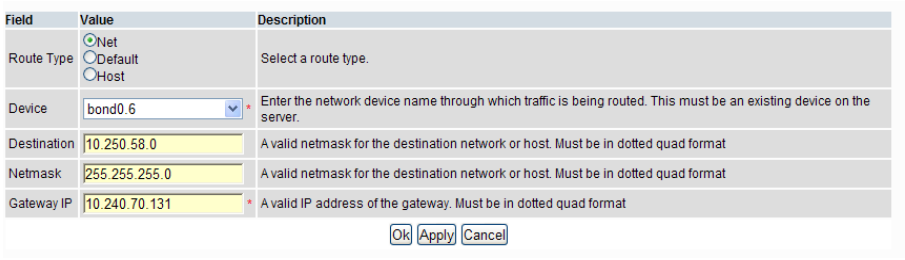
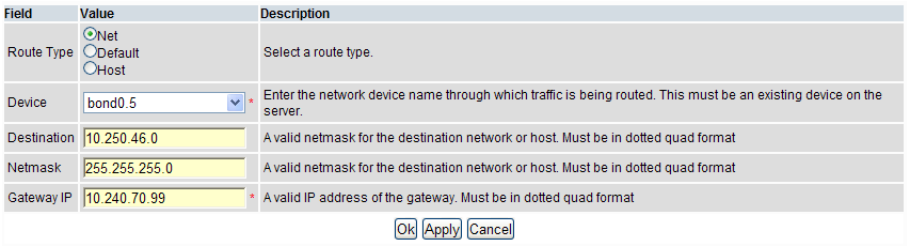
Procedure 46. Configure the Signaling Devices

		For "Start on Boot", verify that the checkbox is selected. For "Boot Protocol", verify that "None" is selected Now Click on the **IP Interfaces** tab as shown below.  Now Click on **Add Row**, the following will be displayed  Select the first Signaling Network from the drop down menu. Enter the IP address that corresponds to the IPv4 or IPv6 interface. Click on Ok at the bottom of the screen.  Now repeat this step to configure the second signaling interface (eth22). Skip the next step and continue to step 6
5 ☐	**NOAMP VIP:** Configure the Interfaces of the other MPs.	Repeat this procedure to configure the signaling devices of all other MPs.

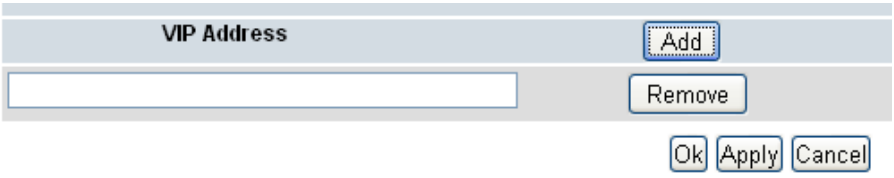
Procedure 47. Configure the Signaling Network Routes

S T E P	This procedure will provide the steps to configure the Signaling Network Routes Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**Establish GUI Session on the NOAMP VIP**	Establish a GUI session on the NOAMP by using the XMI VIP address. Login as user "guiadmin".
2 ☐	**NOAMP VIP:** Navigate to Server Configuration Screen	Navigate to **`Main Menu -> Configuration -> Network -> Routes`** Select the first MP Server Tab as shown. Initially no routes should be present. 
3 ☐	**NOAMP VIP:** Add Route	Click on **`Insert`** at the bottom of the screen to add additional routes. 
4 ☐	**NOAMP VIP:** Add Route for XSI-1	A similar screen will be displayed:  For `Route Type` Select `Net`, for `Device` select `bond0.5` (or bond 1.5, based on the chosen bond) For `Destination` enter the Network ID of the route destination (if rhis is an L3 deployment, this would be Ext-XSI1). For `Netmask` enter the corresponding Netmask. For `Gateway IP` enter the Int-XSI1 switch VIP. Press **`Ok.`**

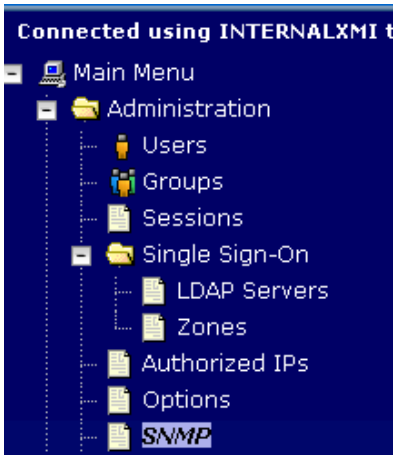
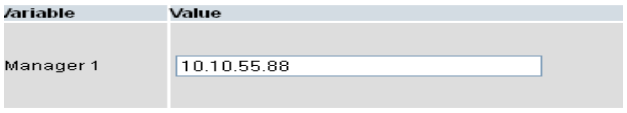
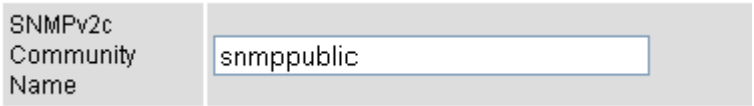
Procedure 47. Configure the Signaling Network Routes

5 ☐	**NOAMP VIP:** Add Route for XSI-2	Click on **Insert** again  For Route Type Select Net, for Device select bond0.6, (or bond 1.6, based on the chosen bond) For Destination enter the Network ID of the route destination (if rhis is an L3 deployment, this would be Ext-XSI2). For Netmask enter the corresponding Netmask. For Gateway IP enter the Int-XSI2 switch VIP. Press **Ok.**
6 ☐	**NOAMP VIP:** Add Additional Routes	If the peers are on a different Network than the Signaling Networks. Additional Routes need to be added to point to those networks. Click on **Add** again  For Route Type Select Net, for Device select the appropriate interface that will be used to connect to that network (bond0.5 or bond0.6), For Destination enter the Network ID of Network to which the peer node is connected to. For Netmask enter the corresponding Netmask. For Gateway IP enter the Int-XSI switch VIP of the chosen Network (either of int-XSI-1 or of int-XSI2). Press **Ok.** Note that if Aggregation switches are used, it may be necessary to add the routes above to the aggregation switches as well. This can be done by editing the 4948E_configure.xml file and adding the routes to it, and re-running netconfig.
7 ☐	Repeat for additional MPs.	Repeat Steps 2 through 6 for any additional MPs.

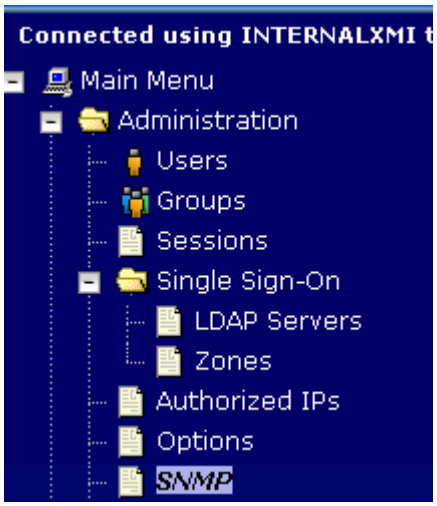
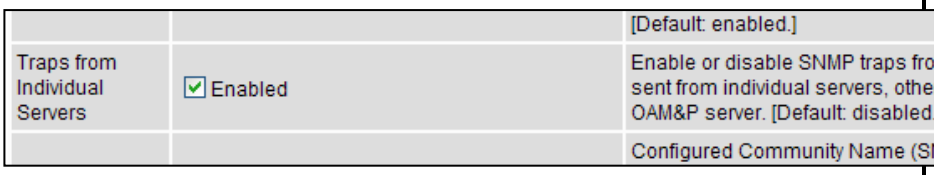
Procedure 48. Add VIP for Signaling Networks (Active/Standby Configurations ONLY)

S T E P #	This procedure will provide the steps to configure the VIPs for the signaling networks on the MPs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**Edit the MP Server Group and add VIPs** **(ONLY FOR 1+1)**	**IF YOUR MPs ARE IN A DSR MULTI-ACTIVE CLUSTER SERVER GROUP CONFIGURATION (N+0), THEN SKIP THIS STEP** From the GUI **Main Menu**->**Configuration**->**Server Groups**, select the MP server group, and then select **Edit**. Click on **Add** to add the VIP for XSI1 Enter the VIP of int-XSI-1 and click on **Apply.** Click on **Add** again to add the VIP for XSI2 Enter the VIP of int-XSI-2 and click on **Apply.** If more Signaling networks exists, add their corresponding VIP addresses . Finally Click on **Ok**. 

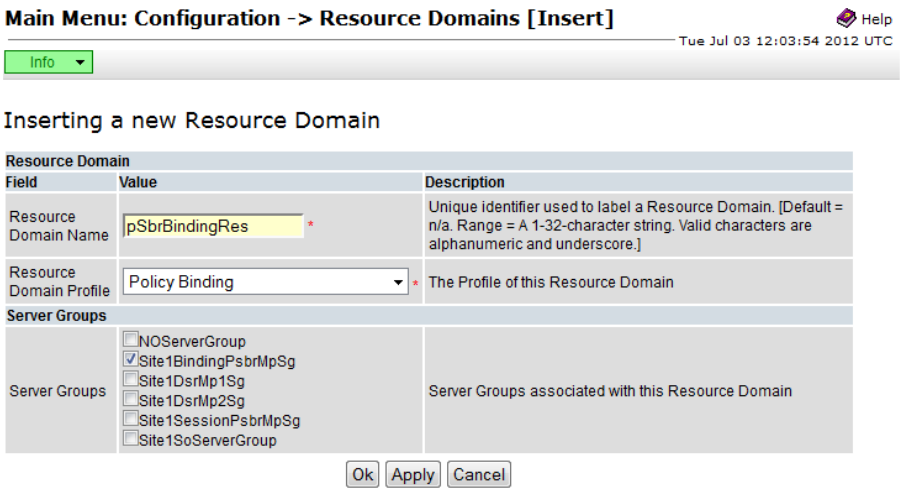
Procedure 49. Configure SNMP Trap Receiver(s) (OPTIONAL)

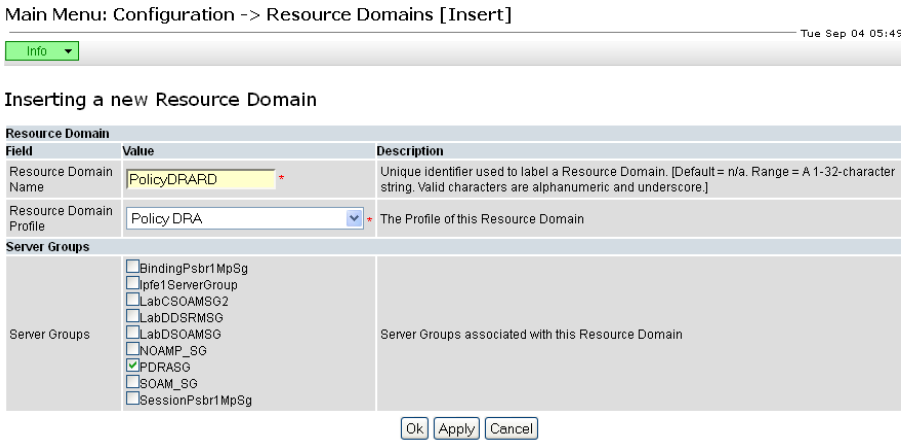
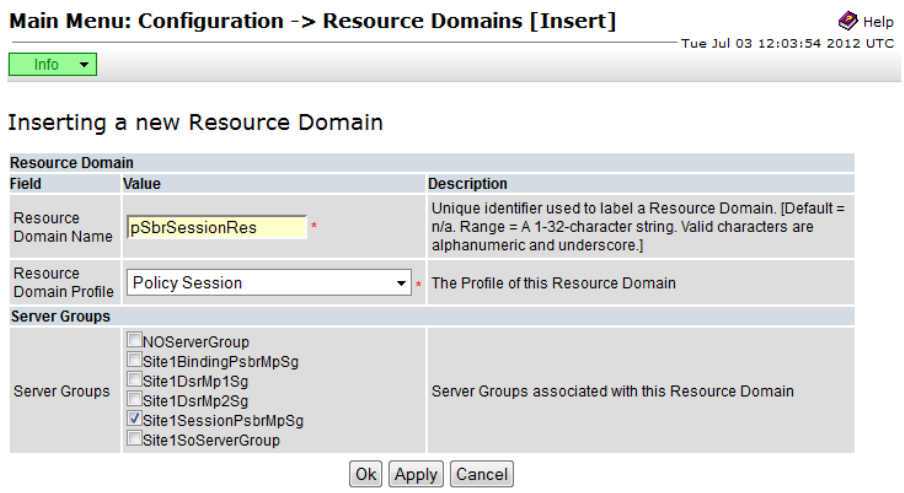
S T E P #	This procedure will provide the steps to configure forwarding of SNMP Traps from each individual server. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**NOAMP VIP:** Configure System-Wide SNMP Trap Receiver(s)	Using a web browser, log onto the NOAMP VIP and navigate to **Main Menu** -> **Administration** -> **SNMP**, as shown below  Verify that "Traps Enabled" is checked:  Fill in the IP address or hostname of the Network Management Station (NMS) you wish to forward traps to. This IP should be reachable from the the NOAMP's "XMI" network. Continue to fill in additional secondary, tertiary, etc.. manager IPs in the corresponding slots if desired.  Enter the SNMP community name:  Leave all other fields at their default values. Press **OK**

Procedure 49. Configure SNMP Trap Receiver(s) (OPTIONAL)

2 ☐	**NOAMP VIP:** Enable Traps from Individual Servers (OPTIONAL)	**NOTE:** By default snmp traps from MPs are aggregated and then displayed at the active NOAMP. If instead, you wish for every server to send its own traps directly to the NMS, then execute this procedure. **This procedure requires that all servers, including MPs, have an XMI interface on which the customer SNMP Target server (NMS) is reachable**. ---------- Using a web browser, log onto the NOAMP VIP and navigate to **Main Menu** -> **Administration** -> **SNMP**, as shown below  Make sure the checkbox next to "Enabled" is checked, if not, check it as shown below  Then click on **Apply** and verify that the data is committed.

