Oracle® Communications Diameter Signaling Router

DSR RMS Productization Installation Procedure

Release 4.X/5.X

909-2255-001

October 2013

Oracle® Communications Diameter Signaling Router DSR RMS Productization Software Installation Procedure, Release 4.X/5.X

Copyright © 2012,2013 Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

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

Before upgrading any system, please access Oracle's Tekelec Customer Support site and review any Technical Service Bulletins (TSBs) that relate to this upgrade.

Refer to **Error! Reference source not found.** for instructions on accessing this site.

Contact Oracle's Tekelec Customer Care Center and inform them of your upgrade plans prior to beginning this or any upgrade procedure.

Phone: 1-888-367-8552 or 919-460-2150 (international)
FAX: 919-460-2126

TABLE OF CONTENTS

1.0 INTRODUCTION....7
1.1 Purpose and Scope....7
1.2 References....7
1.2.1 External....7
1.2.2 Internal (Tekelec)....7
1.3 Variables....7
1.4 Acronyms....7
1.5 Terminology....8

2.0 GENERAL DESCRIPTION....9
2.1 ACQUIRING FIRMWARE....9

3.0 INSTALL OVERVIEW....11
3.1 Required Materials....11
3.2 Installation Overview....11
3.2.1 Installation Matrix....11
3.2.2 Installation Procedures....12
3.3 Optional Features....13

4.0 SOFTWARE INSTALLATION PROCEDURE....15
4.1 Prepare Servers for IPM....15
4.2 Install and Configure TVOE on First RMS (PM&C Host)....21
4.3 Install PM&C....35
4.4 Gather and Prepare Configuration Files....38
4.5 Configure Cisco 4948E Aggregation Switch....40
4.6 Configure PM&C Server....55
4.7 Install TVOE on second RMS....62
4.8 Create Virtual Machines for Applications....80
4.9 Install Software on Virtual Machiness....94
4.10 Application Configuration....98
4.11 Signaling Network Configuration....131
4.12 Install Optional Features....139

APPENDIX A. SAMPLE NETWORK ELEMENT AND HARDWARE PROFILES....140

APPENDIX B. CONFIGURING FOR EAGLE XG TVOEILO ACCESS....143

APPENDIX C. TVOE ILO ACCESS....145

APPENDIX D. TVOE ILO GUI ACCESS....148

APPENDIX E. CHANGING TVOE ILO ADDRESS....150

APPENDIX F. PM&C/NOAMP/SOAM/MP/IPFE CONSOLE ACCESS....152

APPENDIX G. ACCESSING THE NOAMP GUI USING SSH TUNNELING WITH PUTTY....154

APPENDIX H. MANUAL TIMEZONE SETTING PROCEDURE....157

APPENDIX I. LIST OF FREQUENTLY USED TIME ZONES....158

APPENDIX J. APPLICATION NETBACKUP CLIENT INSTALLATION PROCEDURES 161
APPENDIX J.1. NETBACKUP CLIENT INSTALL USING PLATCFG 161
APPENDIX J.2. NETBACKUP CLIENT INSTALL/UPGRADE WITH NBAUTOINSTALL 168

APPENDIX K. DATA DEFINITION AND INSTALLATION VARIABLE MAP 170

APPENDIX L. CREATING A BOOTABLE USB DRIVE 179
Procedure L.1 Creating a Bootable USB Drive on Windows 179
Procedure L.2 Creating a Bootable USB Drive on Linux 180

APPENDIX M. CONFIGURE ADDITIONAL SIGNALING INTERFACES ON AN MP 181
Procedure M.1 Configure Additional Signaling Interfaces on an MP 181

APPENDIX N. SWOPS SIGN OFF. 184

APPENDIX O. CUSTOMER SIGN OFF 185
Sign-Off Record 185

APPENDIX P. ACCESSING TEKELEC'S CUSTOMER SUPPORT SITE 186

List of Figures

Figure 1. Example of an instruction that indicates the server to which it applies 8
Figure 2. Initial Application Installation Path – Example shown 9

List of Tables

Table 1. Acronyms 8
Table 2. Installation Overview 12
Table 3. List of Selected Time Zone Values 158
Table 4. Data Definition Table 170

List of Procedures

Procedure 1. Configure the RMS Server BIOS Settings and Update Firmware 15
Procedure 2. Install TVOE 2.0 on First RMS Server 21
Procedure 3. First RMS Configuration 23
Procedure 4. PM&C Deployment Procedure 35
Procedure 5. Gather/Prepare Configuration Files 38
Procedure 6. Configure Cisco 4948E/4948E-F Switch using NetConfig 40
Procedure 7. Configure the PM&C Server 55
Procedure 8. Install TVOE on Second RMS 62
Procedure 9. Configure TVOE on Second RMS Server 67
Procedure 10. Load ISOs onto PM&C Server 80
Procedure 11. Create NOAMP Guest VMs 82
Procedure 12. Create SOAM Guest VMs 85
Procedure 13. Create MP Guest VMs 88
Procedure 14. Create IPFE Guest VMs (Optional) 91
Procedure 15. Install the Software on the VMs 94
Procedure 16. Configure the First NOAMP NE and Server 98
Procedure 17. Configure the NOAMP Server Group 102
Procedure 18. Configure the Second NOAMP Server 103
Procedure 19. Complete Configuring the NOAMP Server Group 105
Procedure 20. Install NetBackup Client (Optional) 107
Procedure 21. NO Configuration for DR Site (Optional) 107
Procedure 22. NO Pairing for DSR NO DR Site (Optional) 112
Procedure 23. Configure the SOAM NE 116
Procedure 24. Configure the SOAM Servers 116
Procedure 25. Configure the SOAM Server Group 119
Procedure 26. Configure RMS-specific B-level Resources 121
Procedure 27. Optimize NO and SO Databases 122
Procedure 28. Configure the MP Servers 123
Procedure 29. Configure the MP Server Group(s) and Profiles 128
Procedure 30. Configure the Signaling Networks 131
Procedure 31. Configure the Signaling Devices 132
Procedure 32. Configure the Signaling Network Routes 134
Procedure 33. Add VIP for Signaling Networks (Active/Standby Configurations ONLY) 136

Procedure 34. Configure SNMP Trap Receiver(s) (OPTIONAL) 137
Procedure 35. Install Optional Features 139
Procedure 36. Configure ComAgent Connections 139

1.0 INTRODUCTION

1.1 Purpose and Scope

This document describes methods utilized and procedures executed to configure HP DL-380 Gen8 Rack Mount Servers (RMS) to be used with Diameter Signaling Router 4.1 (DSR 4.1) and to install DSR 4.1. 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] *DSR 4.1RMS Productization Networking Interconnect TR,* TR007187, 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] HP Solutions Firmware Upgrade Pack Upgrade Procedures 2.2, 909-2234-001, 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 4.12Appendix K

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
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:

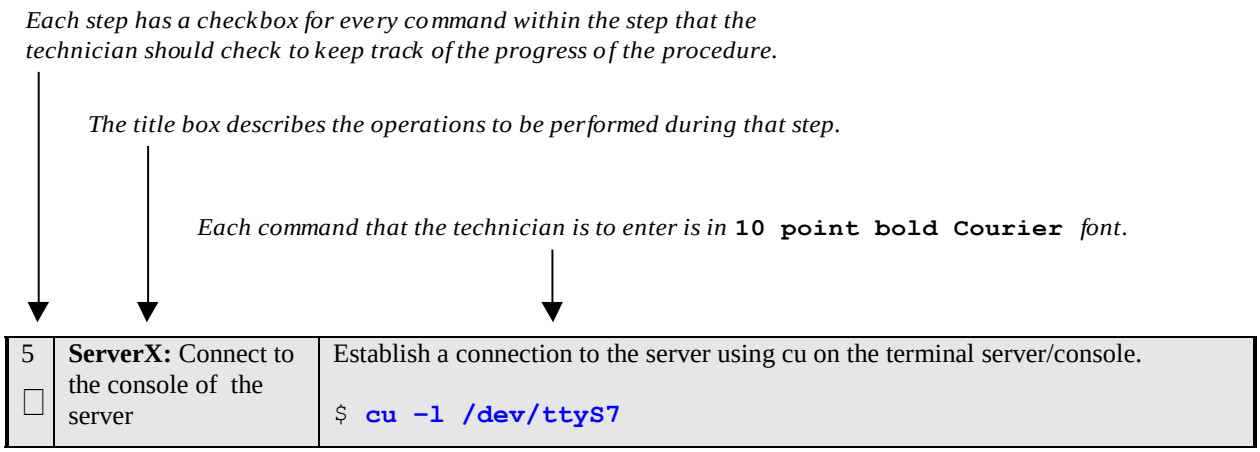


Figure 1. Example of an instruction that indicates the server to which it applies

2.0 GENERAL DESCRIPTION

This document defines the steps to execute the initial installation of the Diameter Signaling Router 4.1 (DSR 4.1) application.

DSR 4.1 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.

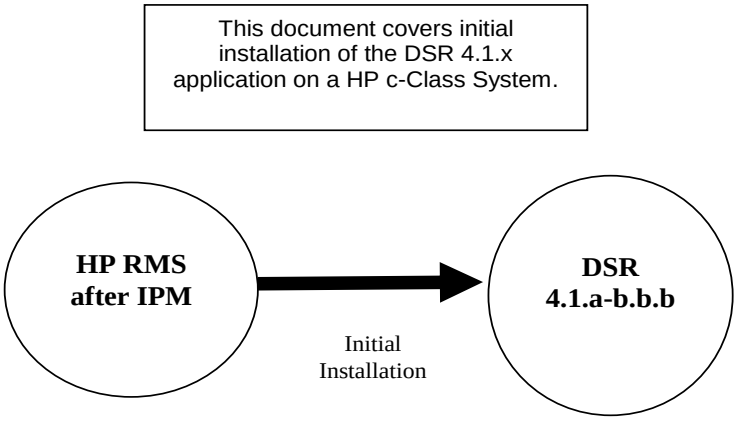


Figure 2. Initial Application Installation Path – Example shown

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 2.1.3* (PN: 795-0000-201) although the latest 2.1.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 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 2.1.x* releases are:

- HP Smart Update Firmware DVD/ISO
- HP Misc Firmware CD/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 4.1 Servers and devices requiring possible firmware updates are:

- HP DL380 Rack Mount Servers
- 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 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 5.0.0-50.10.0, 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].

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 lists the procedures required for installation with estimated times. Section 3.2.1 contains a matrix of deployment features and the required procedures needed to install them**.** Section 3.2.2 lists the steps required to install a DSR 4.1 system. These latter sections expand on the information from the matrix and provide a general timeline for the installation.

3.2.1 Installation Matrix

The table below matches up the list of major installation variables and their corresponding procedures. The first row labeled "ALL SITES" has the list of all **mandatory** procedures checked off. These steps will be executed in all deployments regardless of other variables. The remaining rows list install features that may or may not be present in every deployment. The reader of this document should be aware of what is necessary for a particular installation (such as the type and number of enclosure switches) and then check off the proper features under the ***Site Type*** column. He should then note which columns have check marks for that feature and add the appropriate procedure to his "master" list. In the end, a customized installation sequence should result.

	Procedure # / Site-Type	1-4	5-6	7-10	11	12	13-15	16	17	18-30	31, 33, 36	32-49
☐	ALL SITES – Must Perform	✓		✓			✓			✓		✓
☐	+ 4948E Agg. Switches		✓									
☐	+Net-backup Client										✓	

3.2.2 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
Procedure 2	Install TVOE 2.0 on First RMS Server	30	60
Procedure 3	First RMS Configuration	30	90
Procedure 4	PM&C Deployment Procedure	20	110
Procedure 5	Gather/Prepare Configuration Files and start services	10	120
Procedure 6*	Configure Cisco 4948E/4948E-F Switch using NetConfig*	40*	120-160
Procedure 7	Configure the PM&C Server	10	130-170
Procedure 8	Install TVOE on Second RMS	20	150-190
Procedure 9	Configure TVOE on Second RMS	20	170-210
Procedure 10	Load ISOs onto PM&C Server	10	180-220
Procedure 11	Create NOAMP Guest VMs	5	185-225
Procedure 12	Create SOAM Guest VMs	5	190-230
Procedure 13	Create MP Guest VMs	5	195-235
Procedure 14	Create IPFE Guest VMs*	5	195-240
Procedure 15	Install the Software on the VMs	20	215-260
Procedure 16	Configure the First NO Blade Server	25	240-285

Table 2. Installation Overview

Procedure	Phase	Elapsed Time (Minutes)	
		This Step	Cum.
Procedure 17	Configure the NO Server Group	15	255-300
Procedure 18	Configure the Second NO Server	15	270-315
Procedure 19	Complete Configuring the NOAMP Server Group	10	280-325
Procedure 20	Install NetBackup Client on NOAMP Servers*	10	280-335
Procedure 21	NO Configuration for DR Site*	10	280-345
Procedure 22	NO Pairing for DSR NO DR Site*	10	280-355
Procedure 23	Configure the SOAM NE	15	295-370
Procedure 24	Configure the SOAM Servers	10	305-380
Procedure 25	Configure the SOAM Server Group	10	315-390
Procedure 26	Configure RMS-specific B-level Resources	5	320-395
Procedure 27	Optimize NO and SO Databases	5	325-400
Procedure 28	Configure the MP Blade Servers	10	335-415
Procedure 29	Configure the MP Server Group(s) and Profiles	10	345-420
Procedure 30	Configure the Signaling Network	30	375-450
Procedure 31	Configure the Signaling Devices	10	385-460
Procedure 32	Configure the Signaling Network Routes	15	400-475
Procedure 33	Add VIP for Signaling Networks	5	405-480
Procedure 34	Configure SNMP for Traps Receivers*	5	405-485
Procedure 35	Install Optional Features*	Varies	405-*
Procedure 34	Configure ComAgent Connection*	5	405-*

* denotes Optional Features.

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
Charging Proxy Application (CPA) **Session Binding Repository** (SBR)	*CPA Activation Feature Work Instruction*, WI006780
Diameter Mediation	*DSR Meta Administration Feature Activation*, WI006761

Full Address Based Resolution (FABR**)**	*DSR FABR Feature Activation*, WI006771
Range Based Address Resolution (RBAR**)**	*DSR RBAR Feature Activation*, WI006763
Per connection ingress message control	*DSR 4.0 – Per connection ingress message control*

4.0 SOFTWARE INSTALLATION PROCEDURE

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

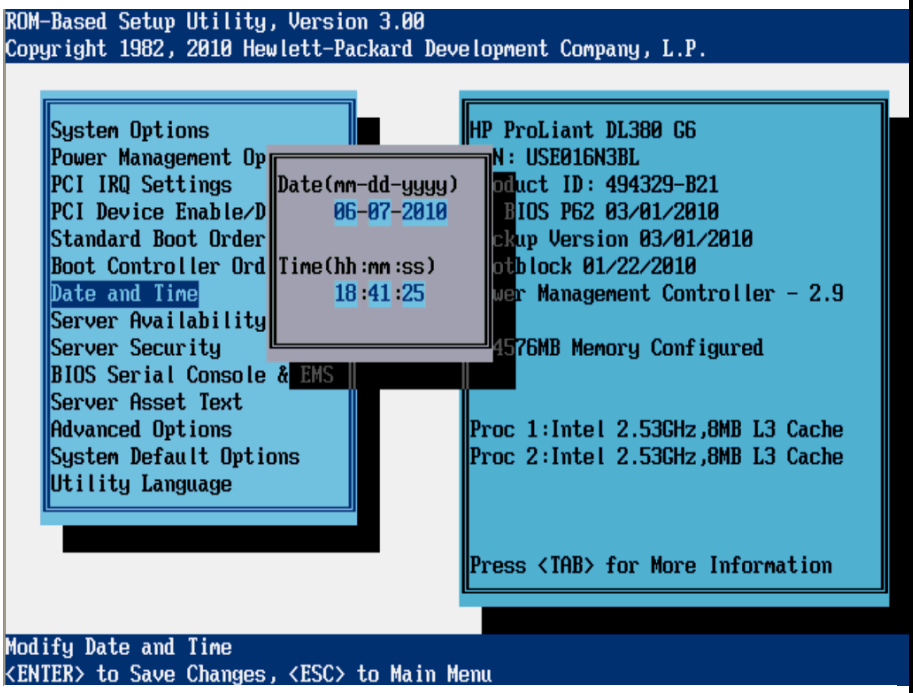
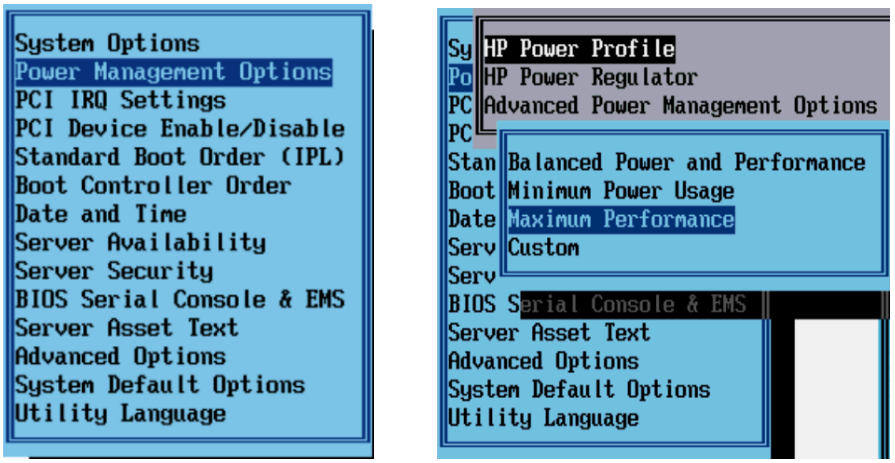
NOTE: Prior to executing the procedures below, please review the DSR release notes, and be aware of any workaround that should be executed.

4.1 Prepare Servers for IPM

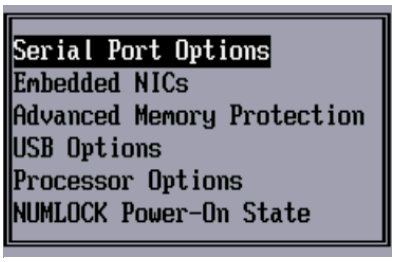
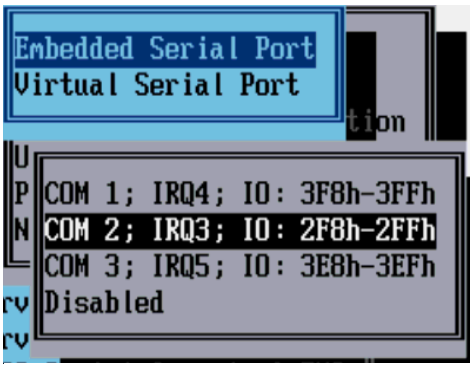
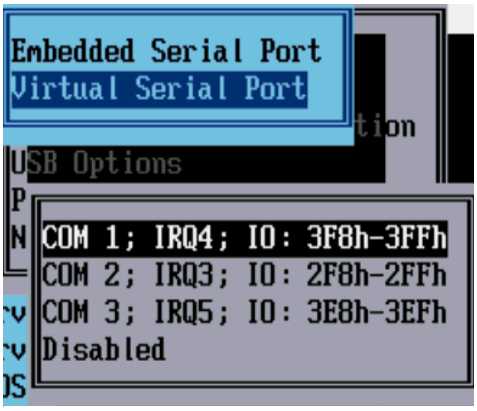
Procedure 1. Configure the RMS Server BIOS Settings and Update Firmware

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 ☐	**DL380 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 iLO and change the address if necessary.
2 ☐	**DL380 server:** Prepare to upgrade DL380 server firmware	Insert HP Smart Update Firmware USB into a USB port of the DL380 server. Refer to [1] for instructions on how to update the firmware.
3 ☐	**DL380 server:** Access the Server BIOS	Reboot the server once the firmware update is complete, 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.