Procedure 50:PDRA Resource Domain Configuration

S T E P #	This procedure configures the Resource Domain Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. SHOULD THIS PROCEDURE FAIL, CONTACT TEKELEC TECHNICAL SERVICES AND **ASK FOR EAGLE XG TAC.** **ASSUMPTION: POLICY DRA FEATURE IS ALREADY ACTIVATED USING WI006835.**	
1 ☐	Establish GUI Session on the NOAMP VIP	Establish a GUI session on the NOAMP by using the XMI VIP address. Login as user "guiadmin".
2 ☐	**NOAMP VIP:** Navigate to Resource Domain Screen	Navigate to **Main Menu -> Configuration -> Resource Domains** Screen.
4 ☐	**NOAMP VIP:** Add Binding Resource Domain	Click on **Insert** in the lower left corner. You will see a screen similar to:  Enter the Binding Resource Domain Name, select "Policy Binding" as the Resource Domain Profile and select the Server Groups associated with the Resource Domain and Press **Ok**.

5	**NOAMP VIP:** Add Policy DRA Resource Domain	Click on **Insert** in the lower left corner. You will see a screen similar to:  Enter the Resource Domain Name, select “Policy DRA” as the Resource Domain Profile and select the Server Groups associated with the Resource Domain and Press **Ok**. NOTE: **For Mated Pair DSR, create only one PDRA Resource Domain and add the DA-MP Server Groups from both sites into this PDRA Resource Domain.** **For non-mated pair DSRs and standalone DSR: Create a PDRA Resource Domain per Site.**
6	**NOAMP VIP:** Add Session Resource Domain	Click on **Insert** in the lower left corner. You will see a screen similar to:  Enter the Session Resource Domain Name, select “Policy Session” as the Resource Domain Profile and select the Server Groups associated with the Resource Domain and Press **Ok**.

7 ☐	**NOAMP VIP:** Add other Session Resource Domains.	Repeat Step 6 for all other Session Resource Domains that are to be added.
8 ☐	**NOAMP VIP:** Restart PDRA MP servers	From the NOAMP GUI, select the **Main menu**->**Status & Manage**->**Server menu** *For each PDRA MP server:* • Select the MP server. • Select the **Restart** button. • Answer **OK** to the confirmation popup. Wait for the message which tells you that the restart was successful.

4.18 Post-Install Activities

Procedure 51. Activate Optional Features

S T E P #	This procedure will provide instruction on how to install DSR optional components once regular installation is complete. **Prerequisite:** All previous DSR installation steps have been completed. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**Refer to Activation Guides for Optional Features**	Refer to 3.3 **Optional Features** for a list of feature activation documents whose procedures are to be executed at this moment.

Procedure 52. Configure ComAgent Connections

S T E P #	This procedure will provide instruction on how to configure ComAgent connections on DSR for use in the FABR application. **Prerequisite:** FABR application is activated. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	
1 ☐	**Configure ComAgent**	Refer to [5] for the steps required to configure ComAgent

APPENDIX A. SAMPLE NETWORK ELEMENT AND HARDWARE PROFILES

In order to enter all the network information for a network element into an Appworks-based system, a specially formatted XML file needs to be filled out with the required network information. The network information is needed to configure both the NOAMP and any SOAM Network Elements.

It is expected that the maintainer/creator of this file has networking knowledge of this product and the customer site at which it is being installed. This network element XML file is used for DSR deployments using Cisco 4948 switches and HP c-Class blade servers. The following is an example of a Network Element XML file.

The SOAM Network Element XML file needs to have same network names for the networks as the NOAMP Network Element XML file has. It is easy to accidentally create different network names for NOAMP and SOAM Network Element, and then the mapping of services to networks will not be possible.

The NTP server in the NOAM NE should point to the platmgmt or XMI IP of the TVOE host for best results. It is then assumed that the TVOE host's NTP points to an external (customer) source.

Example Network Element XML file:

```
<?xml version="1.0"?>
<networkelement>
    <name>NE</name>
    <ntpservers>
        <ntpserver>192.168.58.247</ntpserver>
        <ntpserver>1.1.1.1</ntpserver>
    </ntpservers>
    <networks>
        <network>
            <name>INTERNALXMI</name>
            <vlanId>3</vlanId>
            <ip>10.2.0.0</ip>
            <mask>255.255.255.0</mask>
            <gateway>10.2.0.1</gateway>
            <isDefault>true</isDefault>
        </network>
        <network>
            <name>INTERNALIMI</name>
            <vlanId>4</vlanId>
            <ip>10.3.0.0</ip>
            <mask>255.255.255.0</mask>
            <gateway>10.3.0.1</gateway>
            <isDefault>false</isDefault>
        </network>
    </networks>
</networkelement>
```

PDRA installs will have a separate network defined for pSBR replication. The following example should be added to the <networks><//networks> section.for PDRA SO site NE XML files:

```
       <network>
            <name>PSBRREPLICATION</name>
            <vlanId>9</vlanId>
            <ip>10.2.5.0</ip>
            <mask>255.255.255.0</mask>
            <gateway>10.5.0.1</gateway>
            <isDefault>false</isDefault>
        </network>
```

The server hardware information is needed to configure the Ethernet interfaces on the servers. This server hardware profile data XML file is used for Appworks 4.0 deployments using HP c-Class blade servers and HP c-Class rack-mount servers. It is supplied to the NOAMP server so that the information can be pulled in by Appworks and presented to the user in the GUI during server configuration. The following is an example of a Server Hardware Profile XML file.

Example Server Hardware Profile XML file – HP c-Class blade:

```
<profile>
    <serverType>HP c-Class Blade</serverType>
    <available>
        <device>bond0</device>
    </available>
    <devices>
        <device>
            <name>bond0</name>
            <type>BONDING</type>
            <createBond>true</createBond>
            <slaves>
                <slave>eth01</slave>
                <slave>eth02</slave>
            </slaves>
          <option>
                <monitoring>mii</monitoring>
                <primary>eth03</primary>
                <interval>100</interval>
                <upstream_delay>200</upstream_delay>
                <downstream_delay>200</downstream_delay>
          </option>
        </device>
    </devices>
</profile>
```

Example Server Hardware Profile XML file – HP c-Class rack-mount server:

```
<profile>
    <serverType>HP Rack Mount</serverType>
    <available>
        <device>bond0</device>
        <device>bond1</device>
    </available>
    <devices>
        <device>
            <name>bond0</name>
            <type>BONDING</type>
            <createBond>true</createBond>
            <slaves>
                <slave>eth01</slave>
                <slave>eth03</slave>
            </slaves>
            <option>
                <monitoring>mii</monitoring>
                <primary>eth01</primary>
                <interval>100</interval>
                <upstream_delay>200</upstream_delay>
                <downstream_delay>200</downstream_delay>
            </option>
        </device>
```

```
        <device>
            <name>bond1</name>
            <type>BONDING</type>
            <createBond>true</createBond>
            <slaves>
                <slave>eth11</slave>
                <slave>eth12</slave>
            </slaves>
            <option>
                <monitoring>mii</monitoring>
                <primary>eth11</primary>
                <interval>100</interval>
                <upstream_delay>200</upstream_delay>
                <downstream_delay>200</downstream_delay>
            </option>
        </device>
    </devices>
</profile>
```

Example Server Hardware Profile XML file – Virtual Guest on TVOE:

```
<profile>
    <serverType>TVOE Guest</serverType>
    <available>
        <device>eth0</device>
        <device>eth1</device>
        <device>eth2</device>
        <device>eth3</device>
        <device>eth4</device>
    </available>
    <devices>
        <device>
            <name>eth0</name>
            <type>ETHERNET</type>
        </device>
        <device>
            <name>eth1</name>
            <type>ETHERNET</type>
        </device>
        <device>
            <name>eth2</name>
            <type>ETHERNET</type>
        </device>
        <device>
            <name>eth3</name>
            <type>ETHERNET</type>
        </device>
        <device>
            <name>eth4</name>
            <type>ETHERNET</type>
        </device>
    </devices>
</profile>
```

APPENDIX B. CONFIGURING FOR EAGLE XG TVOEILO ACCESS

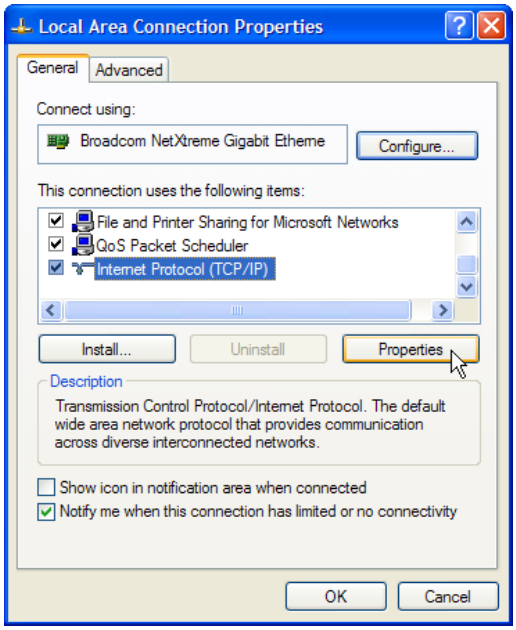
This procedure contains the steps to connect a laptop to the TVOEiLO via a directly cabled Ethernet connection. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

Procedure B.1 Connecting to the EAGLE XG TVOE iLO

<table>
<tr><th>Step</th><th>Procedure</th><th colspan="2">Result</th></tr>
<tr><td rowspan="2">1. ☐</td><td rowspan="2">Access the laptop network interface card's TCP/IP "Properties" screen.

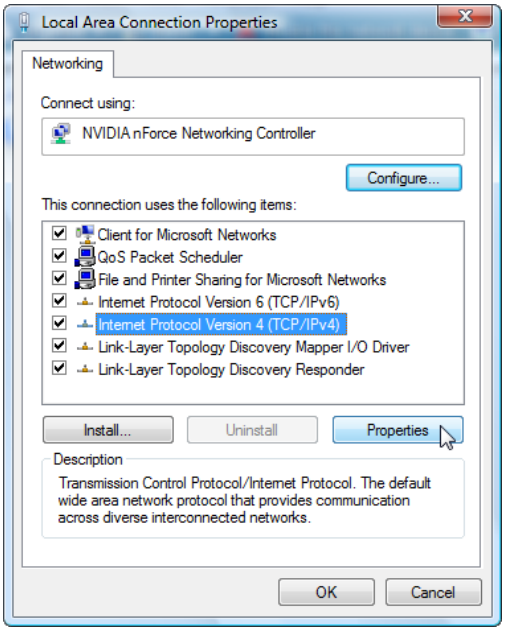
NOTE: For this step follow the instruction specific to the laptop's OS (XP or Vista).</td><th>Windows XP</th><th>Windows Vista</th></tr>
<tr>
<td>

Go to Control Panel
Double-click on Network Connections
Right-click the wired Ethernet Interface icon and select "Properties"
Select "Internet Protocol (TCP/IP)" and select "Properties"



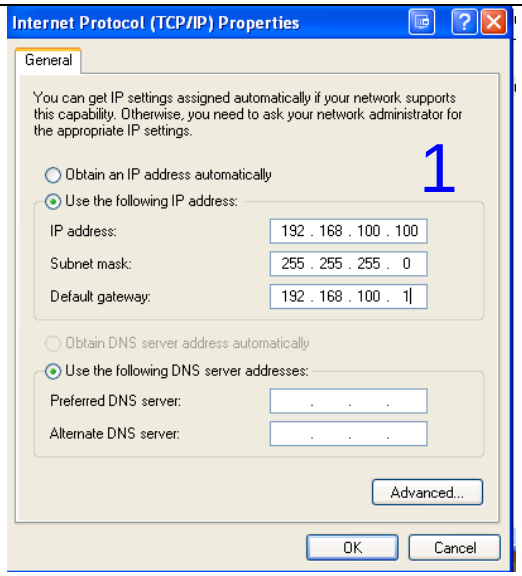
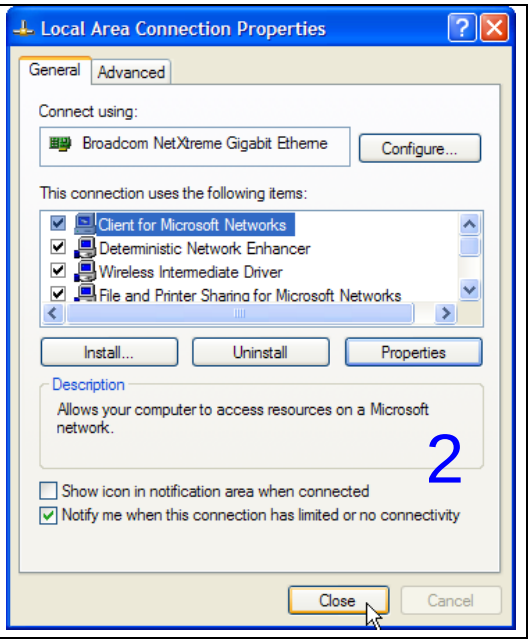
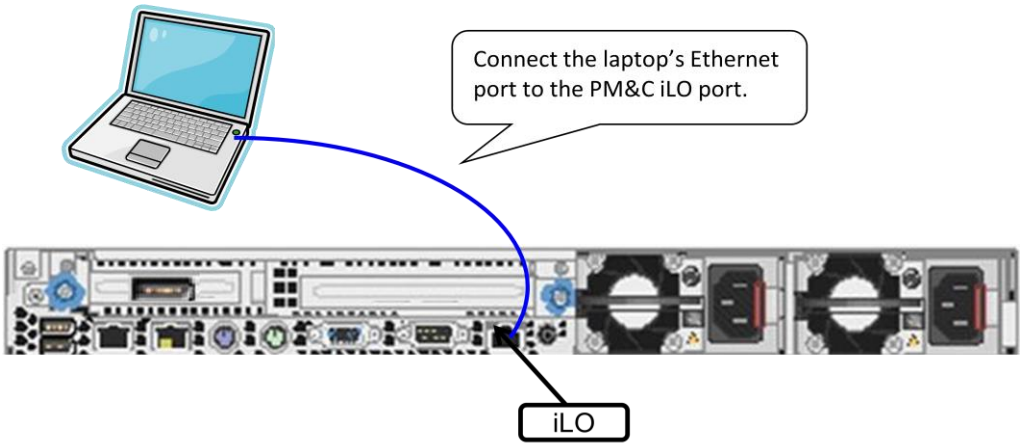
</td>
<td>

Go to Control Panel.
Double-click on Network and Sharing Center
Select Manage Network Connections (left menu)
Right-click the wired Ethernet Interface icon and select "Properties"
Select "Internet Protocol Version 4 (TCP/IPv4)"



</td>
</tr>
</table>

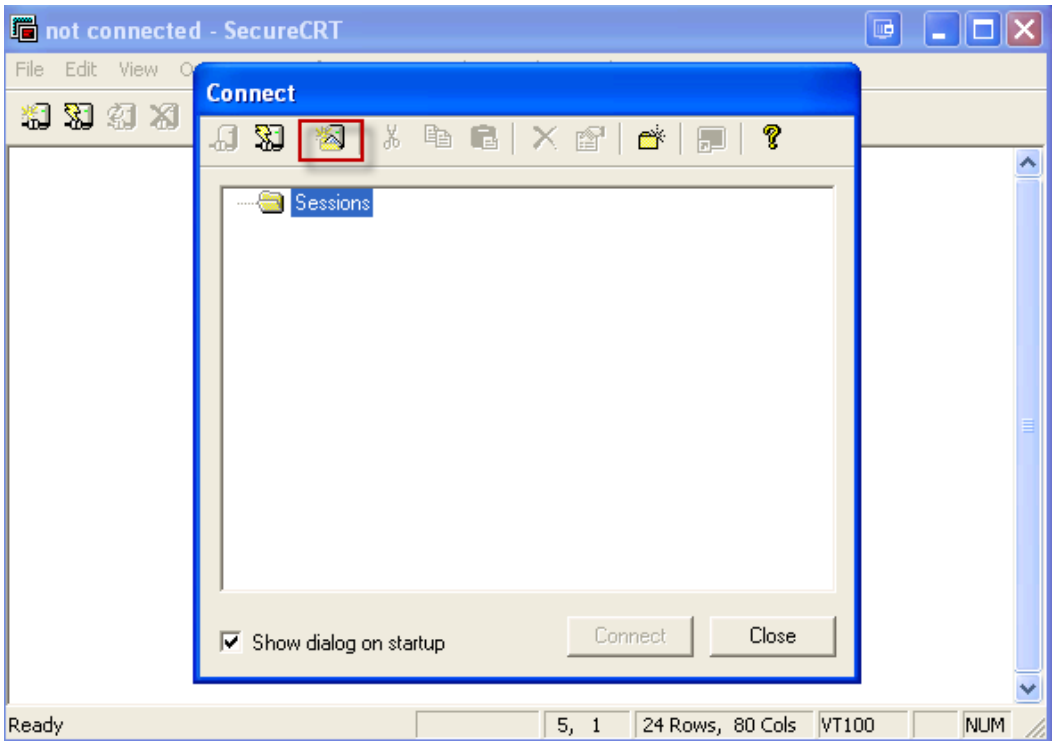
Procedure B.1 Connecting to the EAGLE XG TVOE iLO

2. ☐	**1)** Clock "**use the following IP address**", set the **IP address** to "192.168.100.100", the **Subnet mask** to "255.255.255.0" and th **Default gateway** to "192.168.100.1", click **"OK"**. 2) Click **"Close"** from the network interface card's main "Properties" screen.	 
3. ☐	Connect the laptop's Ethernet port directly to the TVOE iLO port using a standard Cat-5 cross-over cable.	
THIS PROCEDURE HAS BEEN COMPLETED		

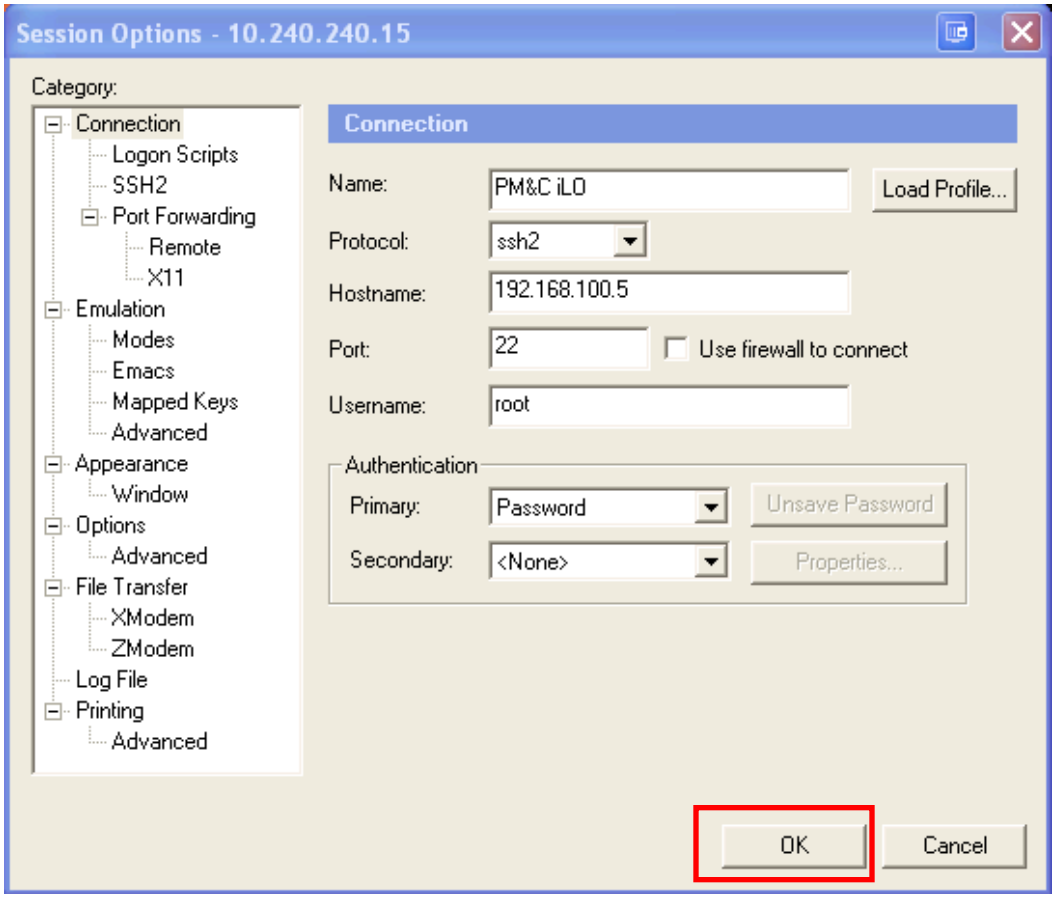
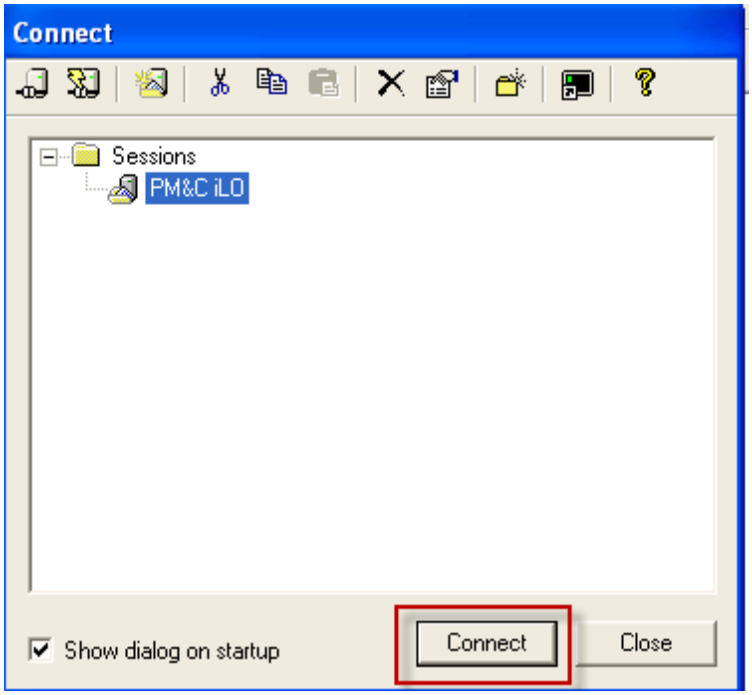
APPENDIX C. TVOE ILO ACCESS

This procedure contains the steps to access the TVOE iLO. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

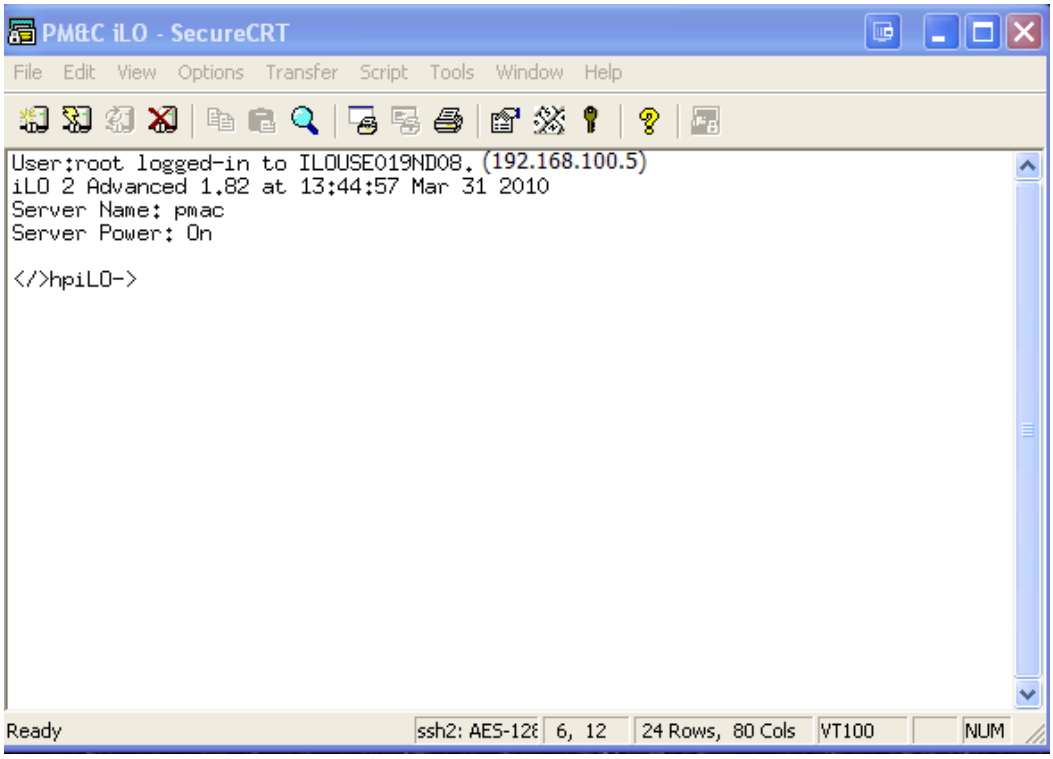
Procedure C.1 Accessing the TVOE iLO

Step	Procedure	Result
1. ☐	Launch a terminal emulator, e.g. Putty, Secure CRT. Navigate to **File=> Connect** Click on the "**New Session**" icon. Note: This example demonstrates Secure CRT.	