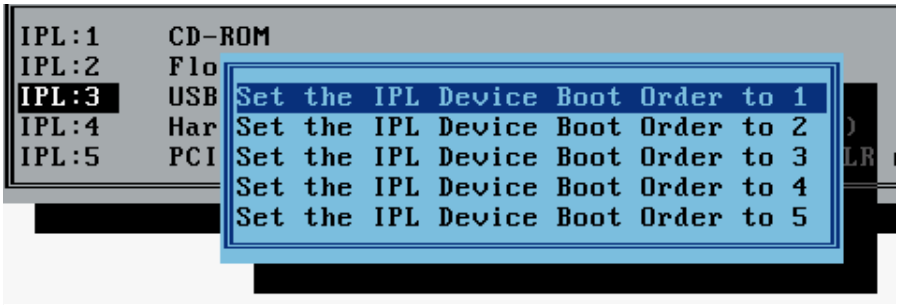
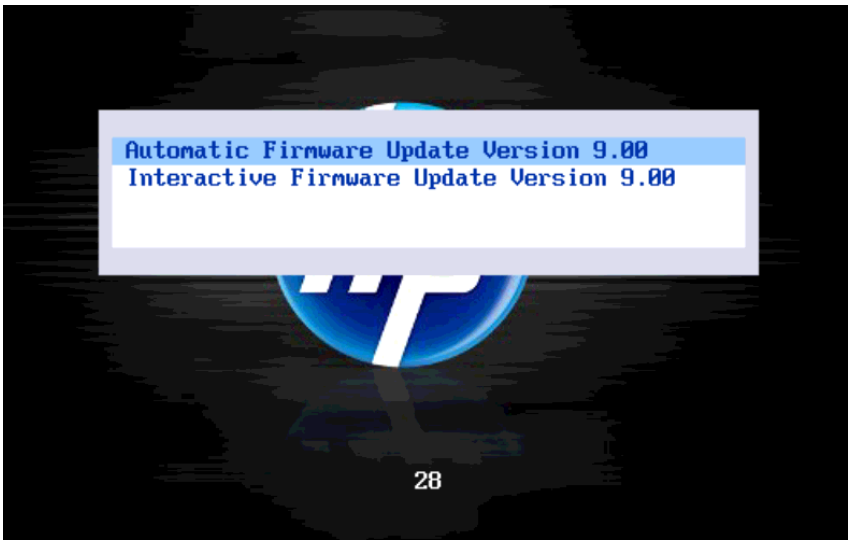
Procedure 1. Configure the RMS Server BIOS Settings and Update Firmware

4 ☐	**DL380 server:** Set CMOS Clock	Scroll to *Date and Time* and press **Enter** Set the date and 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>** to return to the main menu

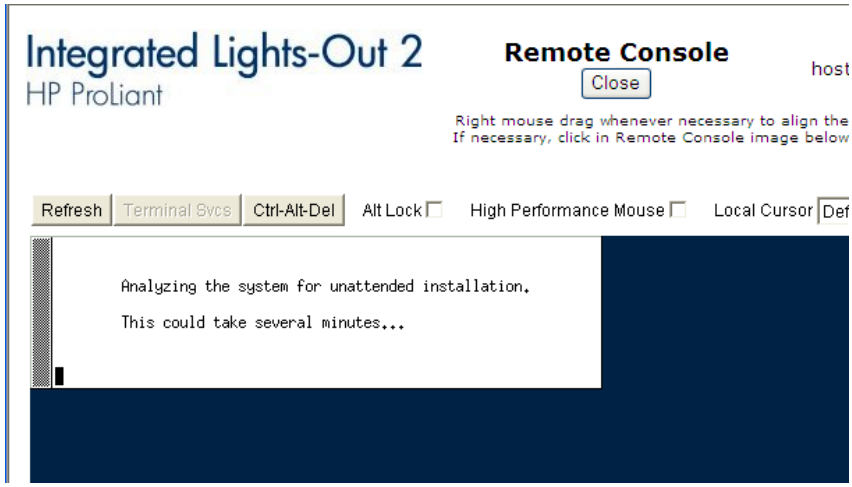
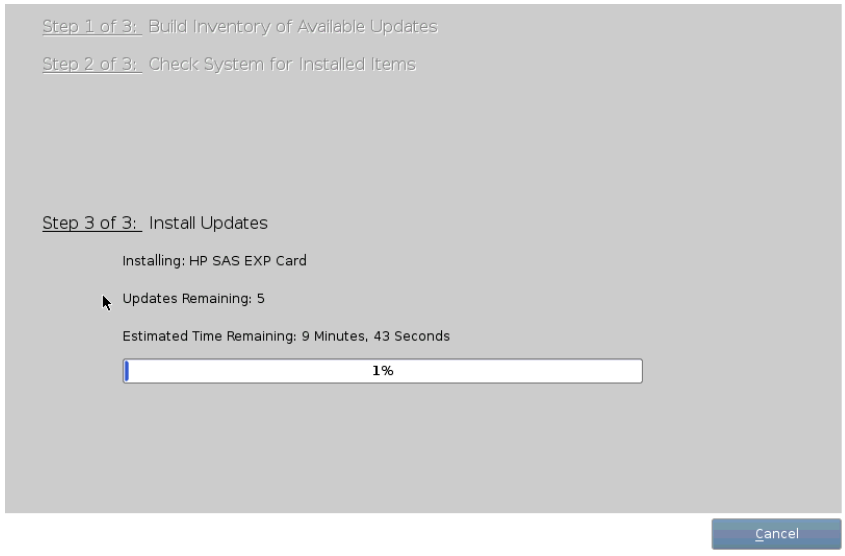
Procedure 1. Configure the RMS Server BIOS Settings and Update Firmware

5 ☐	**DL380 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 ☐	**DL380 server:** Double Check boot Order	Scroll to *Standard Boot Order (IPL)* and press **Enter** Select *USB DriveKey*, and set its boot order to 1 as shown below  Press **Enter** Press **<ESC>** to return to the main menu.
7 ☐	**DL380 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 ☐	**DL380 server:** Save Configuration and Exit	Press **<ESC>** twice then press **F10** to save the configuration and exit. The server will reboot
9 ☐	**DL380 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 ☐	**DL380 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 ☐	**DL380 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 ☐	**DL380 server:** Remove the firmware CD	Remove the HP Smart Update Firmware USB media from the drive. Exit from the `Integrated Remote Console`.
15 ☐	**Repeat for second RMS**	Repeat this procedure for the second RMS Server.

4.2 Install and Configure TVOE on First RMS (PM&C Host)

Throughout this section, the first RMS server refers to the DL380 server that shall host the PM&C VM.

Procedure 2. Install TVOE 2.0 on First RMS Server

S T E P #	This procedure will install TVOE 2.0 on the First RMS Server **Needed material:** - TVOE 2.0 Media on bootable USB Drive 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 ☐	**DL380 Server 1:** Insert TVOE Media into Server	Insert the Bootable USB Drive containg the TVOE media in a USB Port. Refer to Appendix L on how to create a bootable USB Drive. .
3 ☐	**DL380 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 ☐	**DL380 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 disk 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 ☐	**DL380 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. First RMS Configuration

S T E P #	This procedure will configure the First TVOE/Management Server **Prerequisite:** Procedure 2. Install TVOE 2.0 on First RMS Server 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 ☐	Determine Bridge names and interfaces	Determine the bridge interfaces to be used on the TVOE server and fill in the appropriate values in the table below. If netbackup is to be used, determine the bridge interface to be used for the netbackup network and fill in the <TVOE_NetBackup_Bridge_Interface> value.

Guest Interface Alias	TVOE Bridge Name	TVOE Bridge Interface
control	control	Fill in the appropriate value (default is bond0): <TVOE_Control_Bridge_Interface>
management	management	Fill in the appropriate value: <TVOE_Management_Bridge_Interface>
xmi	xmi	Fill in the appropriate value: <TVOE_XMI_Bridge_Interface>
imi	imi	Fill in the appropriate value, (default is bond0.4): <TVOE_IMI_Bridge_Interface>
xsi1	xsi1	Fill in the appropriate value: <TVOE_XSI1_Bridge_Interface>
xsi2	xsi2	Fill in the appropriate value: <TVOE_XSI2_Bridge_Interface>
netbackup (if applicable)	netbackup	Fill in the appropriate value: <TVOE_NetBackup_Bridge_Interface>

2 ☐	**1st RMS 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.
3 ☐	**1st RMS 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 and needs to be deleted. execute the following command to delete it **# netAdm delete --device=bond0** Interface bond0 updated Next execute **ONE** of the following two commands to recreate the control bridge: Option 1: Deployment with Aggregation switches (or when bond0 is connected to customer switches): **# netAdm add --device=bond0 --onboot=yes --type=Bonding --mode=active-backup --miimon=100** Interface bond0 added Option 2: Deployment without switches (i.e. when the 2 RMS servers are directly connected): **# netAdm add --device=bond0 --onboot=yes --type=Bonding --mode=active-backup --miimon=100 --primary=eth01** Interface bond0 added Execute the following to set the slave interfaces: **# 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=bond0**

4 ☐	**1st RMS iLO:** Create tagged control interface and bridge (optional)	If you are using a tagged control network interface on this TVOE Server, 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 ☐	**1st RMS iLO:** Verify/Create 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, otherwise execute option 1 **OR** option 2 below
		
		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.
		
		Option 1: Deployment with Aggregation switches:
		
		`# netAdm add --device=<TVOE_Management_Bridge_Interface>`
		`--onboot=yes`
		`Interface bond0.2 added`
		
		`# netAdm add --type=Bridge --name=management`
		`--bootproto=none --onboot=yes`
		`--address=<Management_Server_TVOE_IP>`
		`--netmask=<Management_Server_TVOE_Netmask>`
		`--bridgeInterfaces=<TVOE_Management_Bridge_Interface>`
		
		Option 2: Deployment without Aggregation switches:
		
		`# netAdm add --device=bond1`
		`--onboot=yes --type=Bonding --mode=active-backup --miimon=100`
		`Interface bond1 added`
		
		`# netAdm set --device=eth11 --type=Ethernet`
		`--master=bond1 --slave=yes --onboot=yes`
		`Interface <ethernet_interface_11> updated`
		
		`# netAdm set --device=eth12 --type=Ethernet`
		`--master-bond1 --slave=yes --onboot=yes`
		`Interface <ethernet_interface_12> updated`
		
		`# netAdm add --device=<TVOE_Management_Bridge_Interface>`
		`--onboot=yes`
		`Interface bond1.<Mgmt_VLAN_ID> added`
		
		`# netAdm add --type=Bridge --name=management`
		`--bootproto=none --onboot=yes`
		`--address=<Management_Server_TVOE_IP>`
		`--netmask=<Management_Server_TVOE_Netmask>`
		`--bridgeInterfaces=<TVOE_Management_Bridge_Interface>`
		`Interface bond1.<Mgmt_VLAN_ID> was updated.`
		`Bridge management added!`

6 ☐	**1st RMS iLO:** Create the XMI Network	Configure the XMI Network using option 1 **OR** option 2 below
		
		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.
		
		Option 1: Deployment with Aggregation switches:
		
		`# netAdm add --device=<TVOE_XMI_Bridge_Interface> --onboot=yes`
		`Interface bond0.3 added`
		
		`# netAdm add --type=Bridge --name=xmi --onboot=yes --bridgeInterfaces=<TVOE_XMI_Bridge_Interface>`
		`Interface bond0.3 was updated.`
		`Bridge xmi added!`
		
		Option 2: Deployment without Aggregation switches:
		
		`# netAdm add --device=<TVOE_XMI_Bridge_Interface> --onboot=yes`
		`Interface bond1.<XMI_VLAN_ID> added`
		
		`# netAdm add --type=Bridge --name=xmi --onboot=yes --bridgeInterfaces=<TVOE_XMI_Bridge_Interface>`
		`Interface bond1.<XMI_VLAN_ID> was updated.`
		`Bridge xmi added!`

7 ☐	**1st RMS iLO:** Create the IMI Network	Configure the IMI Network using the following commands
		
		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.
		
		`# netAdm add --device=<TVOE_IMI_Bridge_Interface> --onboot=yes`
		`Interface bond0.4 added`
		
		`# netAdm add --type=Bridge --name=imi --onboot=yes --bridgeInterfaces=<TVOE_IMI_Bridge_Interface>`
		`Interface bond0.4 was updated.`
		`Bridge imi added!`

8 ☐	**1st RMS iLO:** Create the XSI-1 Network	Execute option 1 **OR** option 2 below to configure the first XSI network
		
		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.
		
		Option 1: Deployment with Aggregation switches:
		
		`# netAdm add --device=<TVOE_XSI1_Bridge_Interface> --onboot=yes`
		`Interface bond0.5 added`
		
		`# netAdm add --type=Bridge --name=xsi1 --onboot=yes --bridgeInterfaces=<TVOE_XSI1_Bridge_Interface>`
		`Interface bond0.5 was updated.`
		`Bridge xsi1 added!`
		
		Option 2: Deployment without Aggregation switches:
		
		`# netAdm add --device=bond2 --onboot=yes --type=Bonding --mode=active-backup --miimon=100`
		`Interface bond2 added`
		
		`# netAdm set --device=eth03 --type=Ethernet --master=bond2 --slave=yes --onboot=yes`
		`Interface eth03 updated`
		
		`# netAdm set --device=eth13 --type=Ethernet --master-bond2 --slave=yes --onboot=yes`
		`Interface eth13 updated`
		
		`# netAdm add --device=<TVOE_XSI1_Bridge_Interface> --onboot=yes`
		`Interface bond2.<XSI1_VLAN_ID> added`
		
		`# netAdm add --type=Bridge --name=xsi1 --onboot=yes --bridgeInterfaces=<TVOE_XSI1_Bridge_Interface>`
		`Interface bond2.<XSI1_VLAN_ID> was updated.`
		`Bridge xsi1 added!`

9 ☐	**1st RMS iLO:** Create the XSI-2 Network	Configure the XSI2 Network using option 1 **OR** option 2 below
		
		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.
		
		Option 1: Deployment with Aggregation switches:
		
		`# netAdm add --device=<TVOE_XSI2_Bridge_Interface> --onboot=yes`
		`Interface bond0.6 added`
		
		`# netAdm add --type=Bridge --name=xsi2 --onboot=yes --bridgeInterfaces=<TVOE_XSI2_Bridge_Interface>`
		`Interface bond0.6 was updated.`
		`Bridge xsi2 added!`
		
		Option 2: Deployment without Aggregation switches:
		
		`# netAdm add --device=<TVOE_XSI2_Bridge_Interface> --onboot=yes`
		`Interface bond2.<XSI2_VLAN_ID> added`
		
		`# netAdm add --type=Bridge --name=xsi2 --onboot=yes --bridgeInterfaces=<TVOE_XSI2_Bridge_Interface>`
		`Interface bond2.<XSI2_VLAN_ID> was updated.`
		`Bridge xsi2 added!`

10 ☐	**1st RMS 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_4> --type=Ethernet`
		`--master=<TVOE_NetBackup_Bridge_Interface> --slave=yes`
		`--onboot=yes`
		`Interface <ethernet_interface_4> 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_4>`
		`--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>`

11 ☐	**1st RMS iLO:** Add/Verify the Default Route	Note: The output below is for illustrative purposes only. The example output below shows the management 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=management`
		`--gateway=<mgmt_gateway_address>`
		`Route to management added`

12 ☐	**1st RMS 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`
		
		If the NetBackup network is non-routed, use a host route instead.
		
		`# netAdm add --route=host`
		`--device=<TVOE_NetBackup_Bridge>`
		`--address=<NetBackup_Server_IP_Address>`
		`--netmask=255.255.255.255`
		`--gateway=<NetBackup_Server_IP_Address>`
		`Route to <TVOE_NetBackup_Bridge> added`

13 ☐	**1st RMS iLO:** Restart the network interfaces	Restart the network interfaces `# service network restart`

14 ☐	**1st RMS 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
15 ☐	**1st RMS 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
16 ☐	**1st RMS 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**
17 ☐	**1st RMS 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. 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.

18 ☐	**1st RMS 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`

19 ☐	**1st RMS 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**
20 ☐	**1st RMS 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.
21 ☐	**1st RMS 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, 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.

4.3 Install PM&C

Procedure 4. PM&C Deployment Procedure

S T E P #	This procedure will deploy PM&C on the TVOE Host **Prerequisite:** First RMS Network Configuration (PM&C Host) has been completed. **Needed material:** - PM&C Media on USB Drive 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 iLO:** Login and launch the integrated remote console	Using IE, log in to iLO of the RMS hosting the PM&C 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 server	Use one of the following 2 options to mount the PM&C Media: 1. If using a USB media, insert the pmac USB into a USB port and execute the following to mount the iso: **# 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/sdb1/872-2441-104-5.0.0_50.8.0-PMAC-x86_64.iso /mnt/upgrade** 2. If using an ISO image, run the following to mount it: **# mount -o loop ISO_FILENAME.iso /mnt/upgrade** Next 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. 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`

4.4 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 4.1 installation. **Needed material:** - HP Misc. Firmware USB - HP Solutions Firmware Upgrade Pack Release Notes [1] - Application USB or ISO Note: The following procedures use NetConfig to configure the switches, if switchconfig is to be used, Execute the equivalent procedure in Appendix L. 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 DSR ISO	Once the PM&C is done rebooting, SSH to the PM&C server as root using the PM&C Management Network IP. Make the upgrade media available to the server.
		
		Mount the media on the TVOE Host using one of the following commands:
		
		1. If using a USB Drive, run the following to mount it:
		
		`# ls /media/*/*.iso`
		`/media/sdb1/872-2507-109-4.1.0_41.12.1-DSR-x86_64.iso`
		
		Use the output of the previous command to populate the next command
		
		`# mount -o loop /media/sdb1/872-2507-109-4.1.0_41.12.1-DSR-x86_64.iso /mnt/upgrade`
		
		2. If the DSR in on an ISO, mount it using the following commands
		`# mount –o loop <path to DSR ISO> /mnt/upgrade`

2
☐
	Management server: Get Netconfig , csv, and other support files from the application ISO	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 /mnt/upgrade/upgrade/overlay/*`
		`root@<PMAC Management_IP Address>:/usr/TKLC/smac/etc`
		
		`# umount /mnt/upgrade`
		
		Remove the DSR 4.1 application media from the management server.

Procedure 5. Gather/Prepare Configuration Files

3 ☐	**Management server:** Copy IOS images into place (this will copy both the 4948E IOS images into place).	Insert the *Misc. Firmware USB* media into the USB drive. 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]. 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/sdb1/files/<4948E_IOS_image_filename> root@<PMAC Management_IP Address>:/var/TKLC/smac/image** 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.

4.5 Configure Cisco 4948E Aggregation 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. **Note:** A generic xml configuration file is provided in Appendix B. It needs to be updated to match the customer's network. **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	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` `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.

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

		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 skip to step 15, there is no upgrade necessary for this switch. 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`
		`service tftp`
		`{`
		`socket_type = dgram`
		`protocol = udp`
		`wait = yes`
		`user = root`
		`server = /usr/sbin/in.tftpd`

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

		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_mgmtBridge> | 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_mgmtBridge> | grep inet The command output should contain the IP address of the variable **<management_server_mgmtVLAN_ip_address>,** note it down. Issue the following command to bring the interface back up: # ifup <ethernet_interface_1> Connect to the Virtual PMAC by logging into the console of the virtual pmac instance found in step 4. # virsh console vm-pmac1A

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

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`
		`Switch(config-if)# spanning-tree portfast trunk`
		`Switch(config-if)# write mem`

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

		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 established.	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** Switch(config)# **end**

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

		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.
14 ☐	**Virtual PM&C:** Turn off the tftp service of the virtual	Issue the following command to stop the tftp service: # **tpdProvd --client --noxml --ns=Xinetd stopXinetdService service tftp**

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

	PM&C.	Login on Remote: **platcfg** Password of platcfg: **<platcfg_password>**
15 ☐	**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? <management_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

16 ☐	**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: tftp`
		`Host: 10.240.8.4`
		`Options:`
		`dir: /var/TKLC/smac/image`
		`[root@pmac5000101 ~]#`

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

17 ☐	**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.
		