Procedure C.1 Accessing the TVOE iLO

2. ☐	Enter **TVOE iLO** for 'Name' and **192.168.100.5**(manufacturing default) or customer IP set during installation for 'Hostname'. Enter **root** for Username. Click **OK** **NOTE 1** *See **Appendix B** to configure your system network to access the EAGLE XG.* .	
3. ☐	Navigate **FILE => Connect** to open the Connect window. Highlight the session you created and click **Connect.**	

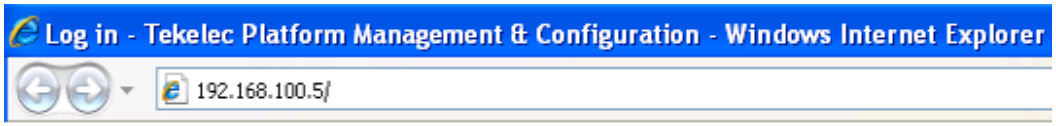
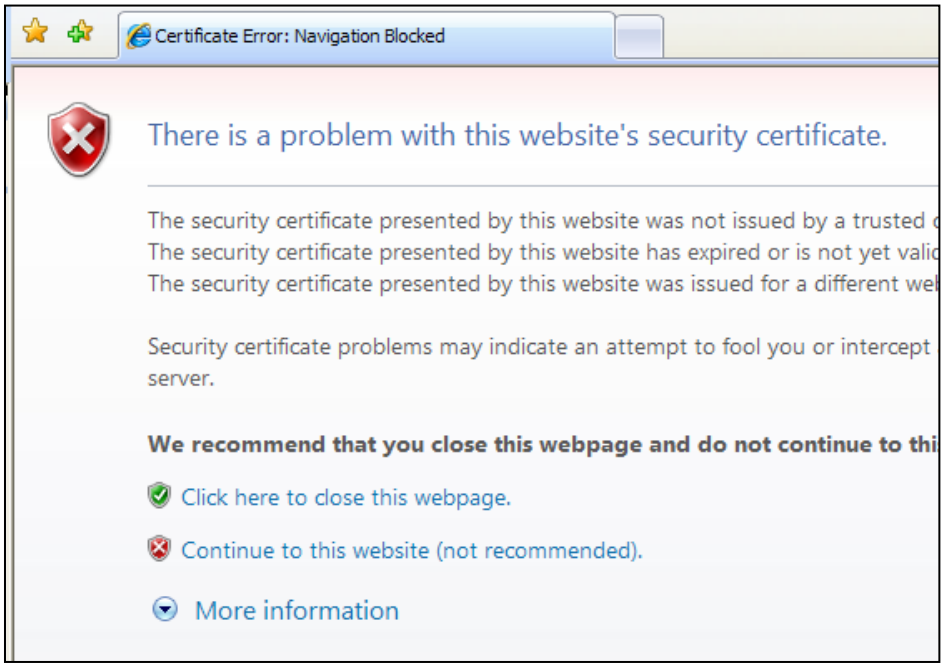
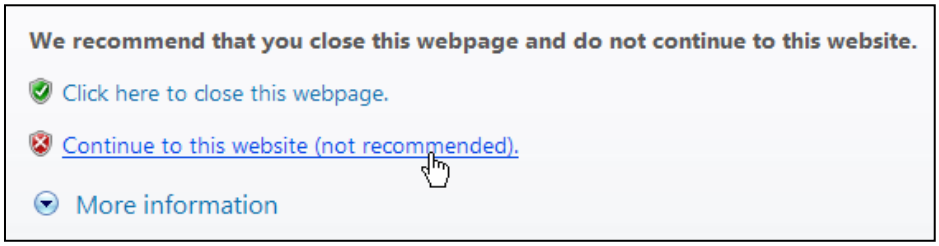
Procedure C.1 Accessing the TVOE iLO

4. ☐	Login to the TVOE iLO using the appropriate password.	
5. ☐	The TVOE iLO is displayed.	
THIS PROCEDURE HAS BEEN COMPLETED		

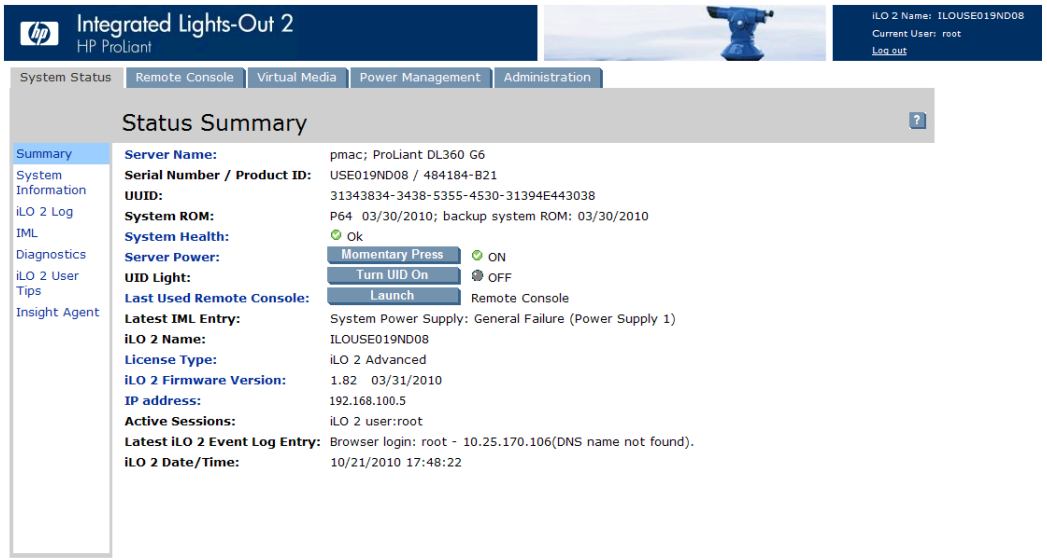
APPENDIX D. TVOE ILO GUI ACCESS

This procedure contains the steps to access the TVOE iLO GUI. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

Procedure D.1 Accessing the TVOE iLO GUI

Step	Procedure	Result
1. ☐	Launch Internet Explorer and "Go To" 192.168.100.5 (manufacturing default) or customer IP set during installation.	
2. ☐	Internet Explorer may display a warning message regarding the Security Certificate.	
3. ☐	Select the option to "Continue to the website (not recommended)"	

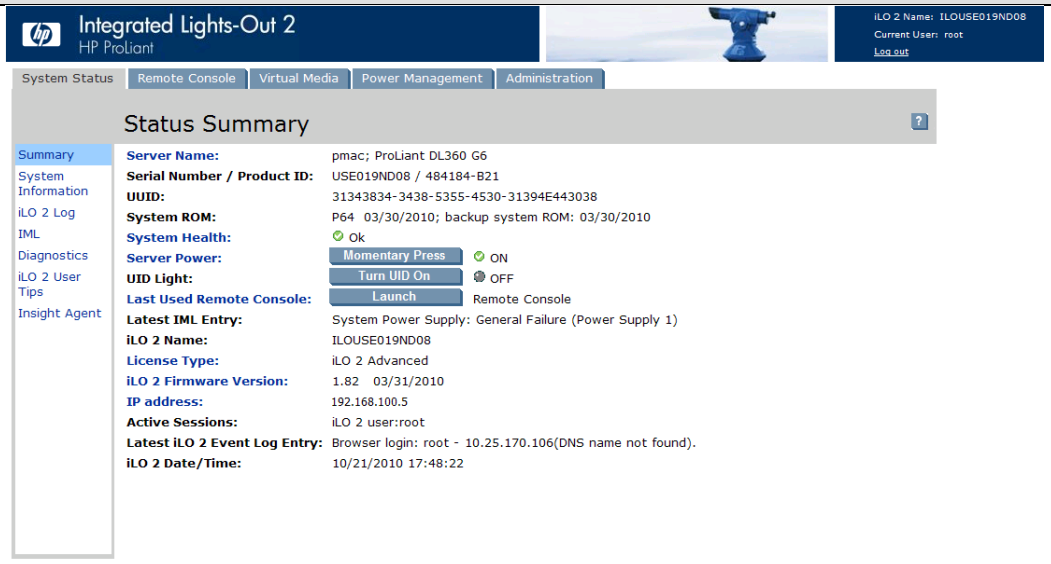
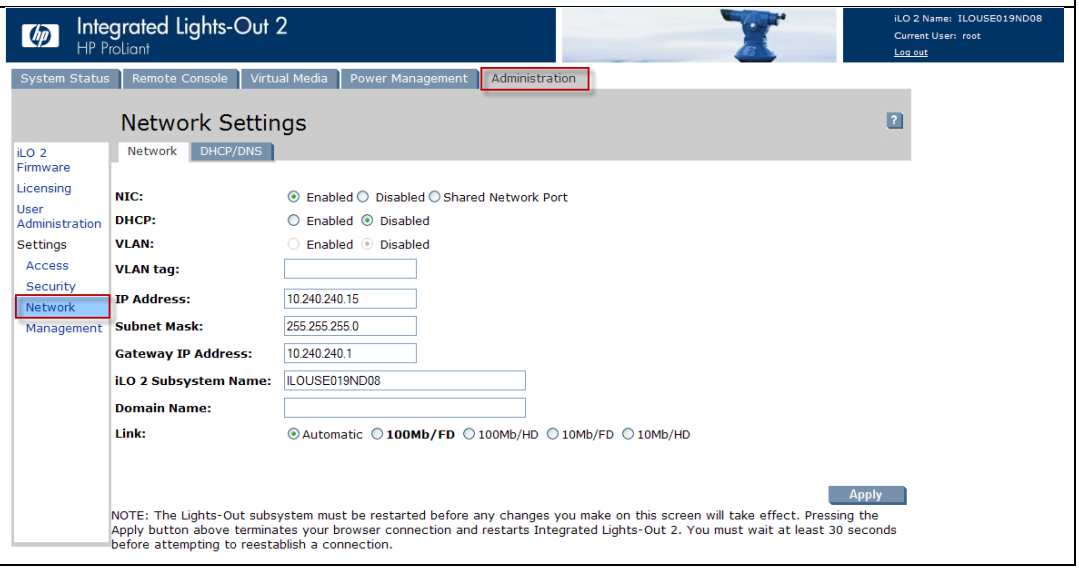
Procedure D.1 Accessing the TVOE iLO GUI

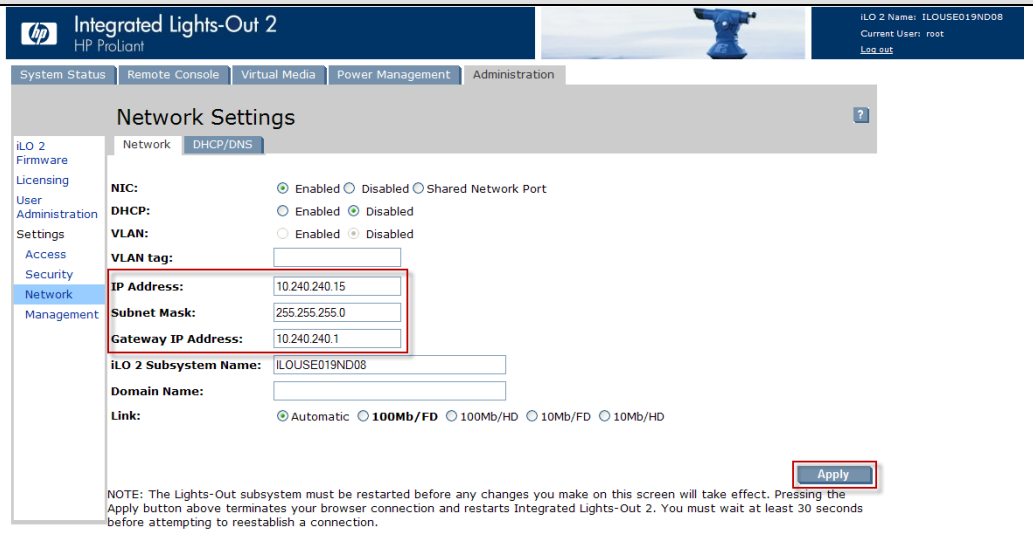
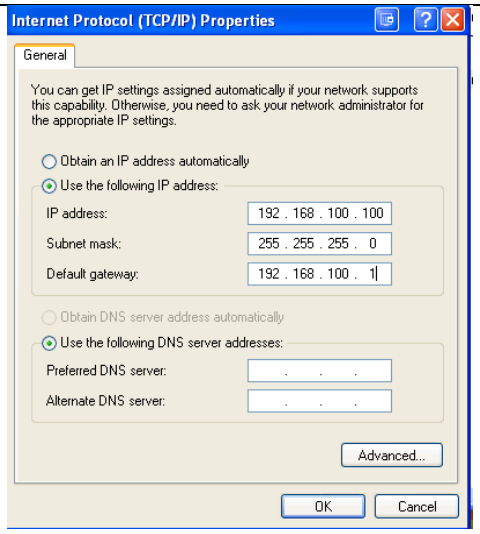
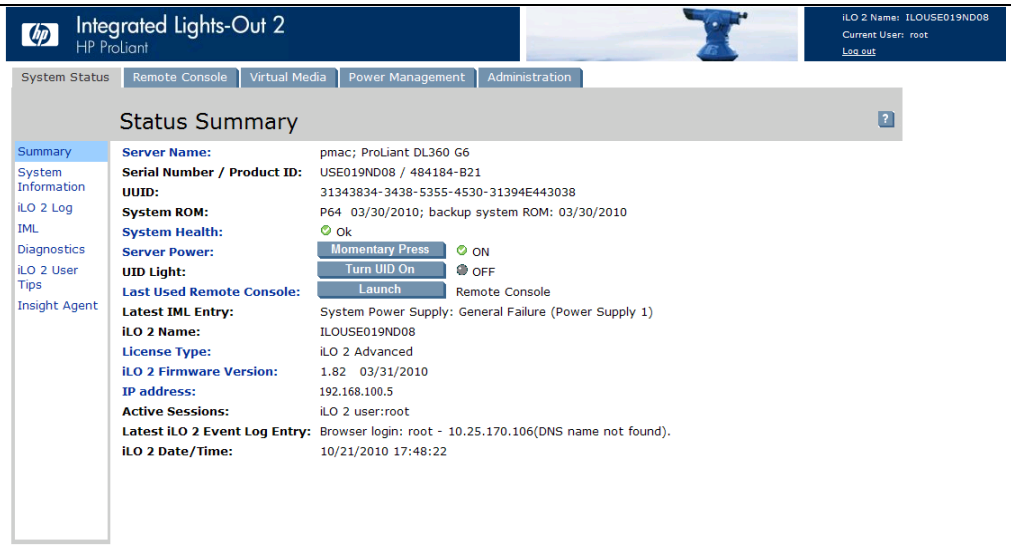
4. ☐	Log in as user "**root**".	
5. ☐	The TVOE iLO Home page is displayed.	
6. ☐	Click on Launch to start the pmac iLO CLI	
THIS PROCEDURE HAS BEEN COMPLETED		

APPENDIX E. CHANGING TVOE ILO ADDRESS

This procedure will set the IP address of the TVOE iLO to the customers network so that it can be accessed by Tekelec support.

Procedure E.1 Accessing the TVOE iLO GUI

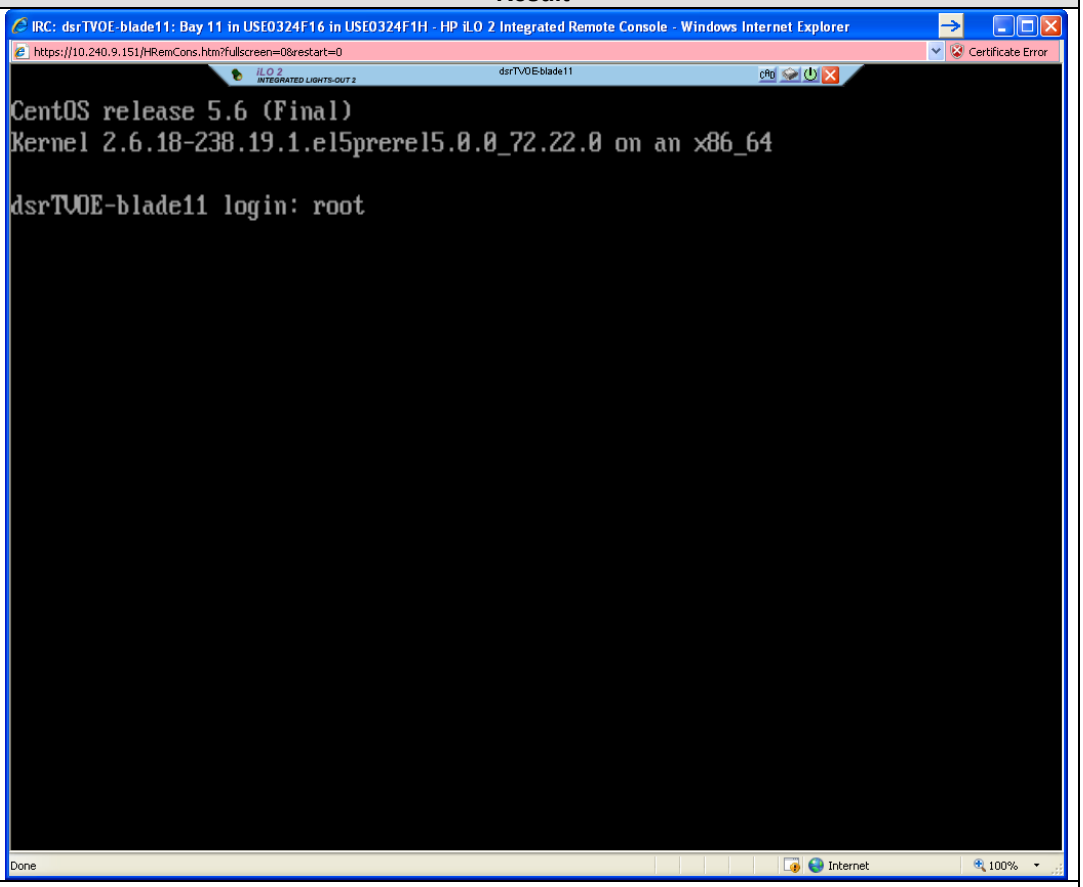
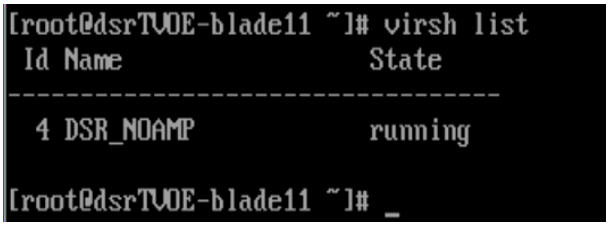
Step	Instruction	Result
1. ☐	Connect to the TVOE iLO GUI using the instructions in **Appendix D**	
2. ☐	Click the "**Administration**" tab. Under "**Settings**" in the left column click on "**Network**".	

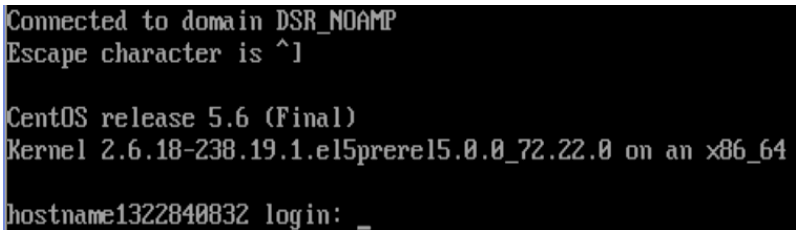
Step	Instruction	Result
3. ☐	Change the **IP Address**, **Subnet Mask** and **Gateway IP Address** to the values supplied in the IP Site Survey for the TVOE iLO. Hit **Apply**. NOTE: You will lose access after you hit the Apply button.	
4. ☐	Using the instructions found in **Appendix B, reset** the PC's network connection replacing the **Subnet Mask** and **Gateway** with those just used for the TVOE iLO. Use an appropriate **IP address** for this subnet. Call Customer Support if needed.	
5. ☐	Connect to the TVOE iLO GUI using the instructions in **Appendix D** **Note**: Use the IP address entered in Step 3 and not the 192.168.100.5.	

THIS PROCEDURE HAS BEEN COMPLETED

APPENDIX F. PM&C/NOAMP/SOAM CONSOLE ILO ACCESS

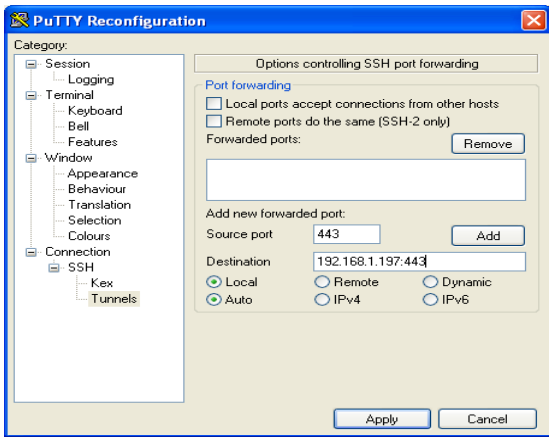
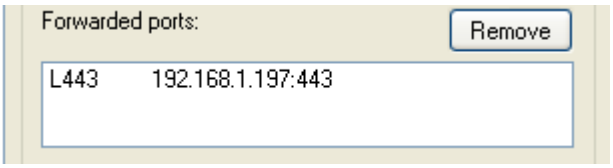
This procedure describes how to log into the PM&C/NOAMP/SOAMP console from ILO.

Step	Instruction	Result
1. ☐	Log In as **root** on the TVOE server hosting the NOAMP using either ILO or SSH to the TVOE server's XMI address	
2. ☐	Find the NOAMP's current VM number	On the TVOE host, execute:. #**virsh list** This will produce a listing of currently running virtual machines.  Find the VM name for your DSR NOAMP and note it's ID number in the first column. **NOTE**: If the VM state is not listed as "running" or you do not find a VM you configured for your NOAMP at all, then halt this procedure and contact Tekelec Customer Support.

Step	Instruction	Result
3. ☐	Connect to console of the VM using the VM number obtained in Step 2.	On the TVOE host, execute:. #**virsh console <DSRNOAMP-VMID>** Where **DSRNOAMP-VMID** is the VM ID you obtained in Step 2:  You are now connected to the DSR NOAMPs console. If you wish to return to the TVOE host, you can exit the session by pressing **CTRL +]**

APPENDIX G. ACCESSING THE NOAMP GUI USING SSH TUNNELING WITH PUTTY

S T E P	**NOTE**: This procedure assumes that the NOAMP server you wish to create a tunnel to has been IPM'ed with the DSR application ISO **NOTE**: This procedure assumes that you have exchanged SSH keys between the PMAC and the first NOAMP server. **NOTE:** This procedure assumes that you have obtained the control network IP address for the first NOAMP server. You can get this from the PMAC GUI's *Software Inventory* screen. That variable will be refered to as *NOAMP-Control-IP* in thiese instructions. **NOTE:** It is recommended that you only use this procedure if you are using Windows XP. There are known issues with putty and Windows 7 that may cause unpredictable results when viewing GUI screens through SSH tunnels.	
1 ☐	**Logon to PMAC Server using PuTTY**	Launch the PuTTY application from your station and open a session to the PMAC's management address, logging in as "root".

2 ☐	**Create SSH Tunnel through the PMAC in PuTTY**	 Click the icon in the upper left hand corner of the PuTTY window to bring down the main menu. Select ***Change Settings*** Select ***Connections -> SSH -> Tunnels***  1. Verify that the **Local** and **Auto** radio buttons are selected. Leave other fields blank **2.** In *Source Port*, enter **443** 3. In *Destination*, enter ***<NOAMP-Control-IP>*:443** 4. **Click Add**  You should now see a display similar to the following in the text box at the center of this dialog. 5. **Click Apply**

3 ☐	**Use Local Web Browser to Connect to GUI**	Using your web browser, navigate to the URL: **`https://localhost/`**  You should arrive at the login screen for the NOAMP GUI. Note that if using windows 7 and a blank screen is displayed, enable "Comptability Mode" in IE, or use a different browser (Firefox or Chrome) **This procedure is now complete**

APPENDIX H. ACCESSING THE NOAMP GUI USING SSH TUNNELING WITH OPENSSH FOR WINDOWS

S T E P		
	NOTE: This procedure assumes that the NOAMP server you wish to create a tunnel to has been IPM'ed with the DSR application ISO **NOTE**: This procedure assumes that you have exchanged SSH keys between the PMAC and the first NOAMP server. **NOTE:** This procedure assumes that you have obtained the control network IP address for the first NOAMP server. You can get this from the PMAC GUI's *Software Inventory* screen. That variable will be refered to as *NOAMP-Control-IP* in thiese instructions. **NOTE**: **This is the recommended tunneling method if you are using Windows 7.**	
1 ☐	**If Needed, Download and Install *openssh* for Windows**	• Dowload ***oppenssh* for Windows** from here. • Extract the installer from the ZIP file, then run the installer. *openssh* is now installed on your PC.
2 ☐	**Create SSH Tunnel Through the PMAC**	• Open up a Command Prompt shell • Within the command shell, enter the following to create the SSH tunnel to the 1st NO, through the PMAC: > **ssh -L 443:<1st_NO_Control_IP_Address>:443 root@<PMAC_Management_IP_Address>** (Answer "yes" if it asks if you want to continue connecting) .  The tunnel to the first NOAMP is now established.
3 ☐	**Use Local Web Browser to Connect to GUI**	Using your web browser, navigate to the URL: **https://localhost/**  You should arrive at the login screen for the NOAMP GUI. **This procedure is now complete**

APPENDIX I. MANUAL TIMEZONE SETTING PROCEDURE

Procedure H.1 Timezome Setting

S T E P		
	NOTE: This procedure assumes that the first NO-AMP server has been initially configured and rebooted. **NOTE:** This procedure assumes that one system-wide time zone has been selected.	
1 ☐	**Access Active NOAMP Console**	Login as "root" to the Active NO-AMP console.
2 ☐	**Active NOAMP Console:** Execute time zone configuration script and verify successful result	From the command line prompt, execute *set_ini_tz.pl*. This will set the system time zone The following command example uses the America/New_York time zone. Replace as appropriate with the time zone you have selected for this installation. See Appendix K for a list of valid time zones. `# /usr/TKLC/appworks/bin/set_ini_tz.pl "America/New_York" >/dev/null 2>&1`
3 ☐	**Verify Success of Time Zone Script**	`# echo $?` **If this returns anything other than "0", then halt this procedure and contact Tekelec Customer Support.**

APPENDIX J. CONFIGURING A DSR SERVER FOR 2-TIER OAM

S T E P #	This procedure configures a single server to operate in 2-tier OAM mode Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. Should this procedure fail, contact the Tekelec Customer Care Center and ask for assistance.	
1 ☐	IPM the server with the proper TPD image.	Execute **Procedure 29 ("IPM Blades and VMs")** of *909-2228-001* for the server. Use the TPD image that corresponds to the DSR release you are using. When done, only the TPD image will be installed on the server.
2 ☐	Login to server using iLO or the control IP address as root and check for existence of 2-tier flag.	1. Login as root to the server using either o iLO facility o -OR- SSH to the server control IP address . You can get this IP from the PMAC' GUI's "Software Inventory" screen. You will then need to log into the PMAC as root and ssh into this IP address. 2. Execute the following command on the server: `touch /usr/TKLC/DsrDataAsourced` (if the command is successful, there will be no output)
3 ☐	Proceed with normal install starting with the Applicaion ISO IPM.	The server is now configured for 2-tier OAM. Proceed with installing the Application ISO (**Procedure 30** of *909-2228-001*) and further tasks.