		`# 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

18 ☐	**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

19 ☐	**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

20 ☐	**Virtual PM&C:** Modify configure xml file with information needed to initialize the switch.	Extract the configuration files from the zip file copied in procedure 5 # **cd /usr/TKLC/smac/etc** # **unzip DSR4.X_NetConfig_Templates.zip** This will create a directory called **DSR4.X_NetConfig_Templates** which contains all the necessary configuration files. Copy the following files using the following commands # **cp DSR4.X_NetConfig_Templates/init/Aggregation/*.xml .** # **cp DSR4.X_NetConfig_Templates /config/DSR_RMS_Productization/4948E-F_L3_configure.xml .** 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**
21 ☐	**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.
22 ☐	**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

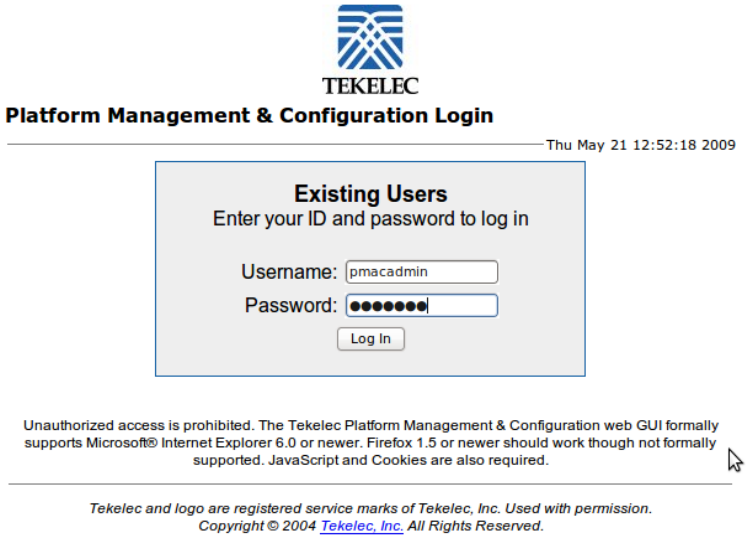
23 ☐	**Virtual PM&C:** Configure the switches	Configure both switches by issuing the following command: # **netConfig --file=/usr/TKLC/smac/etc/4948_4948E_configure.xml** Processing file: /usr/TKLC/smac/etc/4948_4948E_configure.xml **Note:** This step takes about 2-3 minutes to complete. Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Customer Care Center.
24 ☐	**Virtual PM&C:** Verify switch configuration	Ping each of the interfaces to verify switch configuration # **ping <switch1A_mgmtVLANIP>** # **ping <switch1B_mgmtVLANIP>**
25 ☐	**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.
26 ☐	**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>**
27 ☐	**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.
28 ☐	**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>**
29 ☐	**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

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

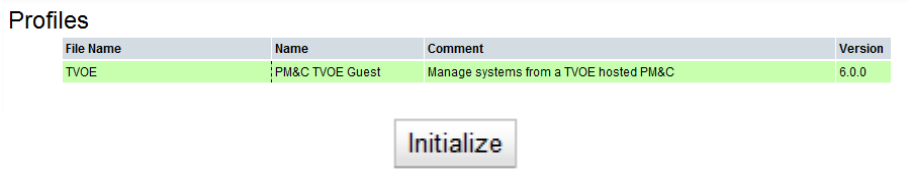
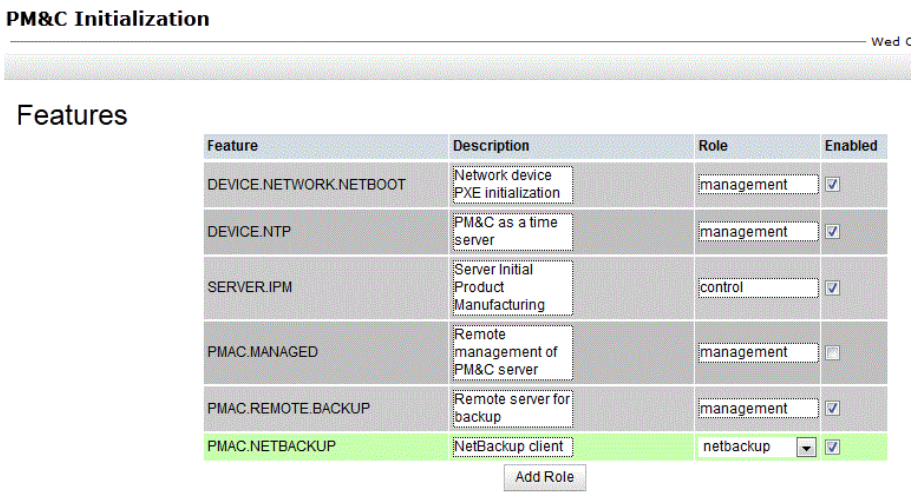
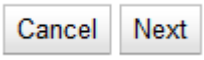
30 ☐	**Virtual PMAC:** Backup Switch Configuration	Ensure the directory where the backups will be stored exists using the following command: # **ls /usr/TKLC/smac/etc/switch/backup** If an error is returned saying "No such file or directory", then create the directory using the following command # **mkdir /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.

4.6 Configure PM&C Server

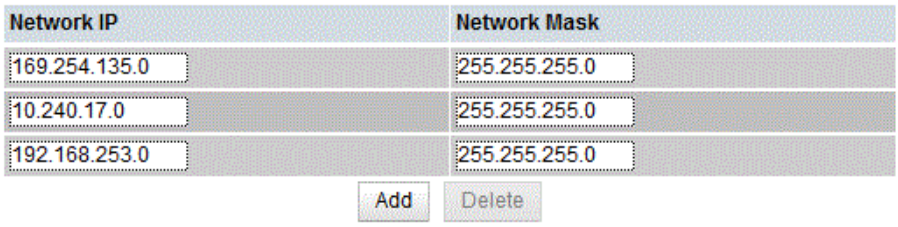
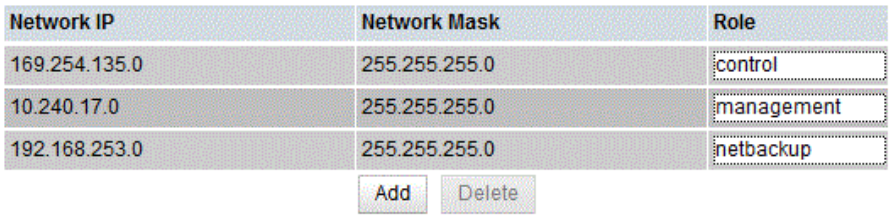
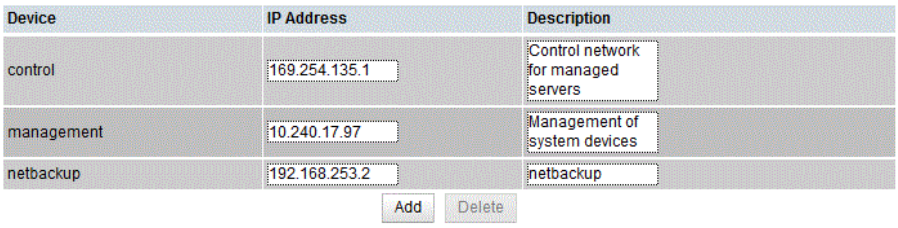
Procedure 7. Configure the PM&C Server

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://<pmac_network_ip>/gui`** Login as pmacadmin user. 

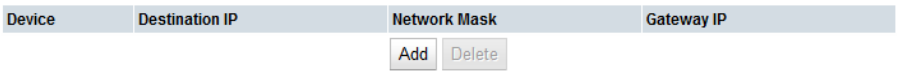
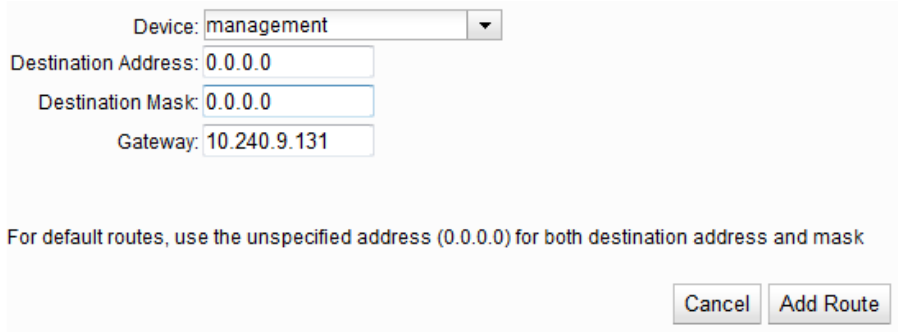
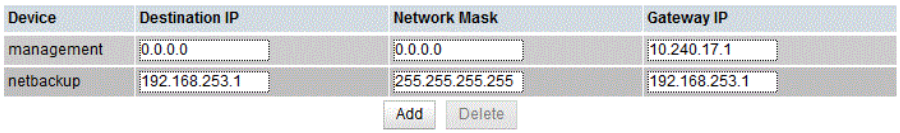
Procedure 7. Configure the PM&C Server

2 ☐	**PM&C GUI:** Select a profile	The first screen will be similar to image below.  Select the TVOE profile and click on **Initialize**, the following features screen will display  Make sure that the roles for DEVICE.NETWORK.NETBOOTand 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.NETBACK (only if NetBackup is used) And click on **Next.** 

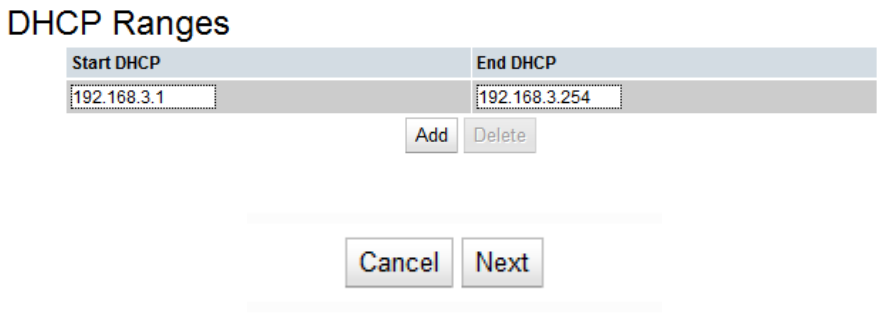
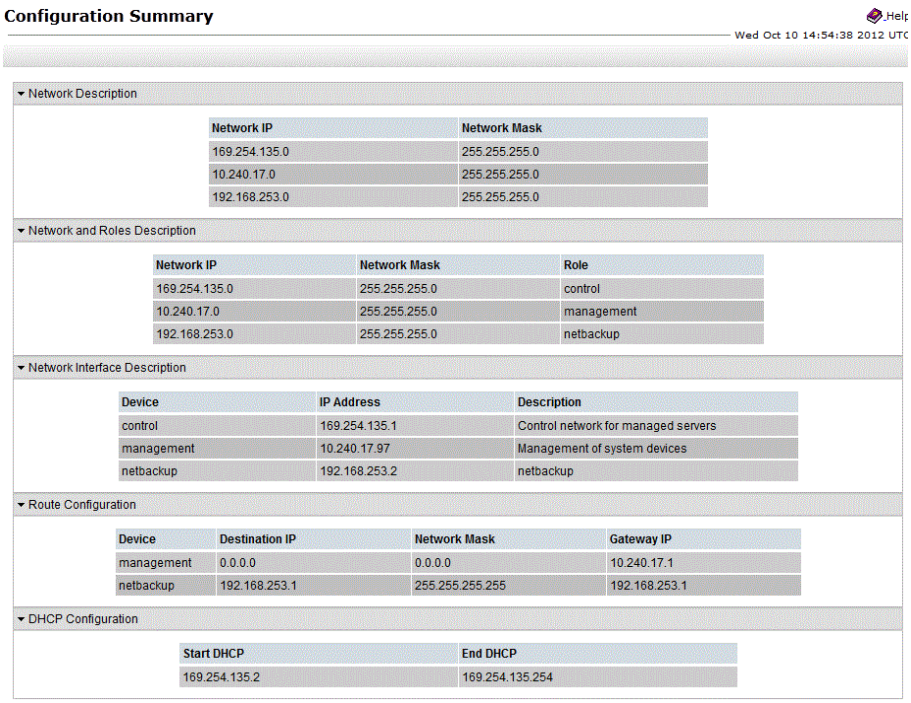
Procedure 7. Configure the PM&C Server

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`**.
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`**.

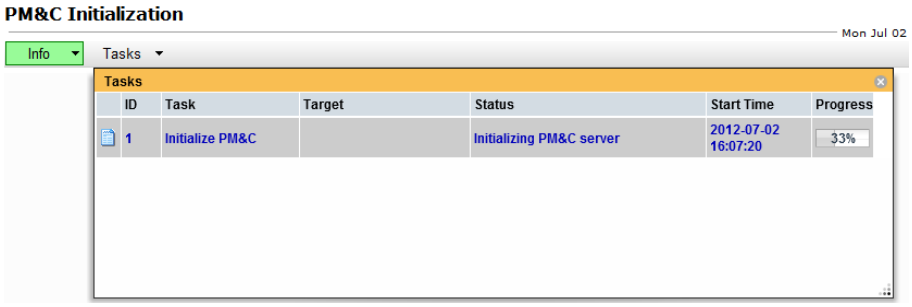
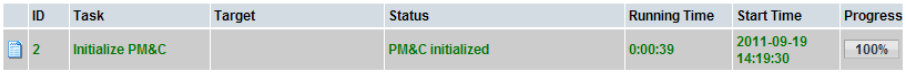
Procedure 7. Configure the PM&C Server

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 NetBacup Rote **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.`

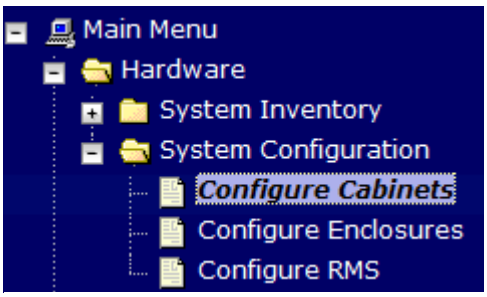
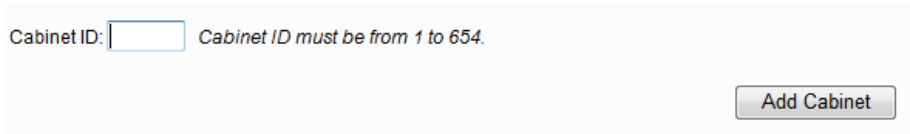
Procedure 7. Configure the PM&C Server

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.

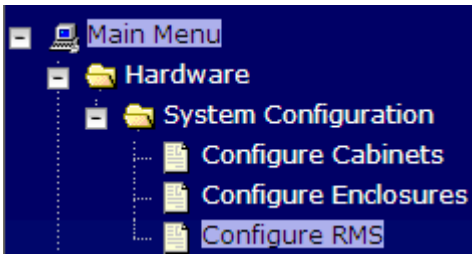
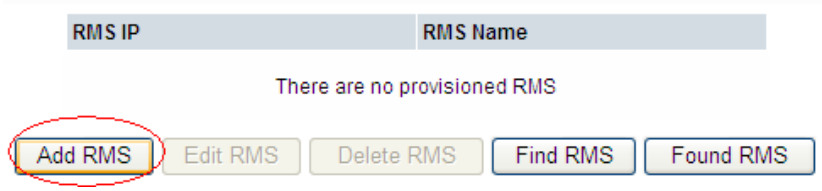
12 ☐	**PM&C Command Line:** Perform a backup	Perform PM&C application backup using the following command:
		
		`# pmacadm backup`
		`PM&C backup been successfully initiated as task ID 7`
		`[root@PMACDev3 ~]#`
		
		Note: The "pmacadm backup" command uses a naming convention which includes a date/time 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. The backup file is located under `/var/TKLC/smac/backup`.

4.7 Install TVOE on second RMS

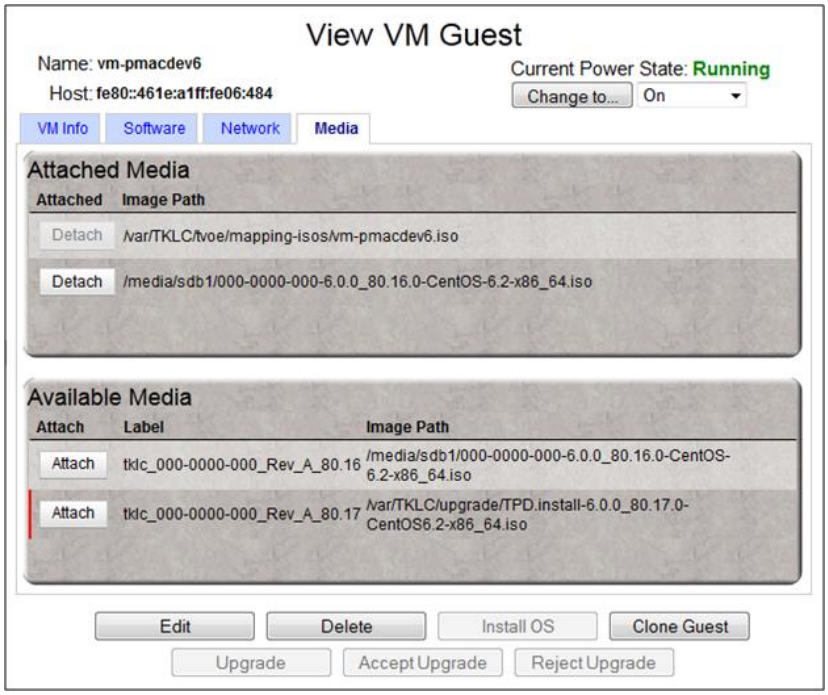
Procedure 8. Install TVOE on Second RMS

S T E P #	This procedure will install the TVOE operating system on the second Rack Mounted Servers. **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 Cabinet housing the RMS Servers	Navigate to **Main Menu -> Hardware -> System Configuration -> Configure Cabinets**.  Click **Add Cabinet**
3 ☐	**PM&C GUI:** Enter Cabinet ID	Enter a Cabinet ID (ID should be between 1 and 654) and click **Add Cabinet** 

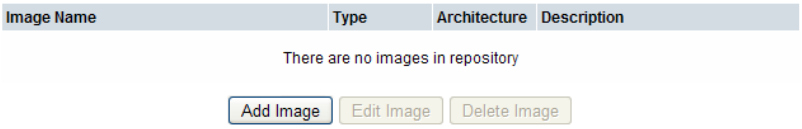
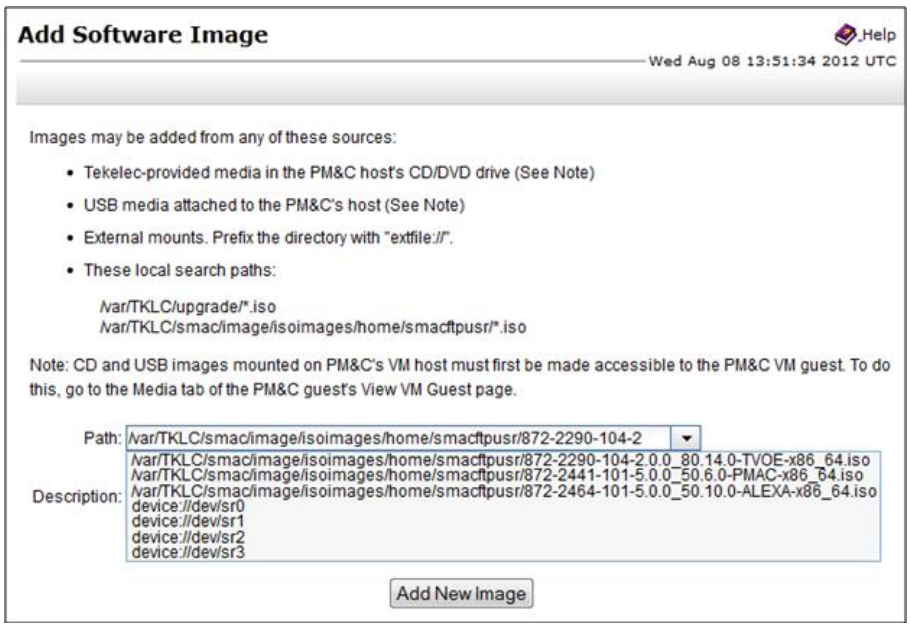
Procedure 8. Install TVOE on Second RMS

4 ☐	**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 be displayed. **REPEAT THIS STEP FOR ANY ADDITIONAL RMSes YOU WISH THE PMAC TO CONFIGURE.**

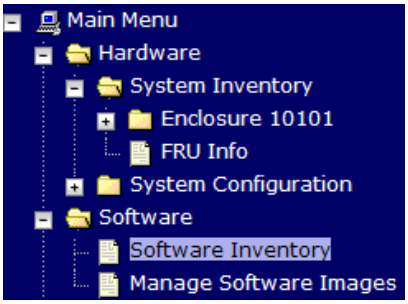
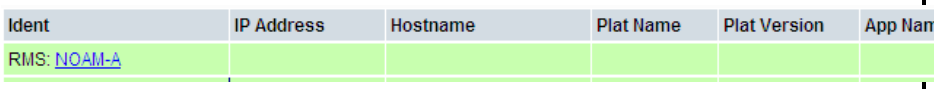
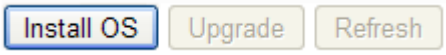
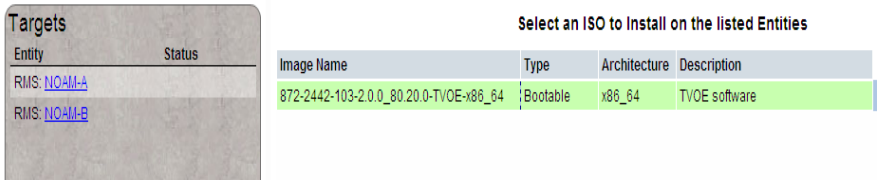
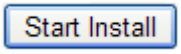
Procedure 8. Install TVOE on Second RMS

5 ☐	**TVOE Host:** Load TVOE 2.0 ISO	Add the TVOE ISO image to the PM&C, this can be done in one of two ways: 1. Attach the USB device containing the ISO image to a USB port. Open a web browser and enter: **http://<management_server_ip>**. Login as pmacadmin user and navigate 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.  2. 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/`

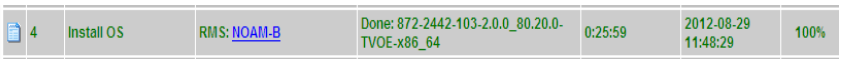
Procedure 8. Install TVOE on Second RMS

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 8. Install TVOE on Second RMS

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 8. Install TVOE on Second RMS

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 9. Configure TVOE on Second RMS Server

S T E P #	This procedure will configure TVOE on the second RMS Servers. **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 9. Configure TVOE on Second RMS Server

<table>
<tr>
<td>1
☐</td>
<td>Determine Bridge names and interfaces</td>
<td>Determine the bridge interfaces to be used on the TVOE server and fill in the appropriate values in the table below. If netbackup is to be used, determine the bridge interface to be used for the netbackup network.