APPENDIX K. LIST OF FREQUENTLY USED TIME ZONES

This table lists several valid timezone strings that can be used for the time zone setting in a CSV file, or as the time zone parameter when manually setting a DSR blade timezone. For an exhaustive list of **ALL** timezones, log onto the PMAC server console and view the text file: `/usr/share/zoneinfo/zone.tab`

Table 3. List of Selected Time Zone Values

Time Zone Value	Description	Universal Time Code (UTC) Offset
America/New_York	Eastern Time	UTC-05
America/Chicago	Central Time	UTC-06
America/Denver	Mountain Time	UTC-07
America/Phoenix	Mountain Standard Time - Arizona	UTC-07
America/Los_Angeles	Pacific Time	UTC-08
America/Anchorage	Alaska Time	UTC-09
Pacific/Honolulu	Hawaii	UTC-10
Africa/Johannesburg		UTC+02
America/Mexico_City	Central Time - most locations	UTC-06
Africa/Monrovia		UTC+00
Asia/Tokyo		UTC+09
America/Jamaica		UTC-05
Europe/Rome		UTC+01

Asia/Hong_Kong		UTC+08
Pacific/Guam		UTC+10
Europe/Athens		UTC+02
Europe/London		UTC+00
Europe/Paris		UTC+01
Europe/Madrid	mainland	UTC+01
Africa/Cairo		UTC+02
Europe/Copenhagen		UTC+01
Europe/Berlin		UTC+01
Europe/Prague		UTC+01
America/Vancouver	Pacific Time - west British Columbia	UTC-08
America/Edmonton	Mountain Time - Alberta, east British Columbia & westSaskatchewan	UTC-07
America/Toronto	Eastern Time - Ontario - most locations	UTC-05
America/Montreal	Eastern Time - Quebec - most locations	UTC-05
America/Sao_Paulo	South & Southeast Brazil	UTC-03
Europe/Brussels		UTC+01
Australia/Perth	Western Australia - most locations	UTC+08

Australia/Sydney	New South Wales - most locations	UTC+10
Asia/Seoul		UTC+09
Africa/Lagos		UTC+01
Europe/Warsaw		UTC+01
America/Puerto_Rico		UTC-04
Europe/Moscow	Moscow+00 - west Russia	UTC+04
Asia/Manila		UTC+08
Atlantic/Reykjavik		UTC+00
Asia/Jerusalem		UTC+02

APPENDIX L. APPLICATION NETBACKUP CLIENT INSTALLATION PROCEDURES

NetBackup is a utility that allows for management of backups and recovery of remote systems. The NetBackup suite is for the purpose of supporting Disaster Recovery at the customer site. The following procedures provides instructions for installing and configuring the NetBackup client software on an application server in two different ways, first using platcfg and second using nbAutoInstall (push Configuration)

Please not that at the writing of this document, the supported versions of Netbackup in DSR 4.0 are 7.1 and 7.5.

APPENDIX J.1. NETBACKUP CLIENT INSTALL USING PLATCFG

NOTE: Execute the following procedure to switch/migrate to having netBackup installed via platcfg instead of using NBAutoInstall (Push Configuration)

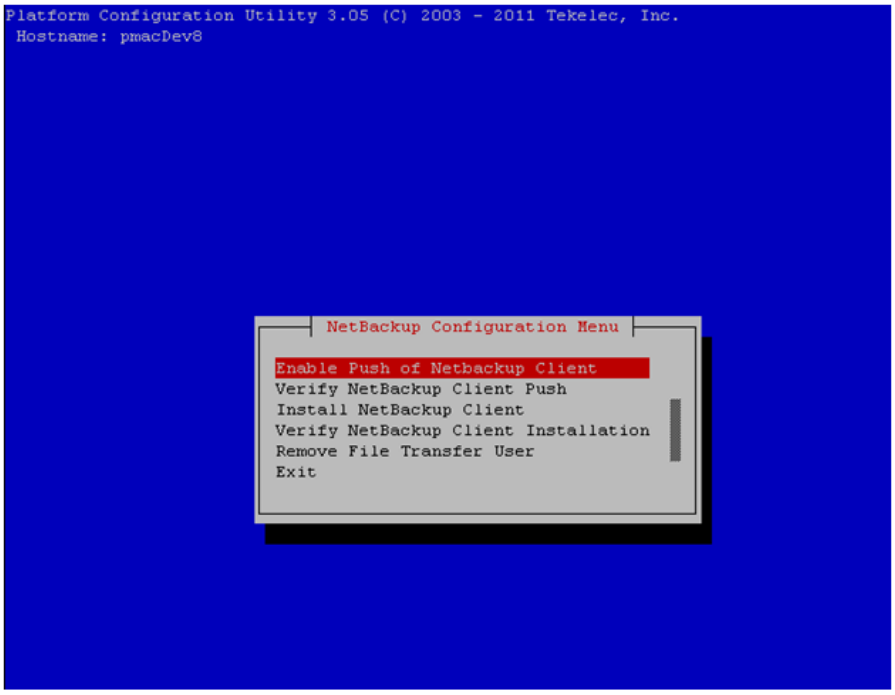
Prerequisites:
• Application server platform installation has been completed.
• Site survey has been performed to determine the network requirements for the application server, and interfaces have been configured.
• NetBackup server is available to copy, sftp, the appropriate NetBackup Client software to the application server.
Note: If a procedural STEP fails to execute successfully, STOP and contact the Customer Care Center.

1. Application server iLO: Login and launch the integrated remote console
- SSH to the application Server (PM&C or NOAMP) as root using the management network for the PM&C or XMI network for the NOAMP.

2. Application server iLO: Configure NetBackup Client on application server

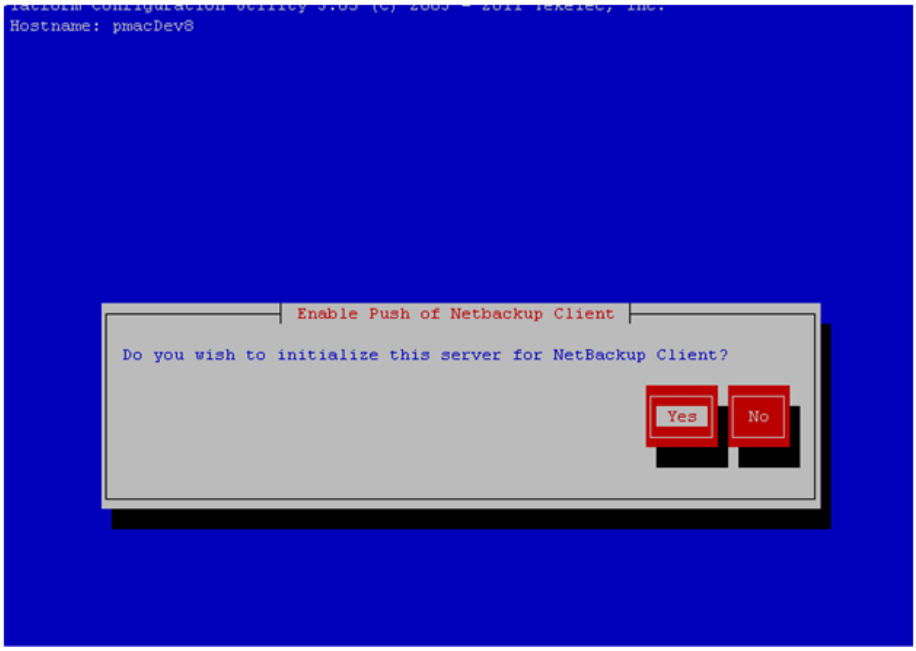
```
# su - platcfg
```

- Navigate to **NetBackup Configuration**



3. Application server iLO: Enable Push of NetBackup Client

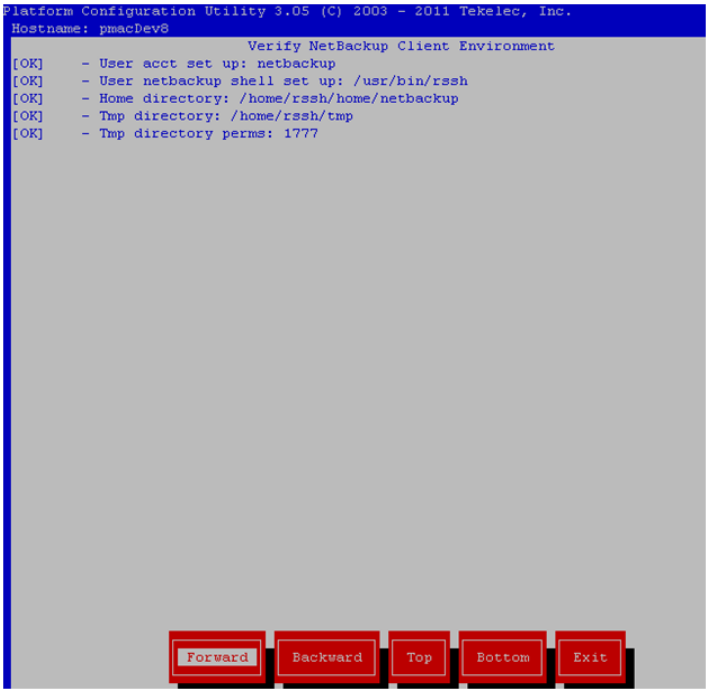
- Navigate to **NetBackup Configuration ➢ Enable Push of NetBackup Client**



- Select **Yes** to initialize the server and enable the NetBackup client software push.

4. Application server iLO: Verify NetBackup Client software push is enabled.

- Navigate to **NetBackup Configuration ➢ Verify NetBackup Client Push**



- Verify list entries indicate "**OK**" for NetBackup client software environment.
- Select "**Exit**" to return to NetBackup Configuration menu.

5. NetBackup server: Push appropriate NetBackup Client software to application server

Note: 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. Below are the steps that are required on the NetBackup server to push the NetBackup Client software to the application server. These example steps assume the NetBackup server is executing in a Linux environment.
Note: The backup server is supported by the customer, and the backup utility software provider. If this procedural STEP, executed at the backup utility server, fails to execute successfully, STOP and contact the Customer Care Center of the backup and restore utility software provider that is being used at this site.

- Log in to the NetBackup server using password provided by customer:
- Navigate to the appropriate NetBackup Client software path:
  Note: The input below is only used as an example. (7.5 in the path below refers to the NetBackup version. If installed a different version (e.g. 7.1), replace 7.5 with 7.1)

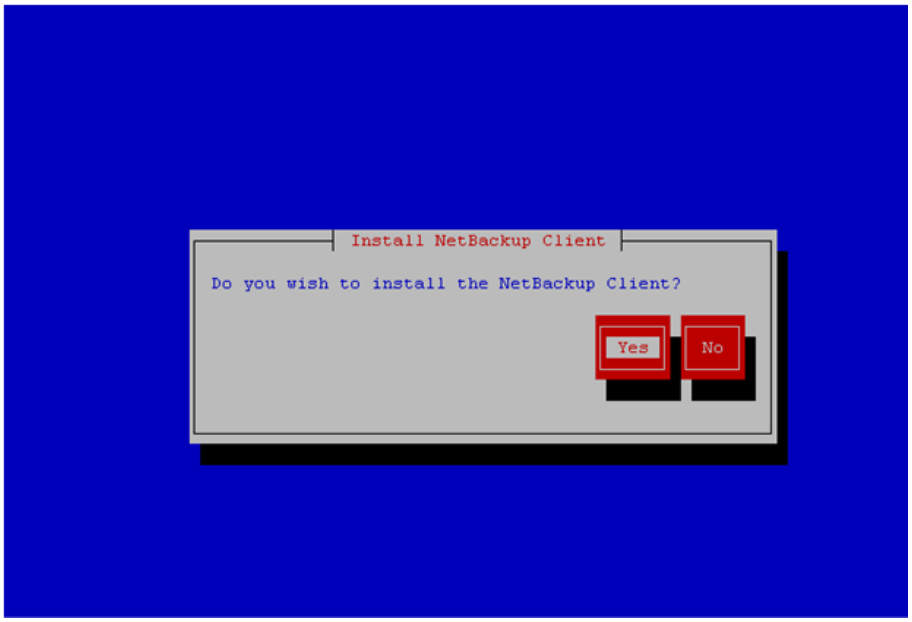
```
# cd /usr/openv/netbackup/client/Linux/7.5
```

- Execute the sftp_to client NetBackup utility using the application IP address and application netbackup user;
  # ./sftp_to_client <application IP> netbackup
  Connecting to 192.168.176.31
  netbackup@192.168.176.31's password:
- Enter application server netbackup user password; the following NetBackup software output is expected, observe the sftp completed successfully:
  File "/usr/openv/netbackup/client/Linux/6.5/.sizes" not found.
  Couldn't rename file "/tmp/bp.6211/sizes" to "/tmp/bp.6211/.sizes": No such file or directory
  File "/usr/openv/NB-Java.tar.Z" not found.
  ./sftp_to_client: line 793: [: : integer expression expected
  ./sftp_to_client: line 793: [: : integer expression expected
  ./sftp_to_client: line 793: [: : integer expression expected
  ./sftp_to_client: line 793: [: : integer expression expected
  ./sftp_to_client: line 793: [: : integer expression expected
  ./sftp_to_client: line 793: [: : integer expression expected
  ./sftp_to_client: line 793: [: : integer expression expected
  ./sftp_to_client: line 793: [: : integer expression expected
  ./sftp_to_client: line 793: [: : integer expression expected
  ./sftp_to_client: line 793: [: : integer expression expected
  sftp completed successfully.
  The root user on 192.168.176.31 must now execute the command "sh /tmp/bp.6211/client_config [-L]". The optional argument, "-L",
  is used to avoid modification of the client's current bp.conf file.
  #

  Note: Although the command executed above instructs you to execute the client_config command, DO NOT execute that command, as it shall be executed by platcfg in the next step.