The entries in this table should match the table that was filled out for the first RMS in procedure 3, step 1.

<table>
<tr><th>Guest 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>management</td><td>Fill in the appropriate value:

_____

<TVOE_Management_Bridge_Interface></td></tr>
<tr><td>xmi</td><td>xmi</td><td>Fill in the appropriate value:

_____

<TVOE_XMI_Bridge_Interface></td></tr>
<tr><td>imi</td><td>imi</td><td>Fill in the appropriate value, (default is bond0.4):

_____

<TVOE_IMI_Bridge_Interface></td></tr>
<tr><td>xsi1</td><td>xsi1</td><td>Fill in the appropriate value:

_____

<TVOE_XSI1_Bridge_Interface></td></tr>
<tr><td>xsi2</td><td>xsi2</td><td>Fill in the appropriate value:

_____

<TVOE_XSI2_Bridge_Interface></td></tr>
<tr><td>netbackup
(if applicable)</td><td>netbackup</td><td>Fill in the appropriate value:

_____

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

Procedure 9. Configure TVOE on Second RMS Server

2 ☐	**2nd RMS iLO:** Login and launch the integrated remote console	Log in to iLO in IE using password provided by application: **http://<second_rms_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.
3 ☐	**2nd RMS 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, execute the following command to set the primary slave interface and skip to step 4: **# netAdm set --device=bond0 --onboot=yes --type=Bonding --mode=active-backup --miimon=100 --primary=eth01** Interface bond0 updated Otherwise execute the following: Create control bridge: **# netAdm add --device=bond0 --onboot=yes --type=Bonding --mode=active-backup --miimon=100 --primary=eth01** Interface bond0 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=bond0**

Procedure 9. Configure TVOE on Second RMS Server

4 ☐	**2nd RMS iLO:** Create tagged control interface and bridge (optional)	If you are using a tagged control network interface on this TVOE Server, 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>`

Procedure 9. Configure TVOE on Second RMS Server

5 ☐	**2nd RMS iLO:** Verify/Create 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, otherwise execute option 1 **OR** option 2 below
		
		Option 1: Deployment with Aggregation switches:
		
		`# netAdm add --device=<TVOE_Management_Bridge_Interface>`
		`--onboot=yes`
		`Interface bond0.2 added`
		
		`# netAdm add --type=Bridge --name=management`
		`--bootproto=none --onboot=yes`
		`--address=<Management_Server_TVOE_IP>`
		`--netmask=<Management_Server_TVOE_Netmask>`
		`--bridgeInterfaces=<TVOE_Management_Bridge_Interface>`
		
		Option 2: Deployment without Aggregation switches:
		
		`# netAdm add --device=bond1`
		`--onboot=yes --type=Bonding --mode=active-backup --miimon=100`
		`Interface bond1 added`
		
		`# netAdm set --device=eth11 --type=Ethernet`
		`--master=bond1 --slave=yes --onboot=yes`
		`Interface <ethernet_interface_11> updated`
		
		`# netAdm set --device=eth12 --type=Ethernet`
		`--master-bond1 --slave=yes --onboot=yes`
		`Interface <ethernet_interface_12> updated`
		
		`# netAdm add --device=<TVOE_Management_Bridge_Interface>`
		`--onboot=yes`
		`Interface bond1.<Mgmt_VLAN_ID> added`
		
		`# netAdm add --type=Bridge --name=management`
		`--bootproto=none --onboot=yes`
		`--address=<Management_Server_TVOE_IP>`
		`--netmask=<Management_Server_TVOE_Netmask>`
		`--bridgeInterfaces=<TVOE_Management_Bridge_Interface>`
		`Interface bond1.<Mgmt_VLAN_ID> was updated.`
		`Bridge management added!`

Procedure 9. Configure TVOE on Second RMS Server

6 ☐	**2nd RMS iLO:** Create the XMI Network	Configure the XMI Network using option 1 **OR** option 2 below
		
		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.
		
		Option 1: Deployment with Aggregation switches:
		
		`# netAdm add --device=<TVOE_XMI_Bridge_Interface> --onboot=yes`
		`Interface bond0.3 added`
		
		`# netAdm add --type=Bridge --name=xmi --onboot=yes --bridgeInterfaces=<TVOE_XMI_Bridge_Interface>`
		`Interface bond0.3 was updated.`
		`Bridge xmi added!`
		
		Option 2: Deployment without Aggregation switches:
		
		`# netAdm add --device=<TVOE_XMI_Bridge_Interface> --onboot=yes`
		`Interface bond1.<XMI_VLAN_ID> added`
		
		`# netAdm add --type=Bridge --name=xmi --onboot=yes --bridgeInterfaces=<TVOE_XMI_Bridge_Interface>`
		`Interface bond1.<XMI_VLAN_ID> was updated.`
		`Bridge xmi added!`

7 ☐	**2nd RMS iLO:** Create the IMI Network	Configure the IMI Network using the following commands
		
		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.
		
		`# netAdm add --device=<TVOE_IMI_Bridge_Interface> --onboot=yes`
		`Interface bond0.4 added`
		
		`# netAdm add --type=Bridge --name=imi --onboot=yes --bridgeInterfaces=<TVOE_IMI_Bridge_Interface>`
		`Interface bond0.4 was updated.`
		`Bridge imi added!`

Procedure 9. Configure TVOE on Second RMS Server

8 ☐	**2nd RMS iLO:** Create the XSI-1 Network	Execute option 1 **OR** option 2 below to configure the first XSI network
		
		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.
		
		Option 1: Deployment with Aggregation switches:
		
		`# netAdm add --device=<TVOE_XSI1_Bridge_Interface> --onboot=yes`
		`Interface bond0.5 added`
		
		`# netAdm add --type=Bridge --name=xsi1 --onboot=yes --bridgeInterfaces=<TVOE_XSI1_Bridge_Interface>`
		`Interface bond0.5 was updated.`
		`Bridge xsi1 added!`
		
		Option 2: Deployment without Aggregation switches:
		
		`# netAdm add --device=bond2 --onboot=yes --type=Bonding --mode=active-backup --miimon=100`
		`Interface bond2 added`
		
		`# netAdm set --device=eth03 --type=Ethernet --master=bond2 --slave=yes --onboot=yes`
		`Interface eth03 updated`
		
		`# netAdm set --device=eth13 --type=Ethernet --master-bond2 --slave=yes --onboot=yes`
		`Interface eth13 updated`
		
		`# netAdm add --device=<TVOE_XSI1_Bridge_Interface> --onboot=yes`
		`Interface bond2.<XSI1_VLAN_ID> added`
		
		`# netAdm add --type=Bridge --name=xsi1 --onboot=yes --bridgeInterfaces=<TVOE_XSI1_Bridge_Interface>`
		`Interface bond2.<XSI1_VLAN_ID> was updated.`
		`Bridge xsi1 added!`

Procedure 9. Configure TVOE on Second RMS Server

9 ☐	**2nd RMS iLO:** Create the XSI-2 Network	Configure the XSI2 Network using option 1 **OR** option 2 below
		
		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.
		
		Option 1: Deployment with Aggregation switches:
		
		`# netAdm add --device=<TVOE_XSI2_Bridge_Interface> --onboot=yes`
		`Interface bond0.6 added`
		
		`# netAdm add --type=Bridge --name=xsi2 --onboot=yes --bridgeInterfaces=<TVOE_XSI2_Bridge_Interface>`
		`Interface bond0.6 was updated.`
		`Bridge xsi2 added!`
		
		Option 2: Deployment without Aggregation switches:
		
		`# netAdm add --device=<TVOE_XSI2_Bridge_Interface> --onboot=yes`
		`Interface bond2.<XSI2_VLAN_ID> added`
		
		`# netAdm add --type=Bridge --name=xsi2 --onboot=yes --bridgeInterfaces=<TVOE_XSI2_Bridge_Interface>`
		`Interface bond2.<XSI2_VLAN_ID> was updated.`
		`Bridge xsi2 added!`

Procedure 9. Configure TVOE on Second RMS Server

10 ☐	**2nd RMS 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 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_4> --type=Ethernet --master=<TVOE_NetBackup_Bridge_Interface> --slave=yes --onboot=yes`
		`Interface <ethernet_interface_4> 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_4> --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>`

Procedure 9. Configure TVOE on Second RMS Server

11 ☐	**2nd RMS iLO:** Add/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=management`
		`--gateway=<mgmt_gateway_address>`
		`Route to management added`

12 ☐	**2nd RMS 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`
		
		If the NetBackup network is non-routed, use a host route instead.
		
		`# netAdm add --route=host`
		`--device=<TVOE_NetBackup_Bridge>`
		`--address=<NetBackup_Server_IP_Address>`
		`--netmask=255.255.255.255`
		`--gateway=<NetBackup_Server_IP_Address>`
		`Route to <TVOE_NetBackup_Bridge> added`

13 ☐	**2nd RMS 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
14 ☐	**2nd RMS 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

Procedure 9. Configure TVOE on Second RMS Server

15 ☐	**2nd RMS 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**
16 ☐	**2nd RMS 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. 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.

Procedure 9. Configure TVOE on Second RMS Server

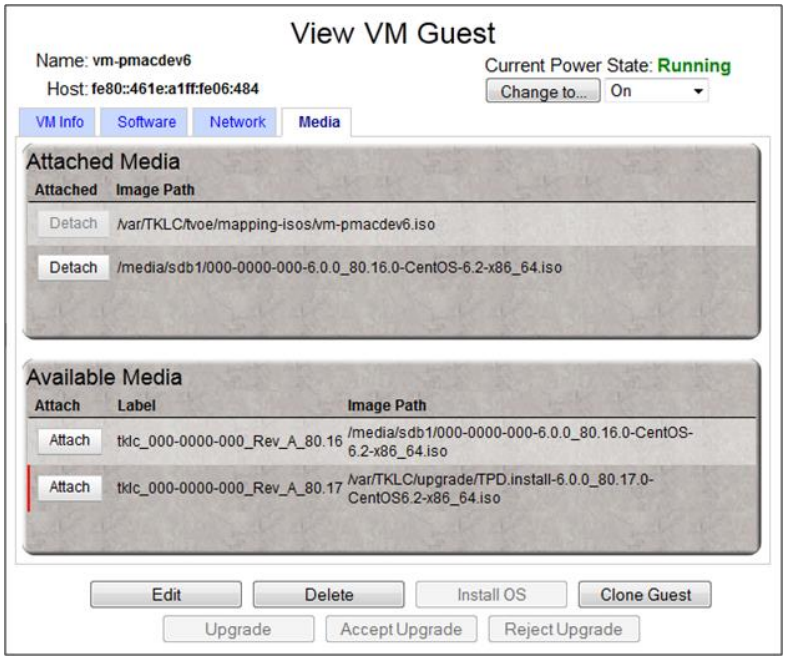
17 ☐	**2nd RMS iLO:** Configure NetBackup (Optional)	If the NetBackup feature is enabled for this system, configure the appropriate NetBackup client on the PM&C TVOE host.
		
		1. Enable and start the TVOE-netbackup service using the following commands:
		
		`# service_conf add TVOE-netbackup rc runlevels=345`
		`# 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`

Procedure 9. Configure TVOE on Second RMS Server

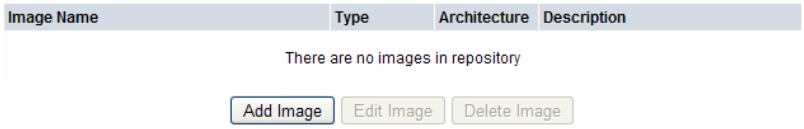
18 ☐	**2nd RMS iLO:** Setup syscheck	syscheck must be configured to monitor bonded interfaces. Replace "bondedInterfaces" with "bond0" or "bond0,bond1" if segregated networks are used: # **syscheckAdm net ipbond --set --var=DEVICES --val=<bondedInterfaces>** # **syscheckAdm net ipbond --enable** # **syscheck -v net ipbond**
19 ☐	**2nd RMS 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.
20 ☐	**2nd RMS 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, 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.

4.8 Create Virtual Machines for Applications

Procedure 10. Load ISOs onto PM&C Server

S T E P #	This procedure will load TPD and the DSR Application ISO into the PM&C Server **Needed material:** - TPD and 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 ☐	**1st RMS TVOE Host:** Load TPD Image	Add the TPD ISO image to the PM&C, this can be done in one of two ways: 1. Attach the USB device containing the ISO image to a USB port. Open a web browser and enter: **http://<management_server_ip>**. Login as pmacadmin user and navigate 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.  2. Using a TPD **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 <TPD_image>.iso root@<pmac_management_network_ip>:/var/TKLC/smac/image/isoimages/home/smacftpusr/`

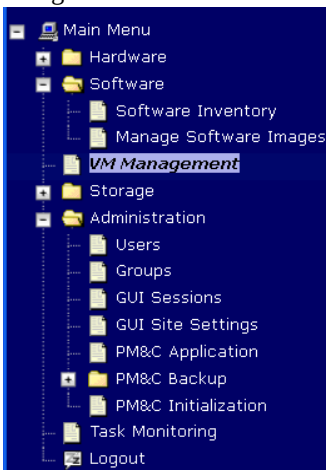
Procedure 10. Load ISOs onto PM&C Server

2 ☐	**PM&C GUI:** Add TPD image	Open web browser and enter: **http://<management_server_ip>**. Login as pmacadmin user and 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 TPD Media from the optical drive of the server.

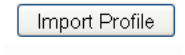
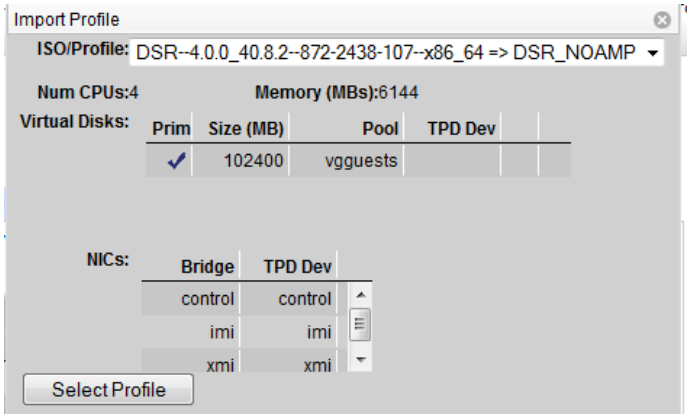
Procedure 10. Load ISOs onto PM&C Server

3 ☐	**PM&C GUI:** Add Application image	Repeat this procedure to load the DSR application onto the PM&C, using either a DSR media or ISO.

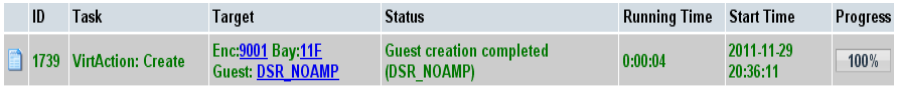
Procedure 11. Create NOAMP Guest VMs

STEP #		
	This procedure will provide the steps needed to create a DSR NOAMP virtual machine (refered to as a "guest") on a TVOE server 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 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 RMS 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 on **`Create Guest`**.

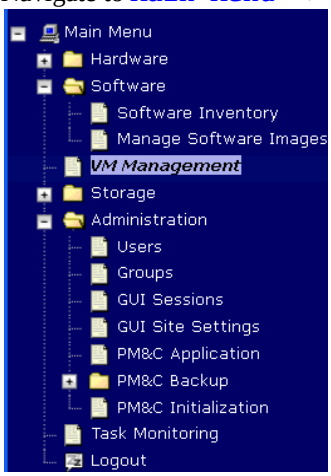
Procedure 11. Create NOAMP Guest VMs

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_NETBACK_RMS - If your NOAMP **DOES** require a dedicated ethernet port for NetBackup • <Application ISO NAME>➔DSR_NOAMP_RMS - If your NOAMP **DOES NOT** 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**

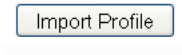
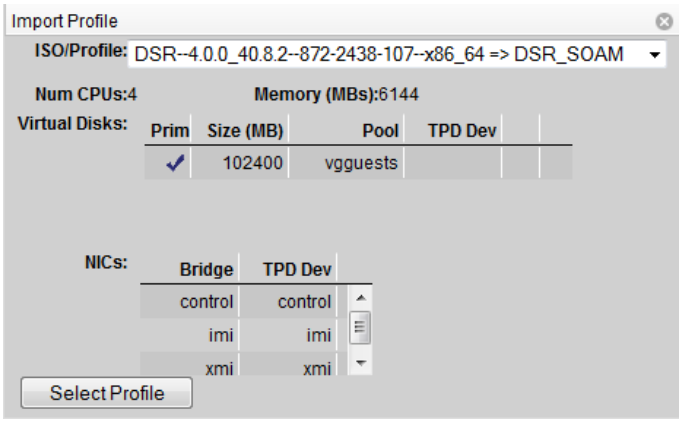
Procedure 11. Create NOAMP Guest VMs

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.  ID / Task / Target / Status / Running Time / Start Time / Progress 1739 / VirtAction: Create / Enc:9001 Bay:11F Guest: DSR_NOAMP / Guest creation completed (DSR_NOAMP) / 0:00:04 / 2011-11-29 20:36:11 / 100%
5 ☐	**PM&C GUI:** Verify Guest Machine is Running	Navigate to **Main Menu -> VM Management** Select the RMS 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”.
6 ☐	**Repeat for Second RMS**	VM Creation for this guest is complete. Repeat from Step 2 to step 5 for the second RMS Server that shall host the second NOAMP.

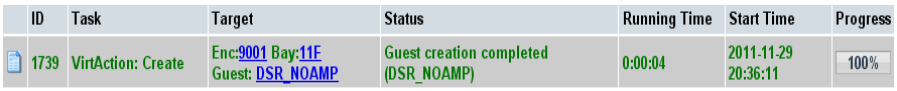
Procedure 12. Create SOAM Guest VMs

S T E P #	This procedure will provide the steps needed to create a DSR SOAM virtual machine (refered to as a "guest") on a TVOE server. It must be repeated for every SOAM server you wish to install. **Prerequisite**: TVOE has been installed and configured on the target 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 RMS from the "VM Entities" listing on the left side of the screen. This RMS guest machine configuration will then be displayed in the remaining area of the window. Click on **`Create Guest`**.

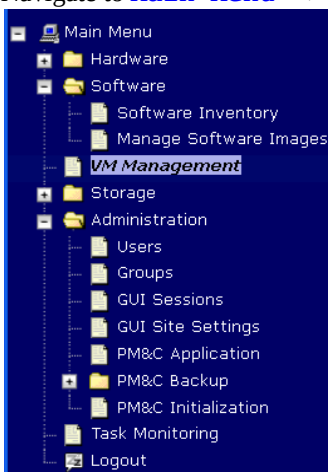
Procedure 12. Create SOAM Guest VMs

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_RMS 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**

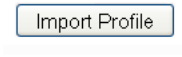
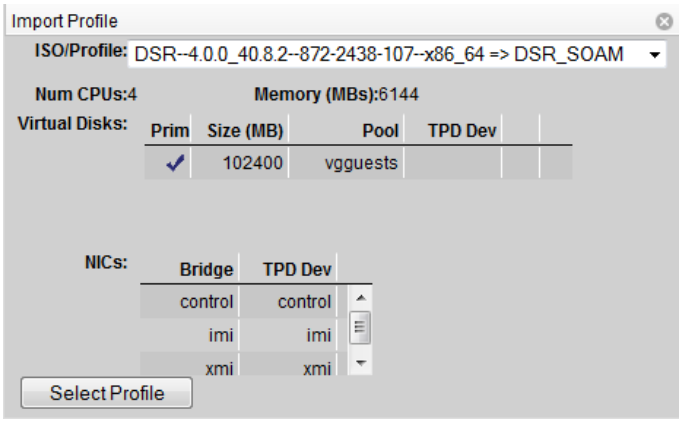
Procedure 12. Create SOAM Guest VMs

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 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”.
6 ☐	**Repeat for second RMS Server**	**VM Creation for this guest is complete. Repeat from Step 2 to step 5 for the second RMS Server that shall host the second SOAMP.**

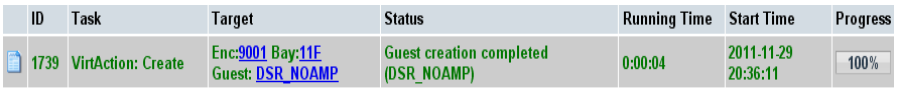
Procedure 13. Create MP Guest VMs

S T E P #	This procedure will provide the steps needed to create a DSR MP virtual machine (refered to as a "guest") on a TVOE server. It must be repeated for every server you wish to install. **Prerequisite**: TVOE has been installed and configured on the target 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 RMS server 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.`**

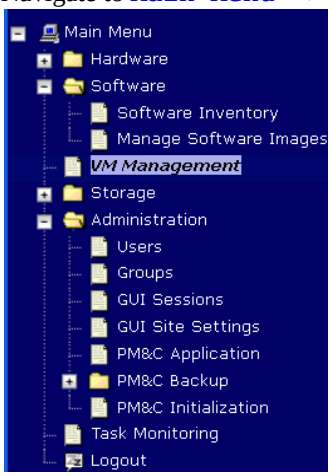
Procedure 13. Create MP Guest VMs

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_MP_RMS Where Application_ISO_NAME is the name of the DSR Appilcation ISO to be installed on this MP. 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_MP_A," or DSR_MP_B". **(This will not become the ultimate hostname. It is just an internal tag for the VM host manager.)** Press **Create**

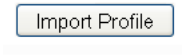
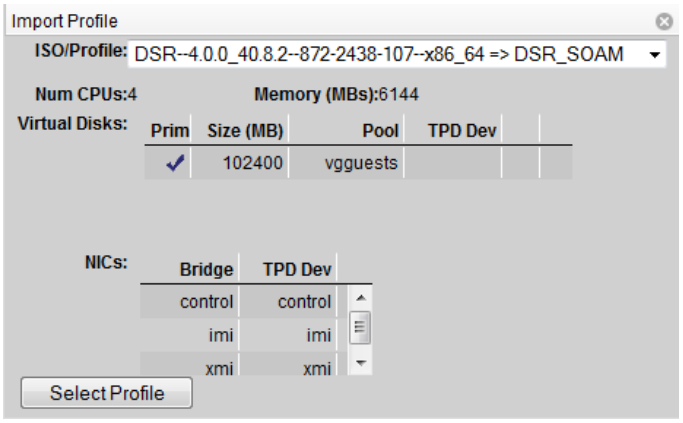
Procedure 13. Create MP Guest VMs

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 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”.
6 ☐	**Repeat for second RMS Server**	**VM Creation for this guest is complete. Repeat from Step 2 to step 5 for the second RMS Server that shall host the second MP.**

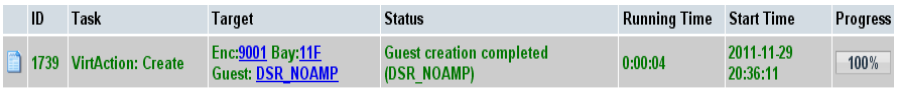
Procedure 14. Create IPFE Guest VMs (Optional)

S T E P #	This procedure will provide the steps needed to create an IFPE virtual machine (refered to as a "guest") on a TVOE server. It must be repeated for every server you wish to install. **Prerequisite**: TVOE has been installed and configured on the target 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 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 14. Create IPFE Guest VMs (Optional)

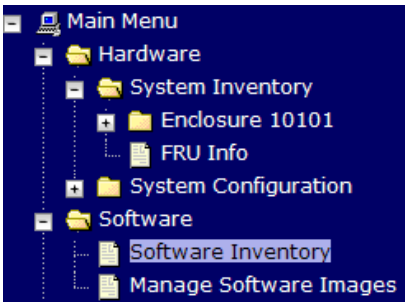
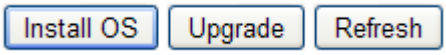
3 ☐	**PM&C GUI:** Configure VM Guest Parameters	Press **Import Profile**   From the "ISO/Profile" drop-down box, select the entry that matches <Application ISO NAME>➔DSR_IPFE_RMS Where Application_ISO_NAME is the name of the DSR Appilcation ISO to be installed on this MP. Press **Select Profile**. Values 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_IPFE_A," or DSR_IPFE_B". (**This will not become the ultimate hostname. It is just an internal tag for the VM host manager.)** Press **Create**

Procedure 14. Create IPFE Guest VMs (Optional)

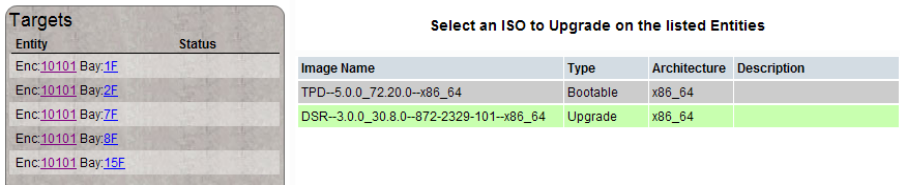
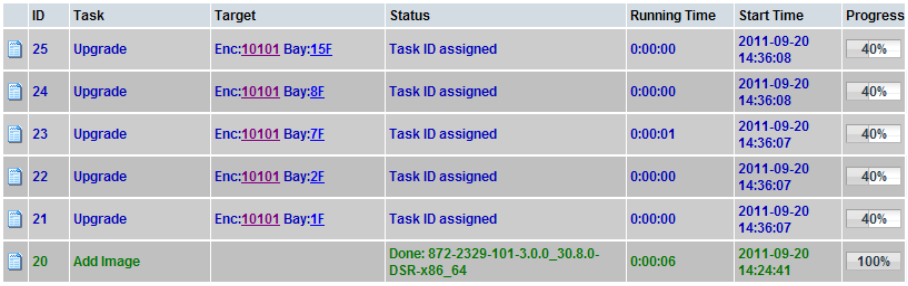
4 ☐	**PM&C GUI:** Wait for Guest Creation to Complete	Navigate to **Main Menu** > **Task Monitoring** to monitor the progress of the guest creation task.. A separate task will appear for each guest creation that you have launched. Wait or referesh the screen until you see that the guest creation task has completed successfully.  ID / Task / Target / Status / Running Time / Start Time / Progress 1739 / VirtAction: Create / Enc:9001 Bay:11F Guest: DSR_NOAMP / Guest creation completed (DSR_NOAMP) / 0:00:04 / 2011-11-29 20:36:11 / 100%
5 ☐	**PM&C GUI:** Verify Guest Machine is Running	Navigate to **Main Menu -> VM Management** Select the TVOE server 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”.
6 ☐	**Repeat for second RMS Server**	**VM Creation for this guest is complete. Repeat from Step 2 to step 5 for the second RMS Server that shall host the second IPFE.**

4.9 Install Software on Virtual Machiness

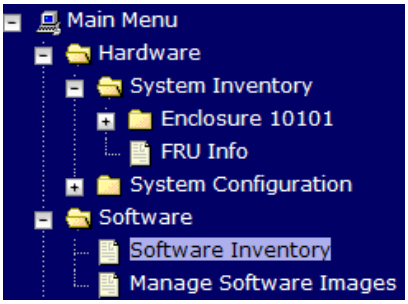
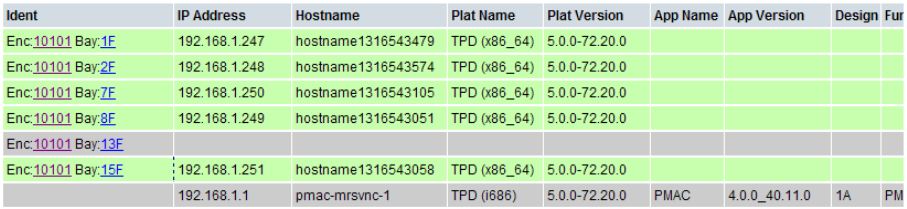
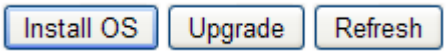
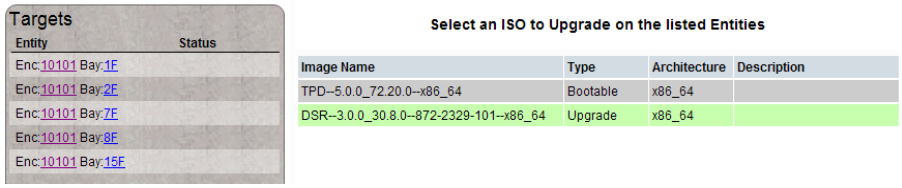
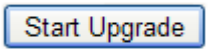
Procedure 15. Install the Software on the VMs

S T E P #		
	This procedure will provide the steps to install Diameter Signaling Router 4.0 on the Blade servers. **Prerequisite**: VM Guests Creationhas 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.
2 ☐	**PM&C GUI:** Select Servers for Application install	Navigate to **`Software -> Software Inventory`**.  Select the servers on which TPD is to be installed (should be the NO, SO, MP and IPFE VMs). You may select multiple servers by pressing <Ctrl> and 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 server that hosts them. Ident / IP Address / Hostname / Plat Name / Plat Version / App Name / App Version / Design / Fur Enc:10101 Bay:1F / 192.168.1.247 / hostname1316543479 / TPD (x86_64) / 5.0.0-72.20.0 Enc:10101 Bay:2F / 192.168.1.248 / hostname1316543574 / TPD (x86_64) / 5.0.0-72.20.0 Enc:10101 Bay:7F / 192.168.1.250 / hostname1316543105 / TPD (x86_64) / 5.0.0-72.20.0 Enc:10101 Bay:8F / 192.168.1.249 / hostname1316543051 / TPD (x86_64) / 5.0.0-72.20.0 Enc:10101 Bay:13F Enc:10101 Bay:15F / 192.168.1.251 / hostname1316543058 / TPD (x86_64) / 5.0.0-72.20.0 192.168.1.1 / pmac-mrsvnc-1 / TPD (i686) / 5.0.0-72.20.0 / PMAC / 4.0.0_40.11.0 / 1A / PM Click on **`Install OS`** 

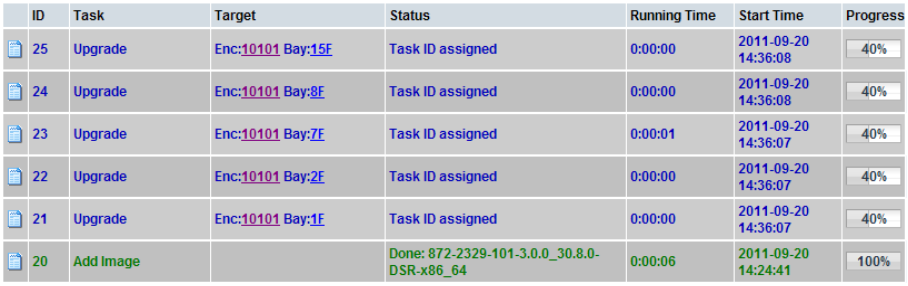
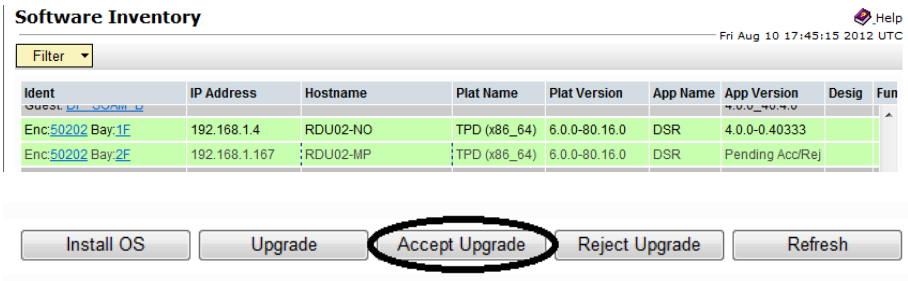
Procedure 15. Install the Software on the VMs

3 ☐	**PM&C GUI:** Initiate TPD 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.  Targets Entity Status Enc:10101 Bay:1F Enc:10101 Bay:2F Enc:10101 Bay:7F Enc:10101 Bay:8F Enc:10101 Bay:15F Select an ISO to Upgrade on the listed Entities Image Name Type Architecture Description TPD--5.0.0_72.20.0--x86_64 Bootable x86_64 DSR--3.0.0_30.8.0--872-2329-101--x86_64 Upgrade x86_64 Click on **Start Install**, a confirmation window will pop up, click on **Ok** to proceed with the install.
4 ☐	**PM&C GUI:** Monitor the TPD installation status	Navigate to **Main Menu** > **Task Monitoring** to monitor the progress of the TPD Installation. A separate task will appear for each blade affected.  ID Task Target Status Running Time Start Time Progress 25 Upgrade Enc:10101 Bay:15F Task ID assigned 0:00:00 2011-09-20 14:36:08 40% 24 Upgrade Enc:10101 Bay:8F Task ID assigned 0:00:00 2011-09-20 14:36:08 40% 23 Upgrade Enc:10101 Bay:7F Task ID assigned 0:00:01 2011-09-20 14:36:07 40% 22 Upgrade Enc:10101 Bay:2F Task ID assigned 0:00:00 2011-09-20 14:36:07 40% 21 Upgrade Enc:10101 Bay:1F Task ID assigned 0:00:00 2011-09-20 14:36:07 40% 20 Add Image Done: 872-2329-101-3.0.0_30.8.0-DSR-x86_64 0:00:06 2011-09-20 14:24:41 100% When the installation is complete, the task will change to green and the Progress bar will indicate "100%". Wait until all “Install OS” tasks are complete.

Procedure 15. Install the Software on the VMs

5 ☐	**PM&C GUI:** Select Servers for Application install	Navigate to **Software -> Software Inventory**.  Select the servers on which the DSR application is to be installed (should be the NO, SO, MP and IPFE VMs). You may select multiple servers by pressing <Ctrl> and 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 server that hosts them. .  Click on **Upgrade** 
6 ☐	**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 the DSR application 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 15. Install the Software on the VMs

7 ☐	**PM&C GUI:** Monitor the installation status	Navigate to **Main Menu** > **Task Monitoring** to monitor the progress of the Application Installation. 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 "Upgrade" tasks are complete.
8 ☐	**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 in certain instances, 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.

4.10 Application Configuration

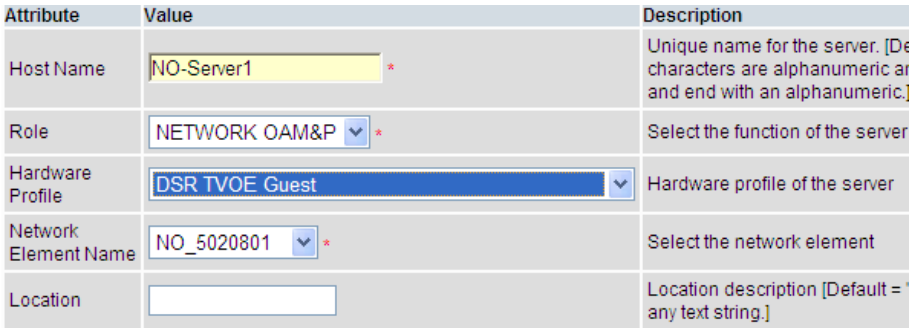
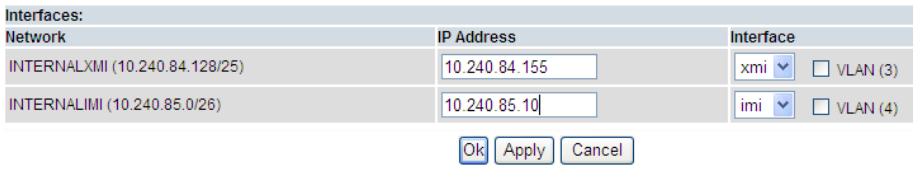
Procedure 16. Configure the First NOAMP NE and Server

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 4.1 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 [2]. 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 4.12Appendix G.** 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 16. 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 ComAgent / ***<IMI Network>*** / Unspecified For example, if your IMI network is named "INTERNALIMI" and your XMI network is named „INTERNALXMI", then your services should config should look like the following: Services Name / Intra-NE Network / Inter-NE Network OAM / INTERNALIMI / INTERNALXMI Replication / INTERNALIMI / INTERNALXMI Signaling / Unspecified / Unspecified ComAgent / INTERNALIMI / Unspecified Ok Apply Cancel Select the "Ok" button to apply the Service-to-Network selections.

Procedure 16. 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**. Next, add the following NTP servers (DSR 5.X and up): **NTP Server** | **Preferred?** ***<RMS1-TVOE-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 16. 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 4.12Appendix 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 4.12Appendix I. `# /usr/TKLC/appworks/bin/set_ini_tz.pl "Etc/UTC" >/dev/null 2>&1`
12 ☐	**Reboot the Server**	Run the following command to 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 17. 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
4 ☐	**Verify NOAMP blade server role**	From terminal window to the first NOAMP VM, execute the **`ha.states`** command to verify that the "DbReplication" 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
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 18. Configure the Second NOAMP Server

S T E P	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.	
1 ☐	**Exchange SSH keys between PMAC and second NOAMP server**	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>**
2 ☐	**NOAMP GUI:** Login	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.
3 ☐	**Insert the 2nd NOAMP server**	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**. Next, add the following NTP servers (DSR 5.X and up): **NTP Server**: ***<RMS2-TVOE-IP-Address>*** — **Preferred?**: Yes Select the **Ok** button when you have completed entering the server data.
4 ☐	**Export the initial configuration**	From the GUI screen, select the second server and then select **Export** action button to generate the initial configuration data for that server.

Procedure 18. 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 PMAC serve (on the management network), - the server inventory will be presented, - prompted for the Control network IP address for the target server (in this case, the second NOAMP server). - prompted for the hostname of the target server,
6 ☐	**Wait for Configuration to Complete**	Obtain a terminal window connection on the 2nd NOAMP (Use the procedure in Appendix 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` **NOTE**: Ignore the warning about removing the USB key, since no USB key is present. .
7 ☐	**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 4.12Appendix I. `# /usr/TKLC/appworks/bin/set_ini_tz.pl "Etc/UTC" >/dev/null 2>&1`
8 ☐	**Reboot the Server**	Run the following command to reboot the server: `# init 6`

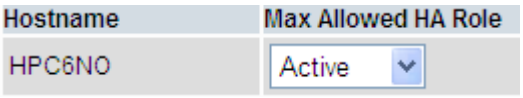
Procedure 18. Configure the Second NOAMP Server

9 ☐	**(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 19. Complete Configuring the NOAMP Server Group

STEP #	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.** RMSNO_900060102 Server | SG Inclusion | Preferred HA Role RMSNOA | ☑ Include in SG | ☐ Preferred Spare RMSNOB | ☑ Include in SG | ☐ Preferred Spare Add a NOAMP VIP by click on **Add**. Fill in the `VIP Address` and press **Ok** as shown below VIP Address [Add] [ ] [Remove] [Ok] [Apply] [Cancel]

Procedure 19. Complete Configuring the NOAMP Server Group

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**)
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.

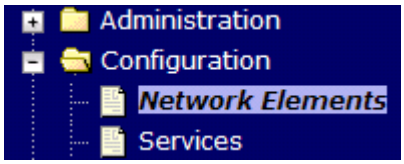
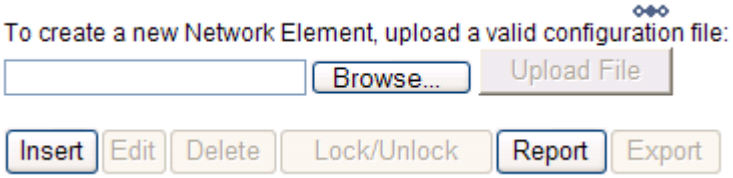
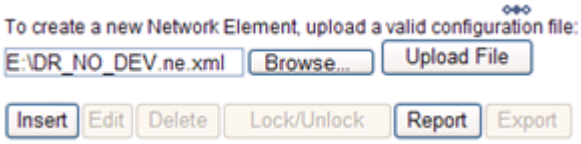
Procedure 20. Install NetBackup Client (Optional)

S T E P #	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.