6. Application server iLO: Install NetBackup Client software on application server.

- Navigate to **NetBackup Configuration ➢ Install NetBackup Client**



- Verify list entries indicate "**OK**" for NetBackup client software installation
- Select "**Exit**" to return to NetBackup Configuration menu

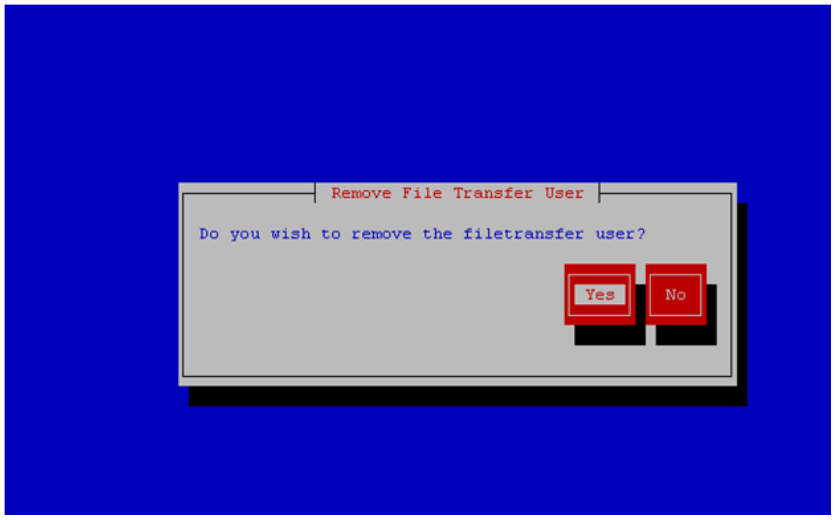
7. Application server iLO: Verify NetBackup CLient software installation on the application server.

- Navigate to **NetBackup Configuration ➢ Verify NetBackup Client Installation**.

- Verify list entries indicate "OK" for NetBackup Client software installation.
- Select "Exit" to return to NetBackup Configuration menu.

8. Application server iLO: Disable NetBackup Client software transfer to the application server.

- Navigate to **NetBackup Configuration ➢ Remove File Transfer User**



- Select "Yes" to remove the NetBackup file transfer user from the application server

9. Application server iLO: Exit platform configuration utility (platcfg)

10. Application server iLO: Use platform configuration utility (platcfg) to modify hosts file with NetBackup server alias.
Note: After the successful transfer and installation of the NetBackup client software the NetBackup servers hostname can be found in the NetBackup "/usr/openv/netbackup/bp.conf" file, identified by the "SERVER" configuration parameter. The NetBackup server hostname and IP address must be added to the application server's hosts file.

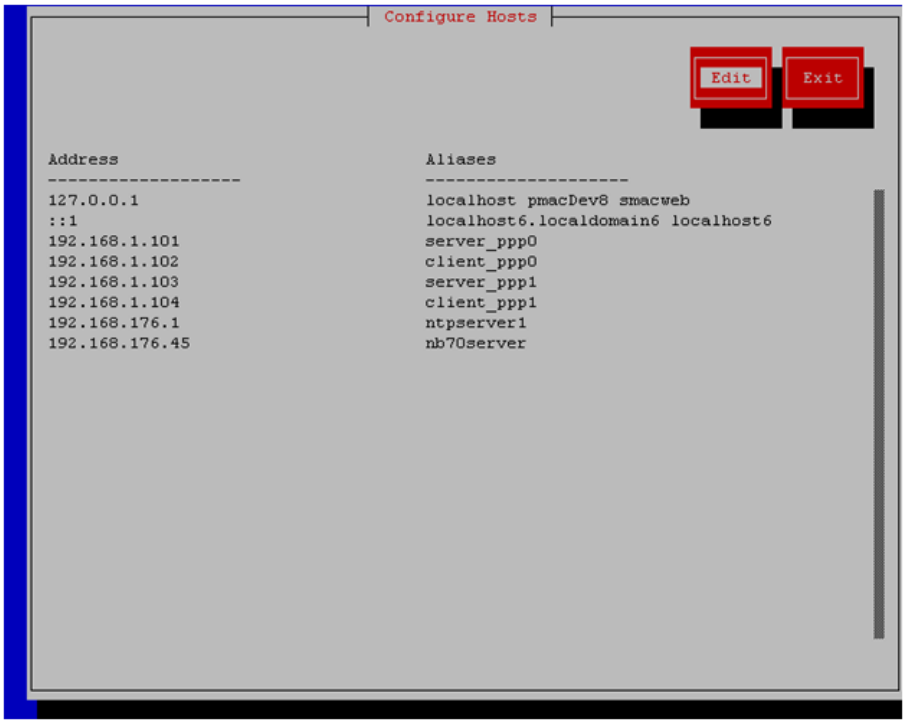
- List NetBackup servers hostname:

```
# cat /usr/openv/netbackup/bp.conf
SERVER = nb70server
CLIENT_NAME = pmacDev8
```

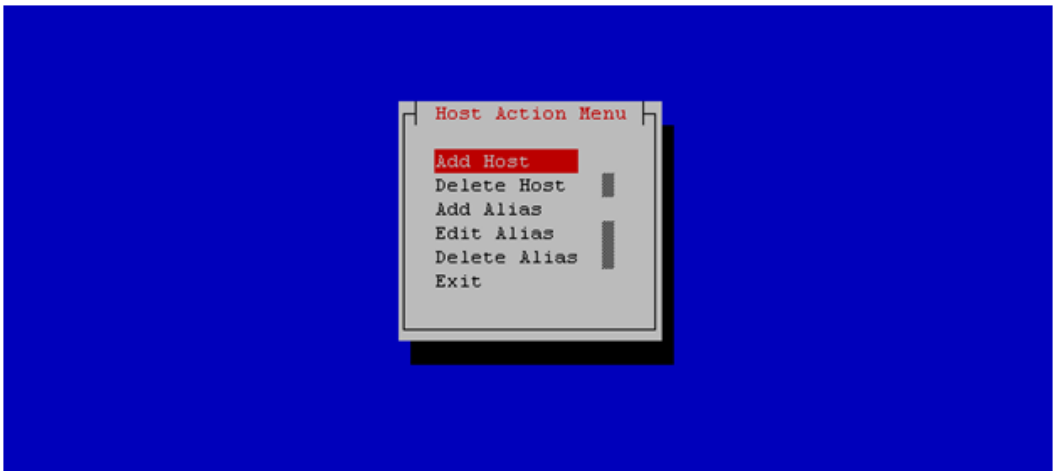
- Use platform configuration utility (platcfg) to update application hosts file with NetBackup Server alias.

```
# su - platcfg
```

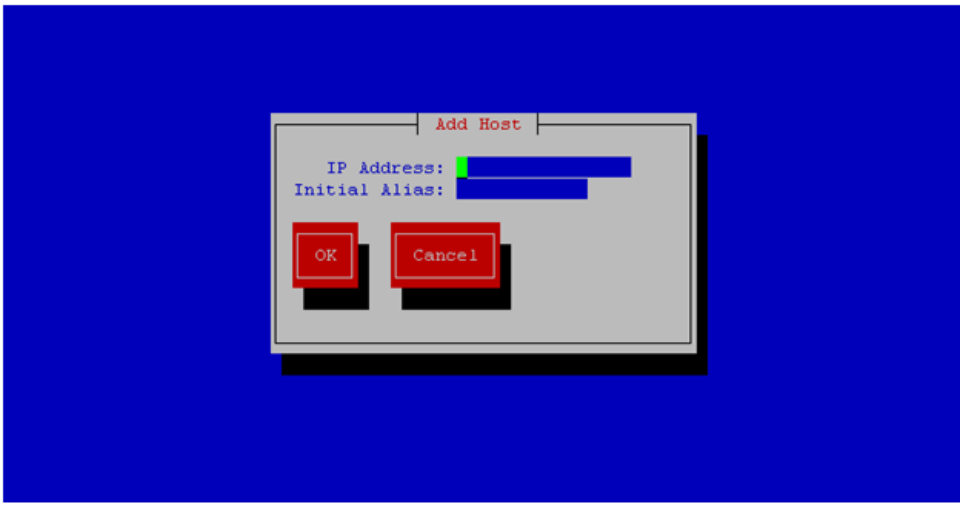
- Navigate to **Network Configuration ➢ Modify Hosts File**



- Select **Edit**, the Host Action Menu will be displayed.



- Select "**Add Host**", and enter the appropriate data



- Select "OK", confirm the host alias add, and exit Platform Configuration Utility

11. Application server iLO: Create links to NetBackup client notify scripts on application server where NetBackup expects to find them.

Note: Copy notify scripts from appropriate path on application server for given application.

```
# ln -s <path>/bpstart_notify /usr/openv/netbackup/bin/bpstart_notify
# ln -s <path>/bpend_notify /usr/openv/netbackup/bin/bpend_notify
```

An example of <path> is **`/usr/TKLC/plat/sbin`**

12. Application server iLO: NetBackup Client software installation complete.

APPENDIX J.2. NETBACKUP CLIENT INSTALL/UPGRADE WITH NBAUTOINSTALL

NOTE: Execute the following procedure to switch/migrate to having netBackup installed via NBAutoInstall (Push Configuration) instead of manual installation using platcfg

Executing this procedure will enable TPD to automatically detect when a Netbackup Client is installed and then complete TPD related tasks that are needed for effective Netbackup Client operation. With this procedure, the Netbackup Client install (pushing the client and performing the install) is the responsibility of the customer and is not covered in this procedure.

Note: If the customer does not have a way to push and install Netbackup Client, then use *Netbackup Client Install/Upgrade with platcfg*.
Note: It is required that this procedure is executed before the customer does the Netbackup Client install.

Prerequisites:
• Application server platform installation has been completed.
• Site survey has been performed to determine the network requirements for the application server, and interfaces have been configured.
• NetBackup server is available to copy, sftp, the appropriate NetBackup Client software to the application server.

1. Application server iLO: Login and launch the integrated remote console

- SSH to the application Server (PM&C or NOAMP) as root using the management network for the PM&C or XMI network for the NOAMP.

2. Application server iLO: Enable nbAutoInstall

```
# /usr/TKLC/plat/bin/nbAutoInstall --enable
```

3. Application server iLO: Create links to NetBackup client notify scripts on application server where NetBackup expects to find them.

```
# mkdir -p /usr/openv/netbackup/bin/
# ln -s <path>/bpstart_notify /usr/openv/netbackup/bin/bpstart_notify
# ln -s <path>/bpend_notify /usr/openv/netbackup/bin/bpend_notify
```

An example of <path> is **/usr/TKLC/plat/sbin**

4. Application server iLO: Verify NetBackup configuration file

- Open */usr/openv/netbackup/bp.conf* and make sure it points to the NetBackup Server using the following command:

  ```
  # vi /usr/openv/netbackup/bp.conf
  ```

  Verify that the highlighted Server name matches the NetBackup Server, and verify that the CLIENT_NAME matches the hostname or IP of the local client machine, if they do not, update them as necessary.

  ```
  SERVER = nb75server
  CLIENT_NAME = 10.240.10.185
  CONNECT_OPTIONS = localhost 1 0 2
  ```

- Edit */etc/hosts* using the following command and add the NetBackup server

  ```
  # vi /etc/hosts
  ```

  ```
  e.g.: 192.168.176.45    nb75server
  ```

The server will now periodically check to see if a new version of Netbackup Client has been installed and will perform necessary TPD configuration accordingly.

At any time, the customer may now push and install a new version of Netbackup Client.

APPENDIX M. DATA DEFINITION AND INSTALLATION VARIABLE MAP

Data Definition Table
Data is required to execute the procedures in 909-2228-001 DSR R4.0 SW Installation
This is a list of:

- text/variable names in the document (where the data needs to be substituted)
- Description of the data

Note: there are multiple text/variable names for some of the data

Table 4. Data Definition Table

ref#	Text/Variables where data is substituted	# Occ	Data Description
1	<switch1A_mgmtVLAN_IP>	3	The IP address in the Platform Management (iLo) subnet that is assigned to the first aggregation switch (switch1A)
	<switch1A_ mgmtVLAN_ip_address>	1	
	<switch1A_mgmtVLAN_address>	4	
	<switch1A_mgmtVLAN_IP>	3	
2	<switch1B_ mgmtVLAN_ip_address>	1	The IP address in the Platform Management (iLo) subnet that is assigned to the second aggregation switch (switch1B)
	<switch1B_mgmtVLAN_address>	4	
3	<management_network_ip>	9	The IP address in the Platform Management (iLo) subnet that is assigned to the PMAC (aka Management) Server. This IP is also known as the "bond0.2 IP", but the name can change to reflect a customer choice of VLAN ID for PlatMgmt (iLo). [2 is the TKLC default]
	<management_server_platmgmt_IP>	4	
	<management_server_mgmtVLAN_ip_address>	20	
	<management_server_bond0.2_ip_address>	4	
	<management_server_mgmtVLAN_ip address>	3	
	<PM&C_ Management _Network _IP>	1	
	<pmac_manangement_network_ip>	3	
	PMAC's management address	1	
	IP Address, **Subnet Mask** and **Gateway IP Address** **PMAC**	1	
	<management_server_ip>	1	

ref#	Text/Variables where data is substituted	# Occ	Data Description
4	<management_server_iLO_ip>	4	The IP address (usually) in the Ext XMI subnet that is reserved for access to the iLo of the PMAC (aka Management) Server. This is a direct connection from the PMAC iLo port to the customer network.
5	<platcfg_password>	13	A standard Tekelec password that specific TPD configuration commands prompt for.
6	<4948E_IOS_image_filename>	2	The file name of the appropriate version of IOS for the 4948E switches
	<IOS_image_file>	4	
7	<3020(6120)_IOS_image_filename>	4	The file name of the appropriate version of IOS for the 3020 switches
	"--iosimage"	2	
8	<3020(6120)_IOS_image_filename>	4	The file name of the appropriate version of IOS for the 6120 switches
	version of HP 6120XG firmware AKA firmware file	2	
9	<PROM_Upgrade_File>	21	The file name of the appropriate version of PROM for the 4948E switches
10	<switch1A_mgmtVLAN_ip_address> <netmask>	3	The netmask of the Platform Management (iLo) subnet
	<switch1B_mgmtVLAN_ip_address> <netmask>	3	
	<mgmtVLAN_netmask>	4	
	Subnet Masks	1	
	mask	1	
	IP Address, Subnet Mask and Gateway IP Address PMAC	1	
11	<switch_mgmtVLAN_id>	4	The VLAN number that is assigned to the Platform Management (iLo) subnet
	<Plat Mgmt vlan id>	10	
12	<mgmtVLAN_Switch_VIP_address>	4	The IP address in the Platform Management (iLo) subnet that is assigned to float (as a VIP) between the two switches. Only in Layer 3 (with the use of Internal
	<switch_mgmtVLAN_VIP>	4	