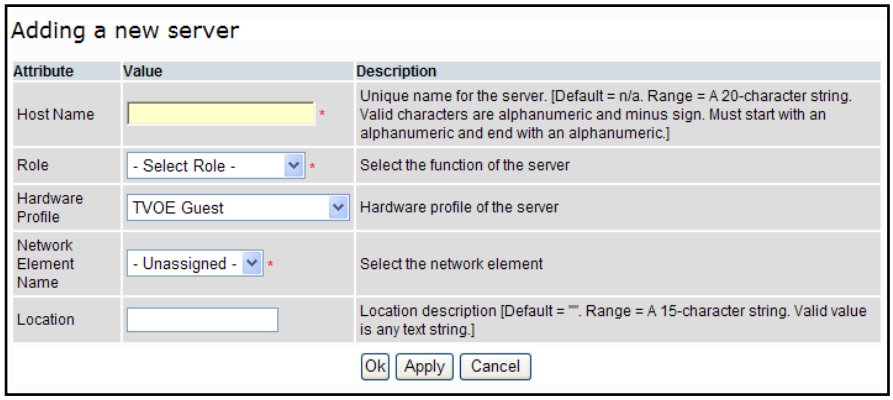
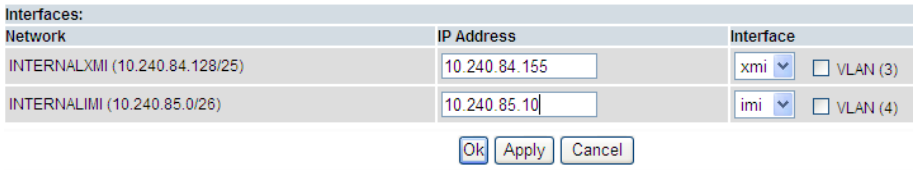
Procedure 21. NO Configuration for DR Site (Optional)

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. **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.

Procedure 21. NO Configuration for DR Site (Optional)

2 ☐	**Primary NOAMP VIP GUI:** Insert Network Element for DR Site	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 21. NO Configuration for DR Site (Optional)

3 ☐	**Primary NOAMP VIP GUI:** Insert Servers	Using the GUI menu, Navigate to **Configuration -> Servers** 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**. Next, add the following NTP servers (DSR 5.X and up): **NTP Server** | **Preferred?** ***<DR-RMS-TVOE-IP-Address>*** | Yes Select the "Ok" button when you have completed entering the server data.

Procedure 21. NO Configuration for DR Site (Optional)

4 ☐	**Primary NOAMP VIP GUI:** Export the Initial Configuration	Navigate to **`Main Menu -> Configuration -> Servers`** 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.
5 ☐	**Copy Configuration File to 1st DR NO Server**	SSH to the NOAMP VIP and use the `awpushcfg` utility to copy the configuration file created in the previous step from the `/var/TKLC/db/filemgmt` 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 `TKLCConfigData.<`***`hostname`***`>.sh`. `# awpushcfg` 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,

Procedure 21. NO Configuration for DR Site (Optional)

6 ☐	**DR NO Server A:** Verify awpushcfg was successful	1. Access the machine hosting the **DR NO Server A** using the **iLO** Connection and log in as root.
		2. 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`
		3. Verify awpushcfg was called by checking the following file
		`# cat /var/TKLC/appw/logs/Process/install.log`

7 ☐	**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. .
8 ☐	**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 4.12Appendix I. `# /usr/TKLC/appworks/bin/set_ini_tz.pl "Etc/UTC" >/dev/null 2>&1`
9 ☐	**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 21. NO Configuration for DR Site (Optional)

10 ☐	**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>`

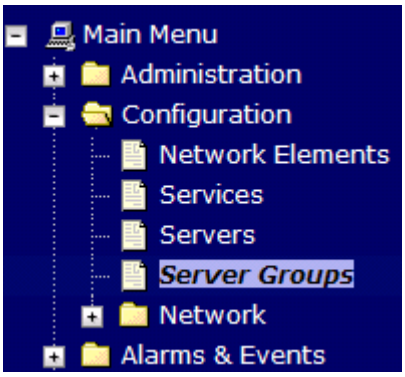
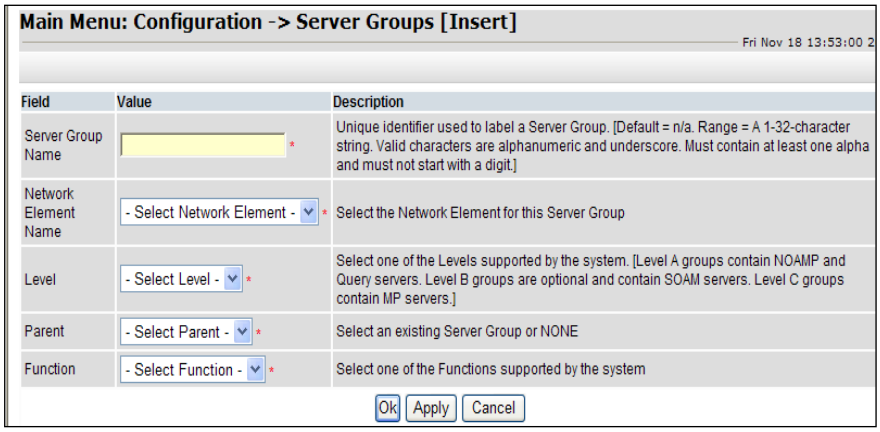
11 ☐	**DR NO Server A VM:** Verify Server Health	Execute the following command and make sure that no errors are returned:
		`# syscheck`
		`Running modules in class hardware... OK`
		`Running modules in class disk... OK`
		`Running modules in class net... OK`
		`Running modules in class system... OK`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

12 ☐	**Repeat for DR NO Server B**	Repeat Steps 3 through 11 to configure DR NO Server B.

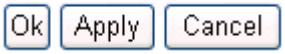
Procedure 22. NO Pairing for DSR NO DR Site (Optional)

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. **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.

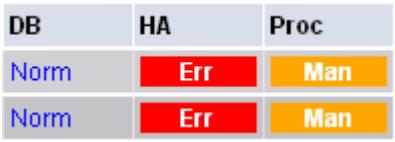
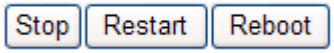
Procedure 22. NO Pairing for DSR NO DR Site (Optional)

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 22. 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 22. 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 11 and 12, but this time selecting DR NO Server B instead of A

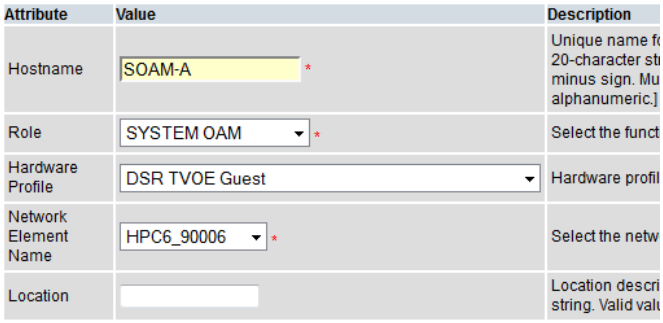
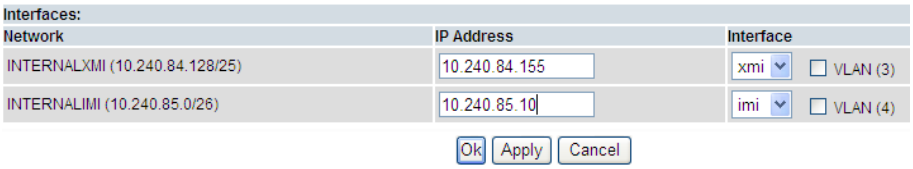
Procedure 23. Configure the SOAM NE

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 29, but defines the SOAM "Network Element". 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 24. 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 PMAC and the SOAM server**	Use the PMAC GUI to determine the Control Network IP address of the server that is to be the SOAM server. From the PMAC GUI, navigate to **Main Menu → Software→Software Inventory**. Note the IP address for the SOAM server. From a terminal window connection on the 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 ☐	**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".

Procedure 24. Configure the SOAM Servers

3 ☐	**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**. Next, add the following NTP servers (DSR 5.X and up): **NTP Server** | **Preferred?** *<RMS1-TVOE-IP-Address>* | Yes Select the "Ok" button when you have completed entering the server data.
4 ☐	**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.

Procedure 24. Configure the SOAM Servers

5 ☐	**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 Control Network IP address of the PMAC server, - the blade inventory will be presented, - 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.
6 ☐	**Wait for Configuration to Complete**	Obtain a terminal window connection on the 2nd NOAMP (Use the procedure in Appendix 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` **NOTE**: Ignore the warning about removing the USB key, since no USB key is present. .
7 ☐	**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 4.12Appendix I. `# /usr/TKLC/appworks/bin/set_ini_tz.pl "Etc/UTC" >/dev/null 2>&1` .
8 ☐	**Reboot the Server**	Run the following command to reboot the server: `# init 6`

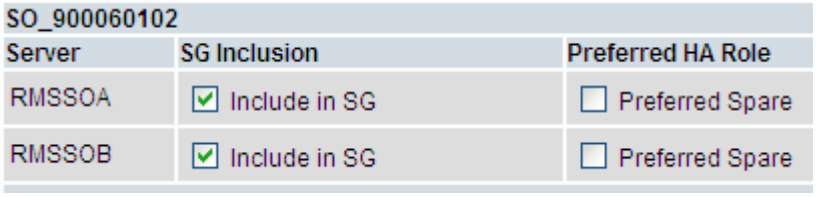
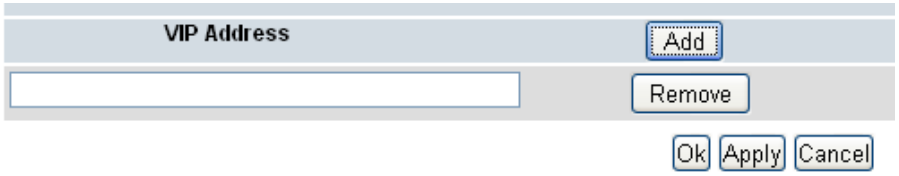
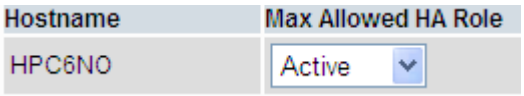
Procedure 24. Configure the SOAM Servers

9 ☐	**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, transfer the TKLCConfigData file to the "B" server, and reboot the "B" server when prompted at a terminal window. Add the following NTP servers (DSR 5.X and up): **NTP Server** / **Preferred?** ***<RMS2-TVOE-IP-Address>*** / Yes

Procedure 25. 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 25. 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".  Select the SOAM Server group and click on **Edit** Add both SOAM servers to the Server Group by clicking the "Include in SG" checkbox Click **Apply.** Add a SOAM VIP by click on **Add**. Fill in the `VIP Address` and press **Ok** as shown below 
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 SOAM server**	In the **Main menu->Status & Manage->HA** menu, verify that the "Max Allowed HA Role" for the 2nd SOAM 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**.
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.
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 26. Configure RMS-specific B-level Resources

S T E P #	This procedure will provide the steps to Configure RMS-specific B-level Resources 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 ☐	**SSH to the active SO**	Obtain a terminal window connection on the **active SO** server console via SSH or iLO. Execute the following on the command line. Wait until the script completes and you are returned to the command line: # **/usr/TKLC/dsr/bin/rmsResourceConfig.sh** Verify that no errors are displayed. If any errors are displayed, halt this procedure and contact Tekelec Support..

Procedure 27. Optimize NO and SO Databases

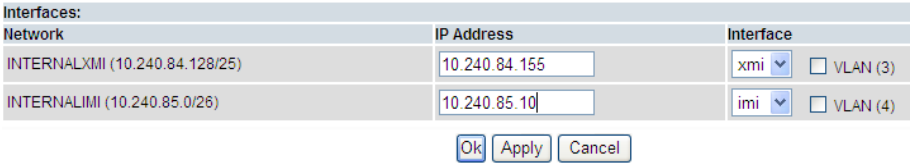
S T E P #	This procedure will provide the steps to optimize the NO and SO databases Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. IF THIS PROCEDURE FAILS, CONTACT TEKELEC TECHNICAL SERVICES AND ASK FOR ASSISTANCE.	

1
☐
	Log into all NO and SO servers and run the database optimization script	Obtain a terminal window connection on the **active NO** server console via SSH or iLO.
		
		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..
		
		Note that in case you are logged into the GUI, this scrip will cause you to be logged out.
		
		Repeat this step for the **standby NO, active SO, and standby SO, and D.R. NO (if applicable) servers.**

Procedure 28. Configure the MP 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 PMAC and the MP server**	Use the PMAC GUI to determine the Control Network IP address of the blade server that is to be an MP server. From the PMAC GUI, navigate to **Main Menu → Software-→Software Inventory**. Note the IP address for an MP server. From a terminal window connection on the 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 28. Configure the MP 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 in the fields as follows: **Hostname:** **<Hostname>** **Role:** **MP** **Hardware Profile:** **DSR TVOE Guest** **Network Element Name:** **[Choose The SO Network Element from the 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**. Next, add the following NTP servers (DSR 5.X and up): **NTP Server** | **Preferred?** ***<MP's-RMS-TVOE-IP-Address>*** | Yes Select the "Ok" button when you have completed entering the server data.
4 ☐	**Export the initial configuration**	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.
5 ☐	**Log onto the MP iLO**	Obtain a terminal window connection on the MP server iLO from the OA.

Procedure 28. Configure the MP Servers

6 ☐	**Copy Configuration File to MP 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 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 `TKLCConfigData.<hostname>.sh`. `# awpushcfg` The awpushcfg utility is interactive, so the user will be - prompted for the IP address of the PMAC server, - 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.
7 ☐	**Wait for Configuration to Complete**	Obtain a terminal window connection on the 2nd NOAMP (Use the procedure in Appendix 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` **NOTE**: Ignore the warning about removing the USB key, since no USB key is present. .
8 ☐	**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 4.12Appendix I. `# /usr/TKLC/appworks/bin/set_ini_tz.pl "Etc/UTC" >/dev/null 2>&1`
9 ☐	**Reboot the Server**	Run the following command to reboot the server: `# init 6`

Procedure 28. Configure the MP Servers

10 ☐	**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** 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 28. Configure the MP Servers

8 ☐	**(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 EXECUTED 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 28. Configure the MP Servers

9 ☐	**Repeat for remaining MPs**	Repeat this entire procedure for all remaining MP blades.

Procedure 29. Configure the MP Server Group(s) and Profiles

STEP #	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 Element Server Group]**

Function**: Select the Proper Function for this MP Server Group:**

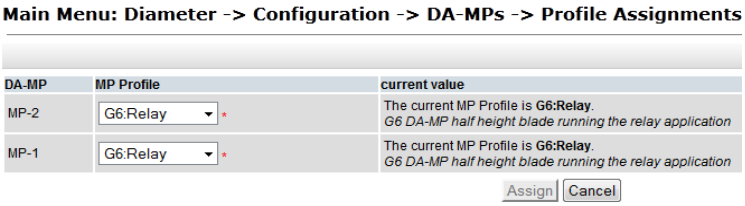
Server Group Function	MPs Will Run	Redundancy Model
DSR (multi-active cluster)	Diameter Relay and Application Services	Multiple MPs active
DSR (active-standby pair)	Diameter Relay and Application Services	1 Active MP and 1 Standby MP
Session Binding Repository	Session Binding Repository Function	1 Active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

Select **`OK`** when all fields are filled in.

Procedure 29. Configure the MP Server Group(s) and Profiles

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.
3 ☐	**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.**
3 ☐	**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
4 ☐	**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 29. Configure the MP Server Group(s) and Profiles

5 ☐	**Assign Profiles to MPs from SOAM GUI.**	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 function that the MP will serve: **Profile Name** / **Description** **VM:Relay** — Virtualized DA-MP on DL380 TVOE Guest running the relay application **VM:Database** — Virtualized DA-MP on DL380 TVOE Guest running relay and database applications **VM:Session** — Virtualized DA-MP on DL380 TVOE Guest running relay and session applications When finished, press the **Assign** button
6 ☐	**Update DpiOption table from the active SOAM**	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 ===**
7 ☐	**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.

4.11 Signaling Network Configuration

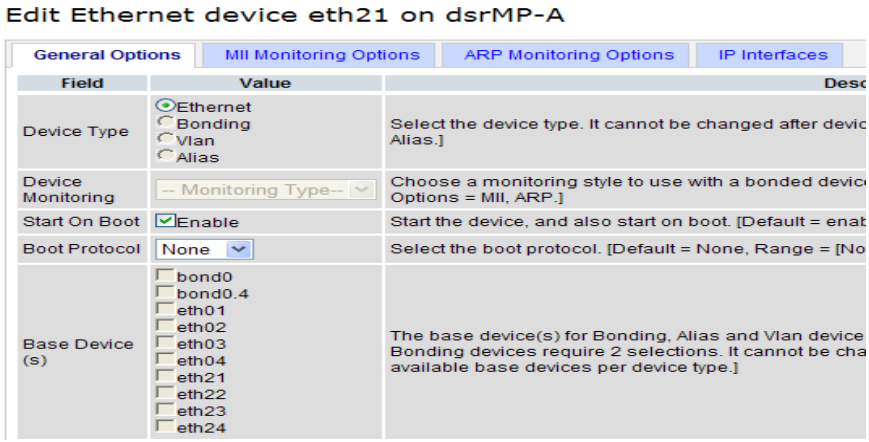
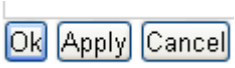
Procedure 30. Configure the Signaling Networks

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.

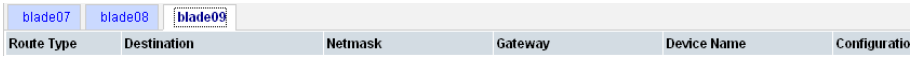
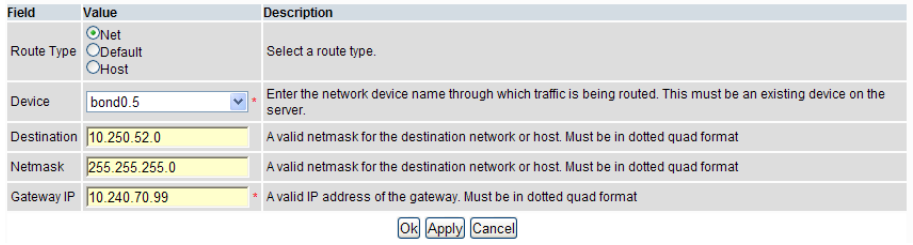
Procedure 31. Configure the Signaling Devices

S T E P	This procedure will provide the steps to configure the Signaling Devices. 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:** Make Signaling Devices Configurable (5.0 only)	Login as root to the NOAMP VIP console. Execute the following commands: **# AppWorks NetworkDevice importDevice xsi1 <MP1_HOSTNAME>** **# AppWorks NetworkDevice importDevice xsi2 <MP1_HOSTNAME>** **# AppWorks NetworkDevice importDevice xsi1 <MP2_HOSTNAME>** **# AppWorks NetworkDevice importDevice xsi2 <MP2_HOSTNAME>** If your installation has xsi3 and xsi4 signaling networks, then execute the above commands again, but substitute "xsi3" and "xsi4" for "xsi1" and "xsi2", respectively.
2 ☐	**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. Select the first signaling interface (xsi1) and click on **Edit**

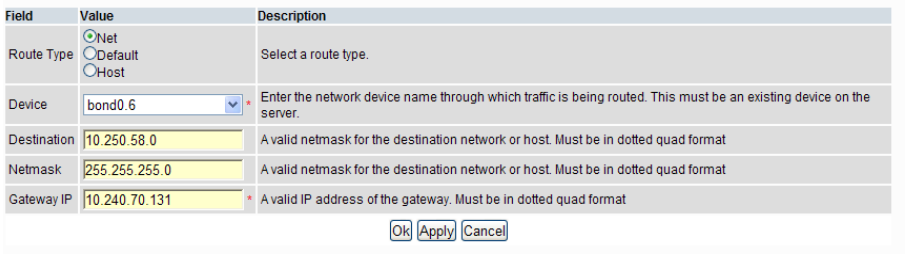
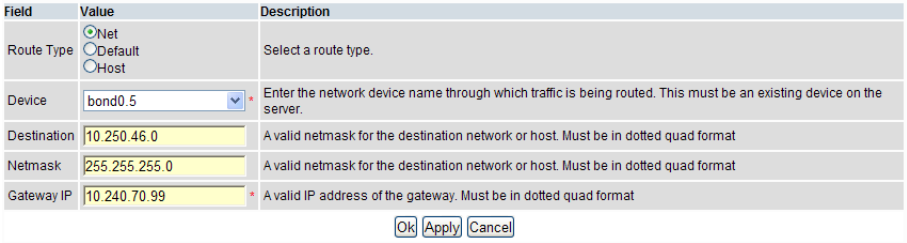
Procedure 31. Configure the Signaling Devices

3 ☐	**NOAMP VIP:** Configure the Signaling Interfaces of the MP	The following screen should be displayed. Verify that the blade name on the top corresponds to the MP.  For `Device Type`, verify that it is set to `Ethernet`. For `Start on Boot`, verify that the checkbox is selected. For `Boot Protocol`, verify that it is set to None 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 IPv6 only and your site has IPv6 auto-configuration, there's no need to enter an IP address, it will be assigned automatically, If configuring an IPv4 or IPv4/IPv6, enter the IP address that corresponds to the IPv4 interface. Click on **`Ok`** at the bottom of the screen.  To configure additional Signaling Interfaces, re-select the MP and click on Edit again and repeat this step, otherwise continue with the next step.
4 ☐	**NOAMP VIP:** Configure the Interfaces of the other MPs.	Repeat this procedure to configure the signaling devices of all other MPs.

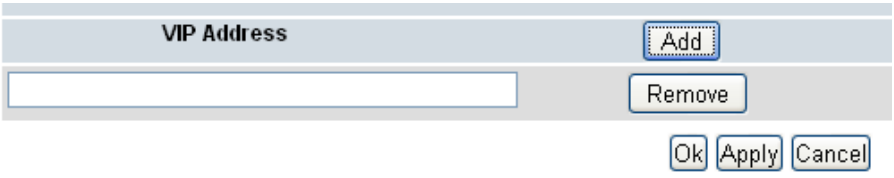
Procedure 32. Configure the Signaling Network Routes

S T E P		
	This procedure will provide the steps to configure the Signaling Network Routes. It is only applicable in a Layer 3 Configuration. **Note: If the default XMI route was deleted earlier (Procedure 28, step 8). It is recommended that a default Signaling route is added.** 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 `XSI1` For `Destination` enter the Network ID of Ext-XSI1 For `Netmask` enter the corresponding Netmask. For `Gateway IP` enter the Int-XSI1 switch VIP. Press **Ok.**

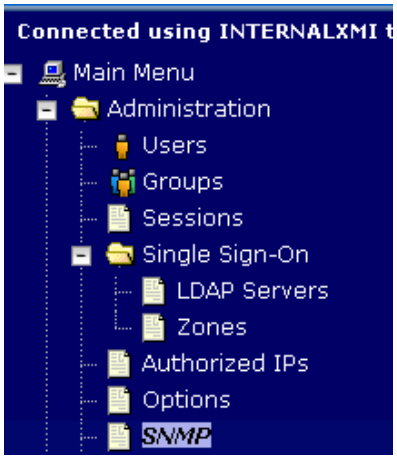
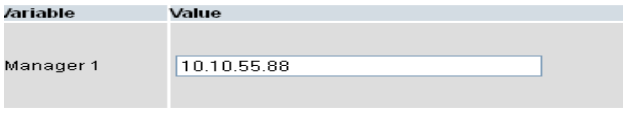
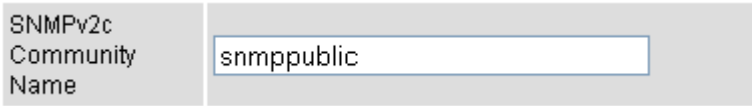
Procedure 32. Configure the Signaling Network Routes

5 ☐	**NOAMP VIP:** Add Route for XSI-2	Click on **Insert** again  For `Route Type` Select `Net`, for `Device` select XSI2 For `Destination` enter the Network ID of 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 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.

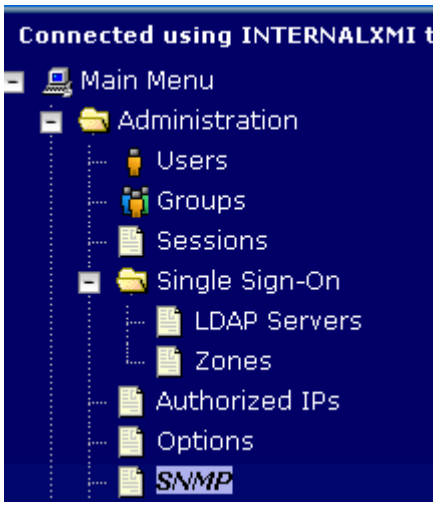
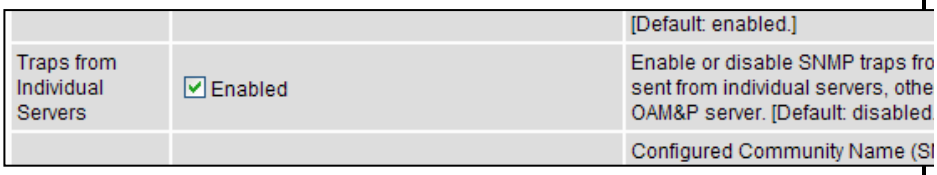
Procedure 33. Add VIP for Signaling Networks (Active/Standby Configurations ONLY)

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 34. 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 34. 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.

4.12 Install Optional Features

Procedure 35. Install 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 Install Guides for Optional Features to Complete Installation**	Refer to 3.3 **Optional Features** for a list of feature install documents whose procedures are to be executed at this moment.

Procedure 36. 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
2 ☐	**Configure FABR**	Refer to [6] for the steps required to configure FABR

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.