ref#	Text/Variables where data is substituted	# Occ	Data Description
	IP Address, **Subnet Mask** and **Gateway IP Address** **PMAC**	1	signaling subnets) is this address on the 4948 aggregation switches. For Layer 2, this IP address is on the customer switches.
13	<switch_console_password>	4	A standard Tekelec password that controls access to the 4948E aggregation switches.
14	<switch_platform_username>	4	A standard Tekelec username that controls access to the platform
15	<switch_platform_password>	8	A standard Tekelec password that validates the platform access.
16	<switch_enable_password>	8	A standard Tekelec password that controls enable privileges to the 4948E switches.
17	<enclosure_switch_IP> **3020 - repeat for bay2**	1	The IP addresses in the Platform Management (iLo) subnet that are assigned to the 3020 enclosure switches - aka EBIPA *Enclosure Bay IP addressing
18	<enclosure_switch_IP> **3020 - repeat for bay4, bay5, bay6 (for additional pairs of enclosure switches)**	2 or 4	The IP addresses in the Platform Management (iLo) subnet that are assigned to the 3020 enclosure switches beyond bay1 and bay2 - - aka EBIPA *Enclosure Bay IP addressing
19	<enclosure_switch_IP> **6120 - repeat for bay2**	14	The IP addresses in the Platform Management (iLo) subnet that are assigned to the 3020 enclosure switches - - aka EBIPA *Enclosure Bay IP addressing
20	<enclosure_switch_IP> **6120XG repeat for bay4, bay5, bay6 - (for additional pairs of enclosure switches)**	14	The IP address in the Platform Management (iLo) subnet that is assigned to the 6120 enclosure switch in bay3 - - aka EBIPA *Enclosure Bay IP addressing
21	<manager_password>	2	Password to login to an enclosure switch

ref#	Text/Variables where data is substituted	# Occ	Data Description
22	**<ethernet_interface_1> 4948E-A**	3	The name of the first ethernet interface on the PMAC (aka Management) Server - which defines the NIC port connected to the first aggregation switch (switch1A)
23	**<ethernet_interface_2> 4948E-B**	3	The name of the second ethernet interface on the PMAC (aka Management) Server - which defines the NIC port connected to the second aggregation switch (switch1B)
24	**<management_server_mgmtInterface>**	2	The name of the interface which, when given as an argument to ifconfig, will return the IP address for use in configuring the console .
25	**<customer_supplied_ntp_server_address>**	2	The IP address supplied by the customer for an NTP server in their network.
	Primary NTP server	1	
26	**<NOAMP blade Control Net IP addr>**	4	Control IP addresses are assigned to blades by the PMAC. Use the PMAC GUI as described to learn the IP address for each NO server
	<NOAMP-Control-IP>:443	1	
27	**<first noamp XMI IP address>**	2	The IP address in the XMI (OAM) subnet that is assigned to the first NOAMP blade server.
28	server IP addresses for the IMI network	1	The IP addresses in the IMI subnet that are assigned to the first and second NOAMP blade servers.
29	server IP addresses for the XMI network	1	The IP addresses in the XMI (OAM) subnet that are assigned to the first and second NOAMP blade servers.
30	**vlanID provided by the customer**	2	The VLAN number that is assigned by the customer to the Platform Management (iLo) subnet
31	**<rack name>**	1	A name supplied by the customer to be assigned to the cabinet
32	CabinetID **AKA** Cabinet ID	3	A numeric value between 1 and 654.

ref#	Text/Variables where data is substituted	# Occ	Data Description
33	**<position>**	1	A name supplied by the customer to be assigned to the enclosure
34	ILO's Ips	1	The IP address in the Platform Management (iLo) subnet that is assigned to each server - aka EBIPA "Enclosure Bay IP Addressing"
35	IP addresses, Subnet Masks, Gateways	1	The gateway of the Platform Management (iLo) subnet
	<mgmtVLAN_gateway_address>	2	
	gateway	1	
36	**System Location**	1	A name supplied by the customer to be assigned to the enclosure
37	NO VIP IP	1	The IP address in the XMI (OAM) subnet that is assigned to float (as a VIP) between the two NOAM servers.
38	firmware version **3020**		An alphanumeric string that indicates an IOS version for 3020
39	firmware version **6120**		An alphanumeric string that indicates a firmware version for 6120
40	firmware version **OA**	9	An alphanumeric string that indicates a firmware version for OA
	<OA_firmware_version>	1	
41	<HPFW_mount_ point>	1	Directory on the management server (PMAC) where the HP firmware solutions CD is mounted.
42	Location ID	1	A numeric value between 1 and 4 used to uniquely identify the enclosure.
43	Bay 1 OA IP	1	The IP addresses in the Platform Management (iLo) subnet that are assigned to the OA's
	<OA_IP>	1	
	OA IP address	4	
	IP addresses,	1	
	Bay 2 OA IP	1	

ref#	Text/Variables where data is substituted	# Occ	Data Description
	OA1 IP address	1	
44	**<root password>**,	1	Standardized Tekelec passwords for use in editing the iLo password XML file
	<iLo root password>	1	
	<iLo Administrator password>	1	
45	password provided by the application documentation.	1	
46	**<HP_blade_type>**		The type of HP blade server is necessary to identify the correct FW version
47	**<image_part_number>**	3	An alphanumeric string that indicates a firmware (fw) version for HP Blade servers
48	<OA_admin_user>	1	An alphanumeric string that is the username for administrative account on the OA's
49	**<OA_admin_password>**	1	An alphanumeric string that controls access to the Administrator user on the OA's.
50	<ISO_filename>	3	The file name of the appropriate version of ISO for TVOE
51	<ISO_filename>	3	The file name of the appropriate version of ISO for the DSR application
	<Application ISO NAME>	3	
52	<ISO_filename>	3	The file name of the appropriate version of ISO for the TPD to be installed on the blades
53	**<TVOE blade Control Net IP addr>**	1	Control IP addresses are assigned to blades by the PMAC. Use the PMAC GUI to learn the IP address for the first TVOE server.
54	**<Management_Server Control_IP_ addr>**	1	Control IP addresses are assigned to blades by the PMAC. Use the PMAC GUI to learn the IP address for the management server.
55	**<XMI_VLAN_ID>**	2	The VLAN number that is assigned to the XMI (OAM) subnet

ref#	Text/Variables where data is substituted	# Occ	Data Description
56	**<IMI_VLAN_ID>**	2	The VLAN number that is assigned to the IMI subnet
57	**<interface>**	2	Quote from doc: In these examples, <*interface*> should be replaced with the actual eterhnet interface that will be used as the dedicated NetBackup port. For instance, "eth01", or "eth22".
58	hostname for your server **TVOE**	1	A name that is assigned to identify the TVOE host (server)
59	***<IMI Network>***	2	An alphanumeric string that is assigned to be the name of the IMI subnet
60	**<Hostname> NO-A**	1	An alphanumeric string that is assigned to be the host name of the first NOAM server (aka NO-A)
61	**<Hostname> NO-B**	1	An alphanumeric string that is assigned to be the host name of the second NOAM server (aka NO-B)
62	**<Hostname> SO-A**	1	An alphanumeric string that is assigned to be the host name of the first SOAM server (aka SO-A)
63	**<Hostname> SO-B**	1	An alphanumeric string that is assigned to be the host name of the second SOAM server (aka SO-B)
64	**<Hostname> MP-A**	1	An alphanumeric string that is assigned to be the host name of the first MP server (aka MP-A)
65	**<Hostname> MP-A**	1	An alphanumeric string that is assigned to be the host name of the second MP server (aka MP-B)
66	Network Element **NOAM - Proc 28, step 2**	1	An alphanumeric name supplied by the customer to be assigned as the name of the NOAM Network Element. Note: limited to alphanumeric and underscore only
67	hostname, role, hardware profile, network element, and location **SOAM**	1	An alphanumeric name supplied by the customer to be assigned as the name of the SOAM Host. Note: limited to alphanumeric and hyphen only

ref#	Text/Variables where data is substituted	# Occ	Data Description
68	hostname, role, hardware profile, network element, and location **SOAM**	1	
69	hostname, role, hardware profile, network element, and location **SOAM**	1	
70	hostname, role, hardware profile, network element, and location **SOAM**	1	
71	hostname, role, hardware profile, network element, and location **SOAM**	1	
72	IP address **SOAM**	1	
73	VLAN-Tagged **SOAM**	1	
74	**<SOAM blade Control Net IP addr>**	2	
75	NOAMP VIP address **SOAM**	2	
76	SOAM Server Group Name	1	
77	Network Name, VLAN ID, Network Address and Netmask	2	XSI-1 or XSI-2 are default names for the first or second signaling network. The customer can specify a name. Note: IP SS will need to be updated to collect the name
78	Network Name, VLAN ID, Network Address and Netmask	2	The VLAN number that is assigned to the first or second signaling subnet
79	Network Name, VLAN ID, Network Address and Netmask	2	The network address of the first or second signaling subnet
	Network ID of Ext-XSI1	2	
80	Network Name, VLAN ID, Network Address and Netmask	2	The netmask of the first or second signaling subnet
	corresponding Netmask	3	
81	the IP address that corresponds to the IPv4 interface.	2	The IP addresses in the signaling subnets that are assigned to the MP blade servers
82	Int-XSI1 switch VIP	1	The IP addresses in each signaling subnet that are assigned to float (as a VIP) between the two switches. Only in Layer 3 (with the use of internal signaling subnets)
	Int-XSI2 switch VIP	1	
	gateway IP for the network	1	

ref#	Text/Variables where data is substituted	# Occ	Data Description
	VIP for XSI1	1	When using aggregation switches, then VIP refers to the internal XSI1or internal XSI2 gateway VIP address. For installations without aggregation switches, the IP of this gateway is supplied by the customer. This may or may not be a VIP, but it will serve as the next-hop gateway regardless.
	VIP of int-XSI-1	1	
	VIP for XSI2	1	
	VIP of int-XSI-2	1	
	corresponding VIP addresses	1	
83	time zone you have selected for this installation	1	The Time Zone needs to be specified by the customer – Specific or UTC
84	**<application IP> netbackup**	1	-
85	NetBackup server alias.	2	-
86	NetBackup servers hostname	2	-
87	**<path>**	2	-
88	**<NO1_NetBackup_IP>**	1	When using a dedicated network for Netbackup, this is the IP address on the Netbackup network of the 1st NO.
89	**<NO2_NetBackup_IP>**	1	When using a dedicated network for Netbackup, this is the IP address on the Netbackup network of the 2nd NO.
90	**<NetBackup_NetMask>**	2	When using a dedicated network for Netbackup, this is the netmask of that network
91	**<NetBackup_Network_ID>**	2	When using a dedicated network for Netbackup, this is the Network ID of that network.
92	**<NetBackup_Network_NetMask>**	2	When using a dedicated network for Netbackup, this is the netmask of that network
93	**<NetBackup_Network_Gateway_IP>**	2	When using a dedicated network for Netbackup, this is the gateway IP on the netbackup network.

APPENDIX N. SWOPS SIGN OFF.

Discrepancy List

Date	Test Case	Description of Failures and/or Issues. Any CSR's / RMA's issued during Acceptance. Discrepancy	Resolution and SWOPS Engineer Responsible	Resolution Date:

APPENDIX O. CUSTOMER SIGN OFF

Sign-Off Record

*** **Please review this entire document**. ***
This is to certify that all steps required for the upgrade successfully completed without failure.

Sign your name, showing approval of this procedure, and fax this page and the above completed matrix to Tekelec, FAX # 919-460-3669.

Customer: Company Name:_____ Date: _____

Site: Location:_____

Customer:(Print)_____ Phone:_____

Fax: _____

Start Date: _____ Completion Date: _____

This procedure has been approved by the undersigned. Any deviations from this procedure must be approved by both Tekelec and the customer representative. A copy of this page should be given to the customer for their records. The SWOPS supervisor will also maintain a signed copy of this completion for future reference.

Tekelec Signature: _____ Date: _____

Customer Signature: _____ Date: _____

APPENDIX P. ACCESSING TEKELEC'S CUSTOMER SUPPORT SITE

Access to the Tekelec's Customer Support site is restricted to current Tekelec customers. This section describes how to log into Tekelec's Customer Support site and how to locate upgrade procedures. Viewing these files requires Adobe Acrobat Reader.

1. Go to Tekelec's Customer Support login page at https://support.tekelec.com/index.asp
2. Enter your assigned username and chosen password and click **Login.**

   Or, if you do not have access to the Customer Support site, click **Need an Account?**
   Follow instructions on the screen.

   Note: After 20 minutes of inactivity, you will be logged off, and you must repeat this step to regain access.
3. After successful login, select a product from the Product Support drop-down menu.
4. Select a release number from the Product Support Release drop-down menu.
5. Locate the Upgrade Procedures section.
6. To open the procedure in the same window, click the procedure name. To open the procedure in a new window, right-click the procedure name and select **Open in New Window**.
7. To download the procedure, right-click the procedure name and select **Save Target As**.