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>
```

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

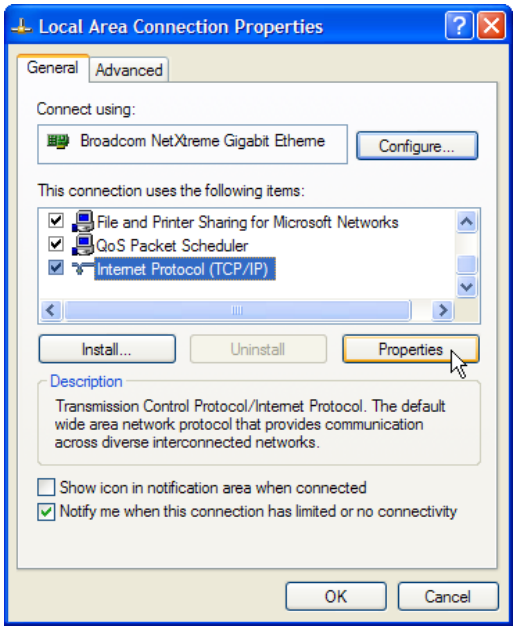
This procedure contains the steps to connect a laptop to the TVOEiLO via a directly cabled Ethernet connection. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

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.

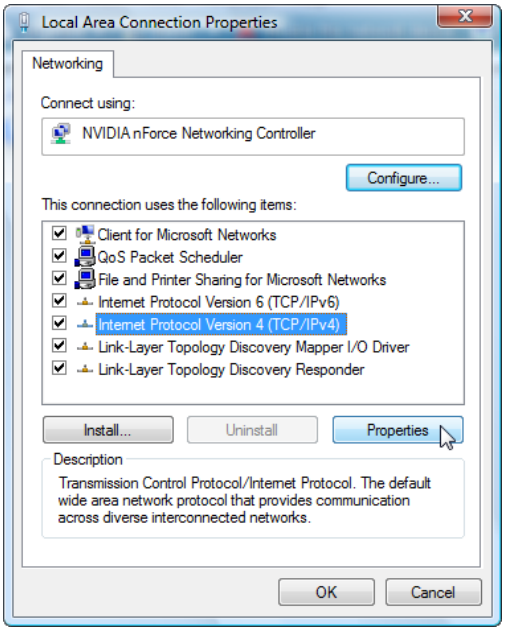
NOTE: For this step follow the instruction specific to the laptop's OS (XP or Vista).</td><th>Windows XP</th><th>Windows Vista</th></tr>
<tr>
<td>

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"



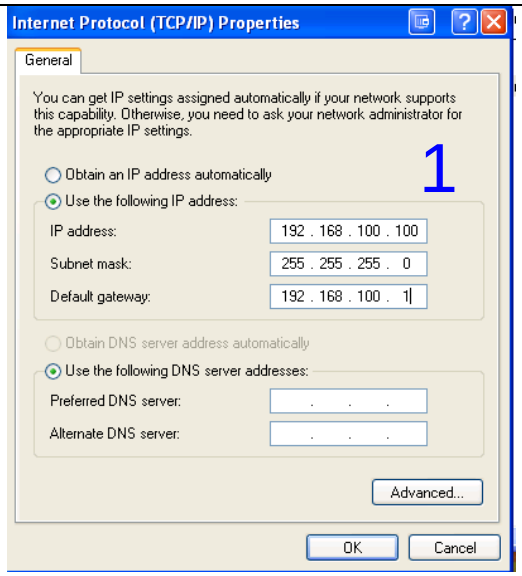
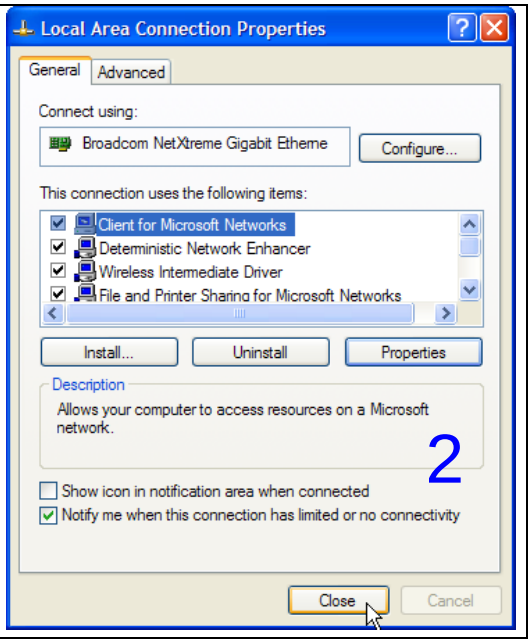
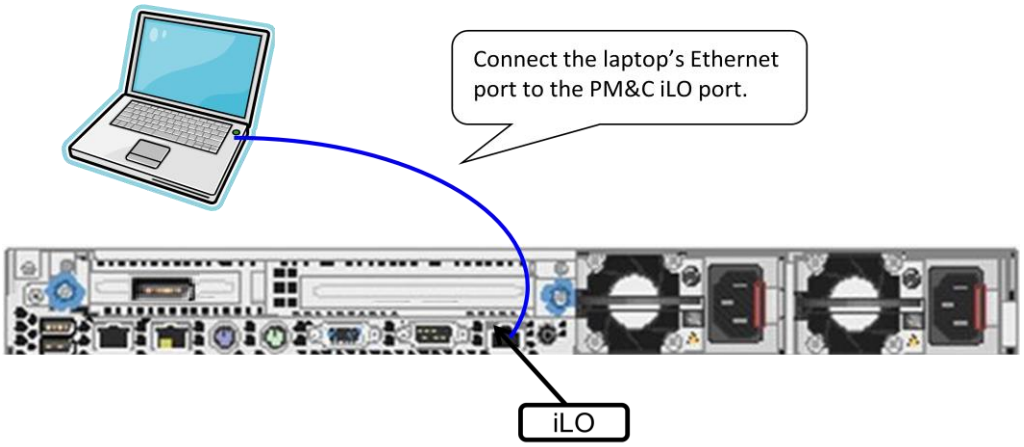
</td>
<td>

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>

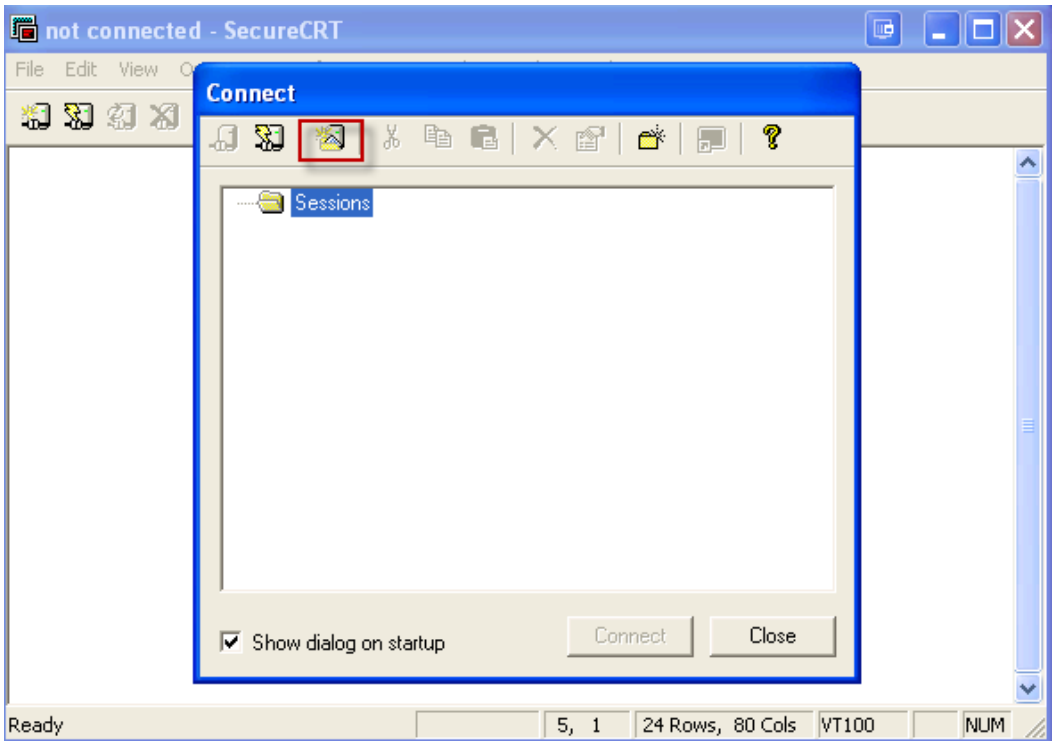
Procedure B.1 Connecting to the EAGLE XG TVOE iLO

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		

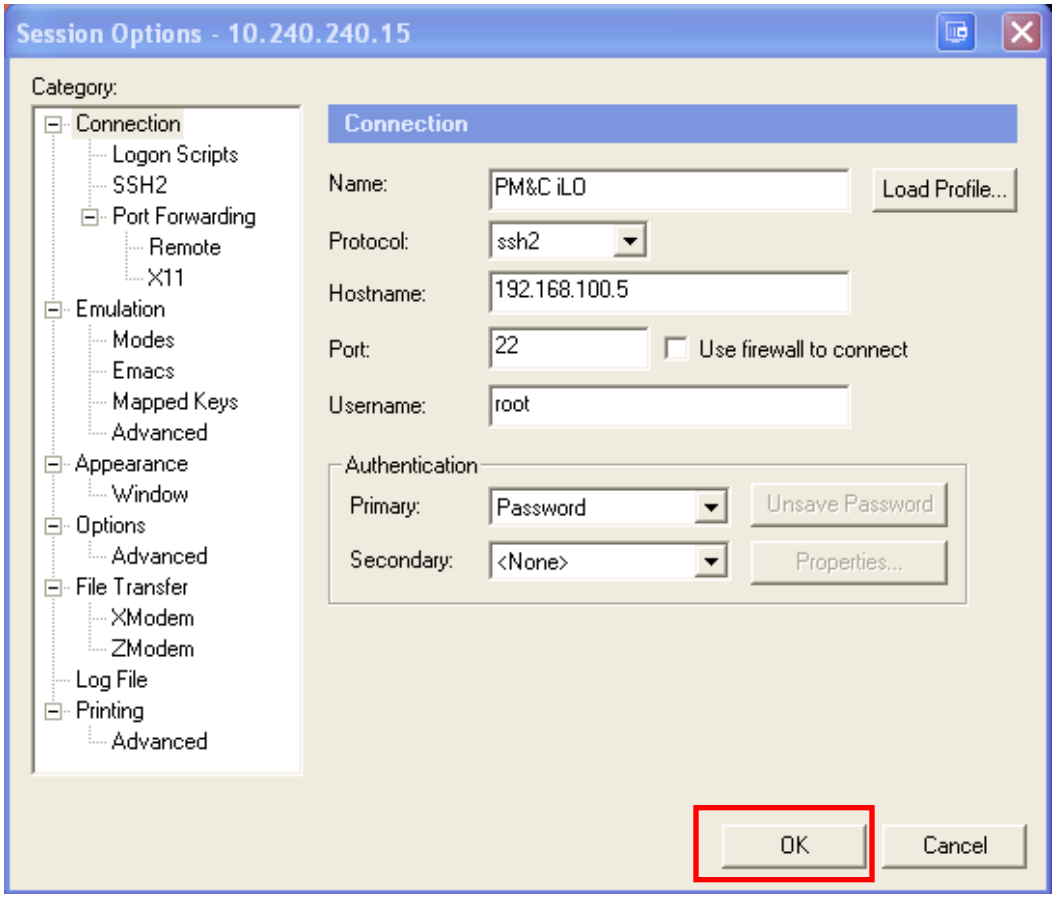
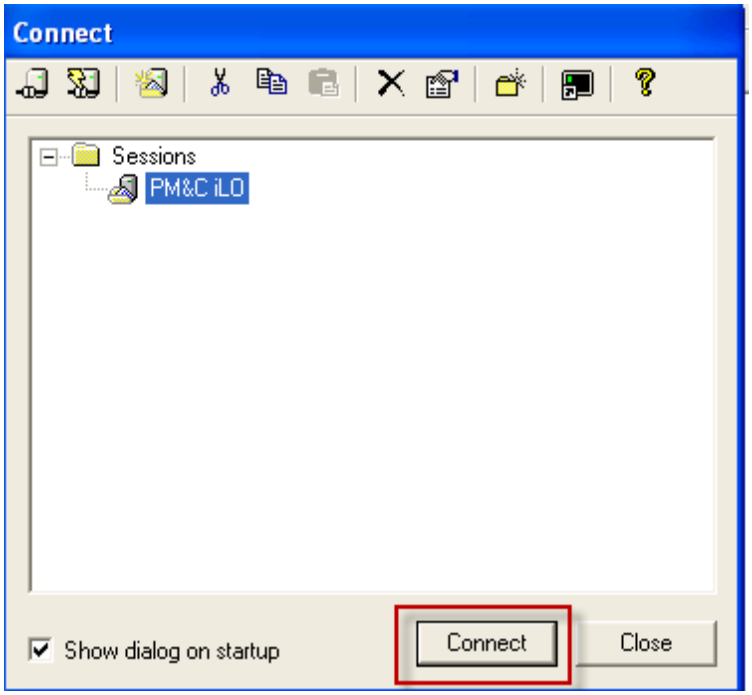
APPENDIX C. TVOE ILO ACCESS

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.

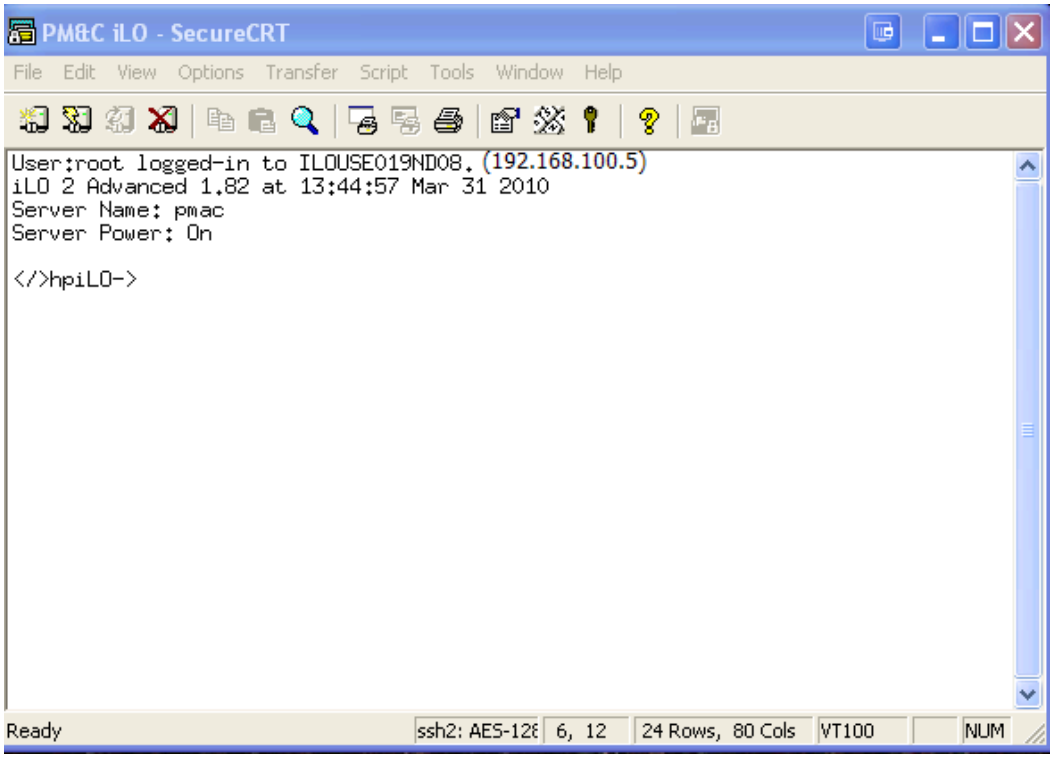
Procedure C.1 Accessing the TVOE iLO

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.**	

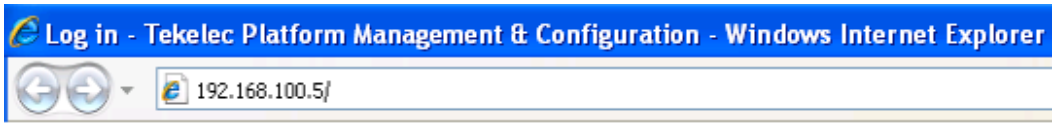
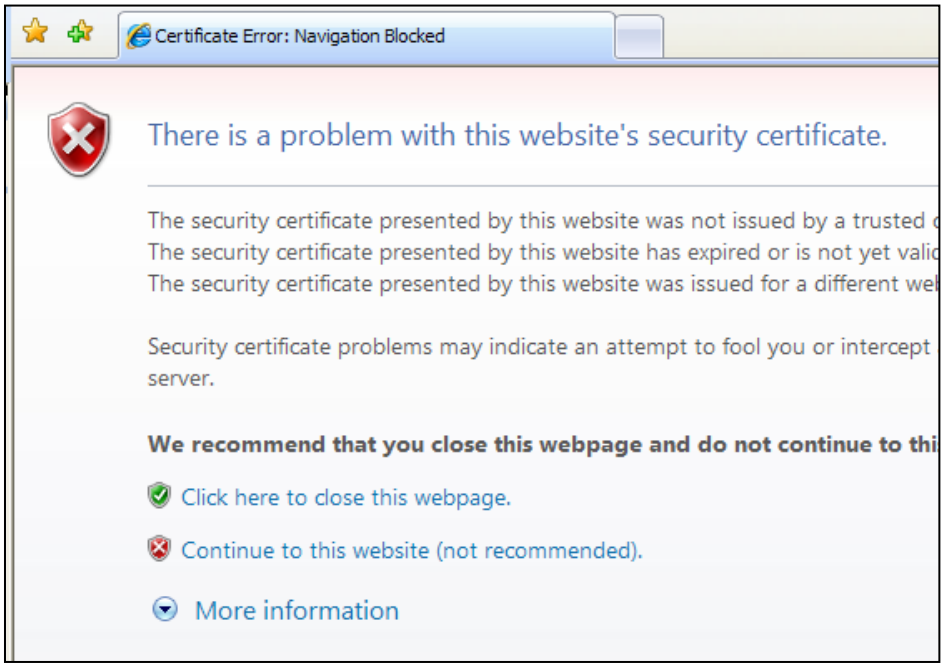
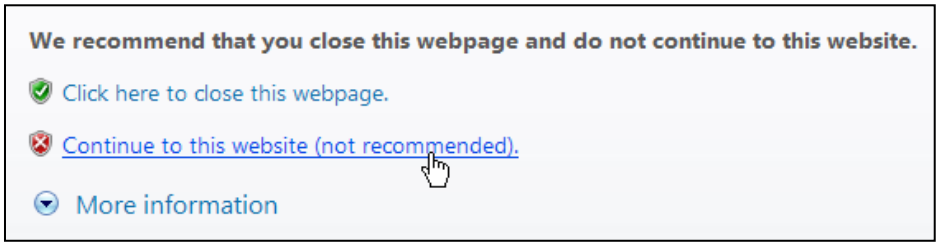
Procedure C.1 Accessing the TVOE iLO

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

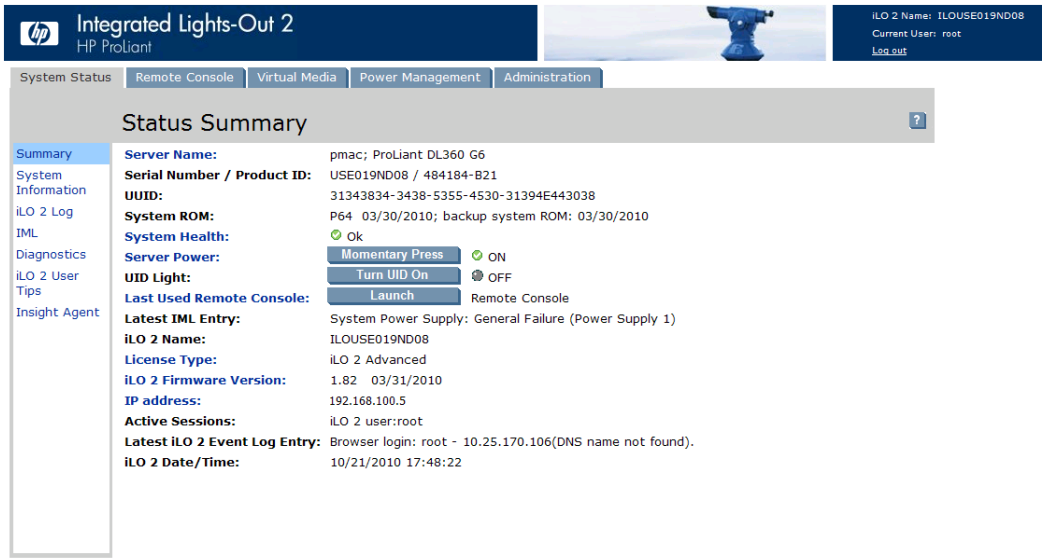
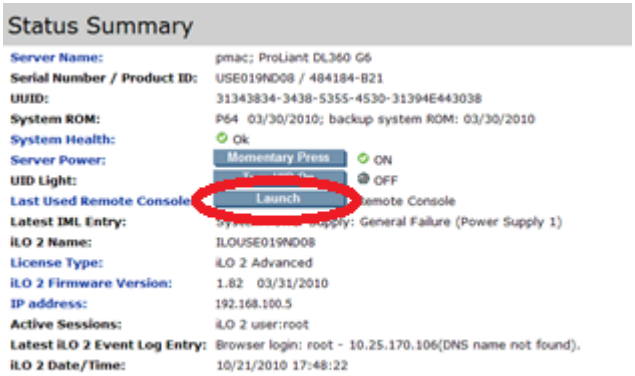
APPENDIX D. TVOE ILO GUI ACCESS

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)"	

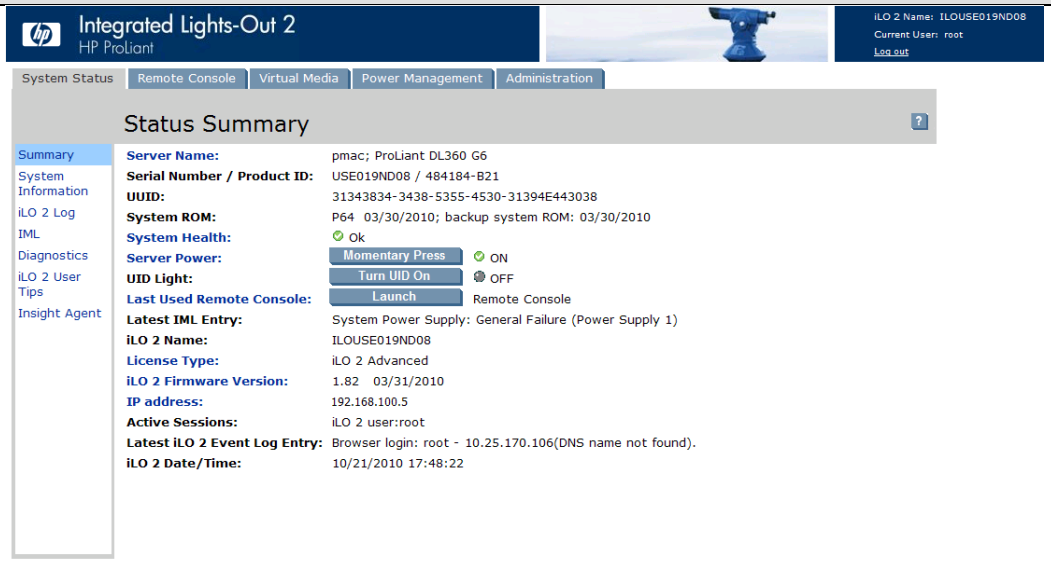
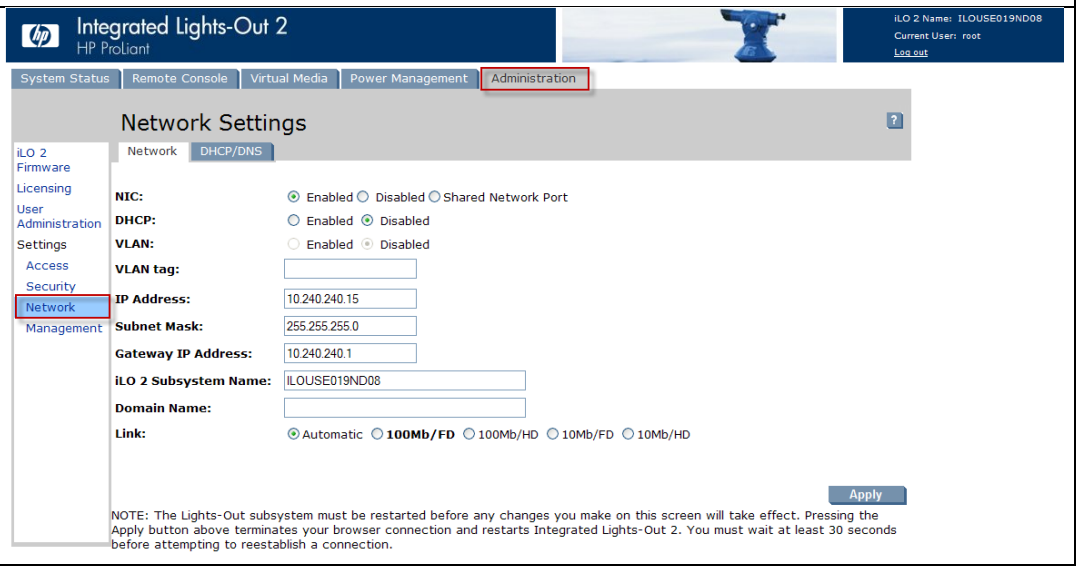
Procedure D.1 Accessing the TVOE iLO GUI

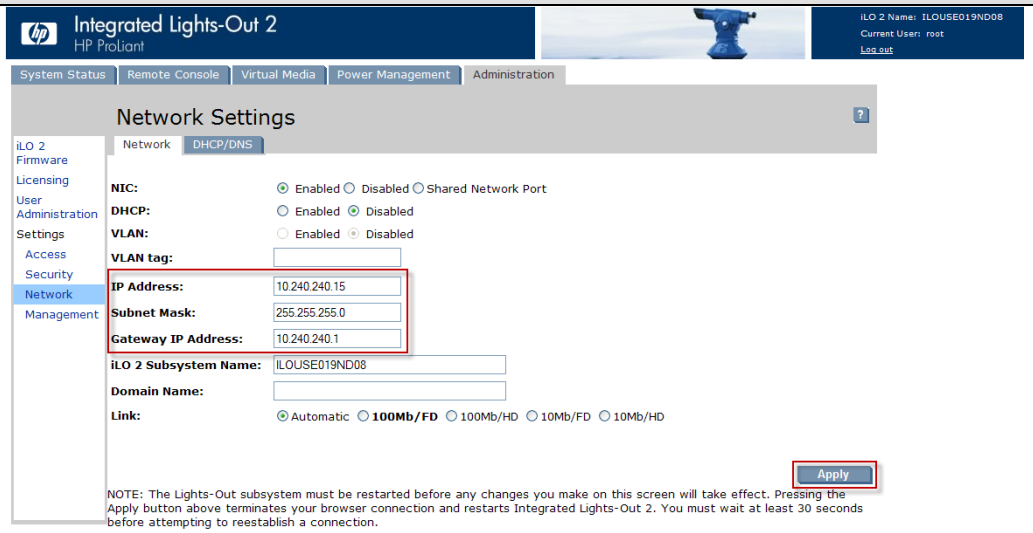
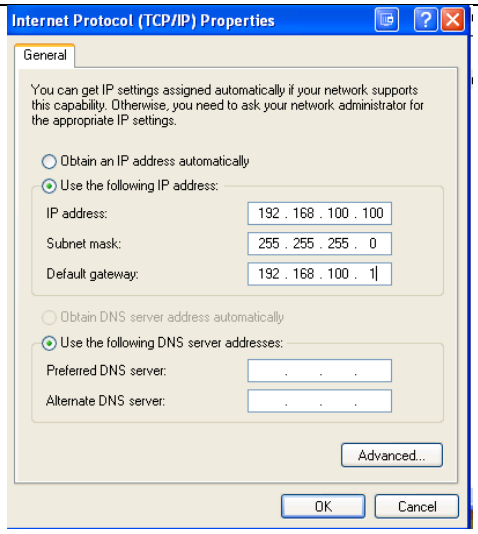
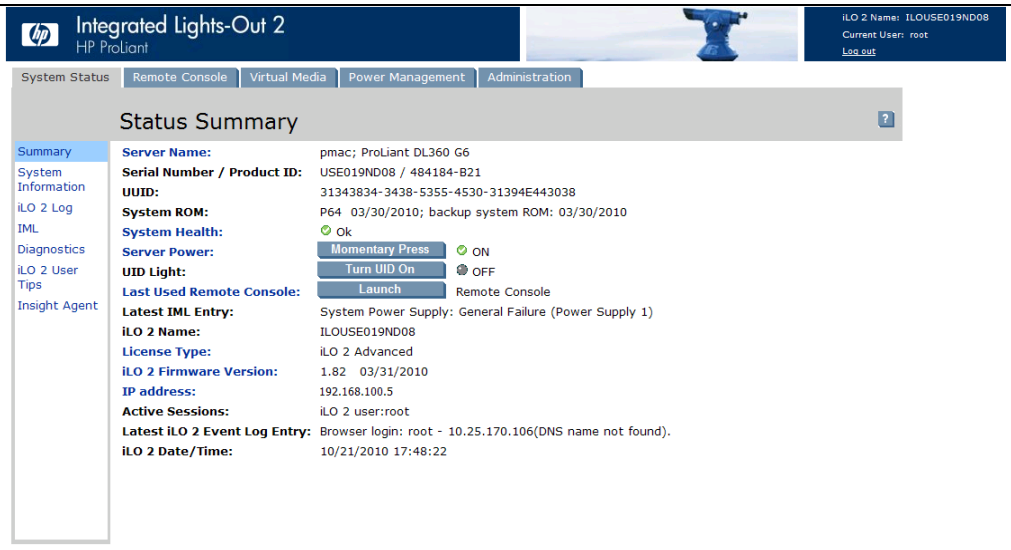
4. ☐	Log in as user "**root**".	
5. ☐	The TVOE iLO Home page is displayed.	
6. ☐	Click on Launch to start the pmac iLO CLI	
THIS PROCEDURE HAS BEEN COMPLETED		

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

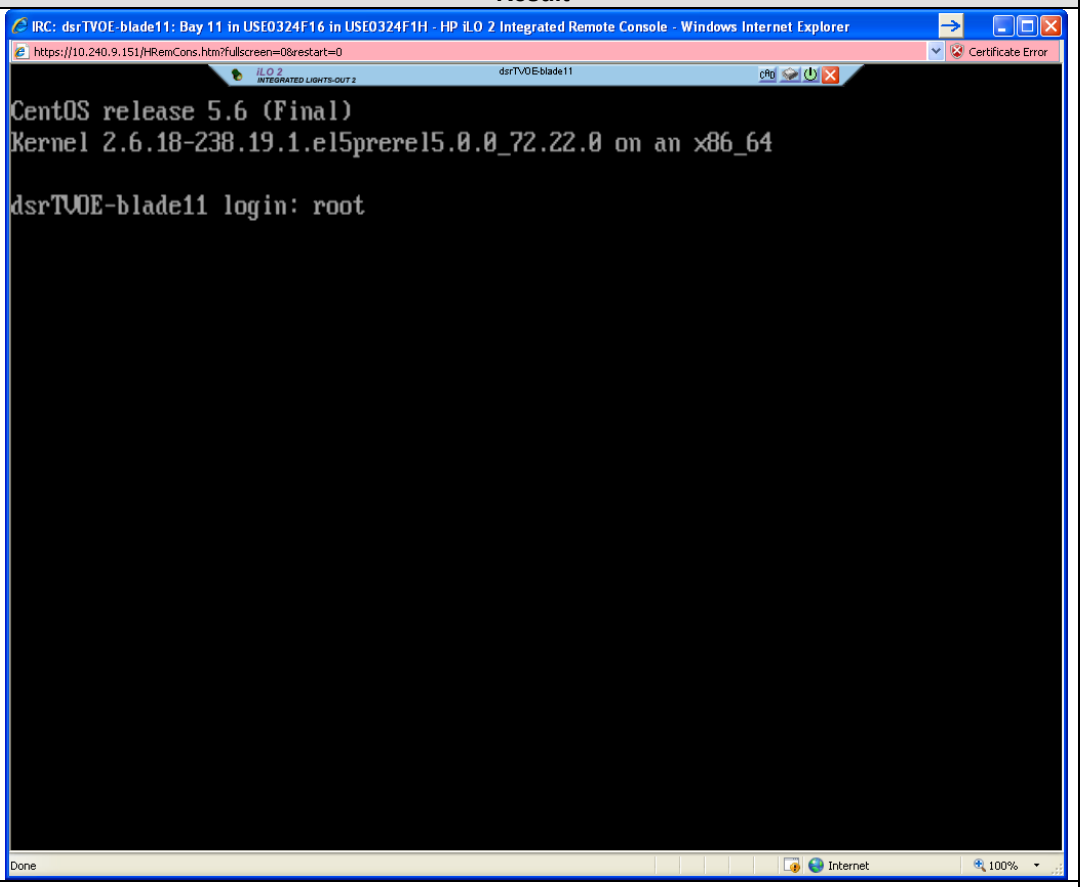
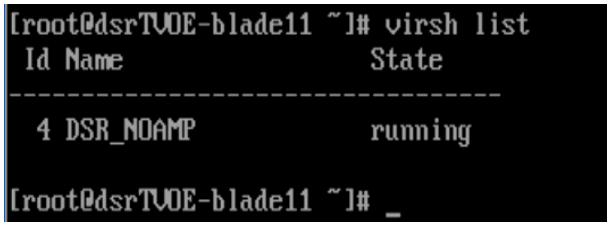
Step	Instruction	Result
1. ☐	Connect to the TVOE iLO GUI using the instructions in **Appendix D**	
2. ☐	Click the "**Administration**" tab. Under "**Settings**" in the left column click on "**Network**".	

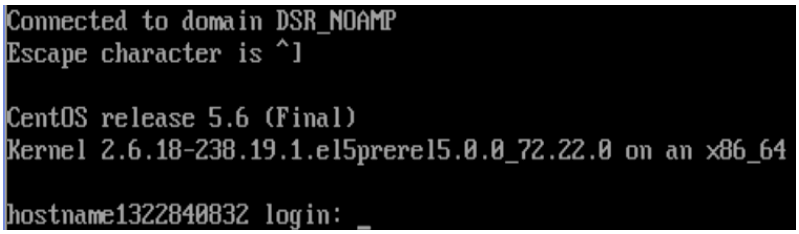
Step	Instruction	Result
3. ☐	Change the **IP Address**, **Subnet Mask** and **Gateway IP Address** to the values supplied in the IP Site Survey for the TVOE iLO. Hit **Apply**. NOTE: You will lose access after you hit the Apply button.	
4. ☐	Using the instructions found in **Appendix B, reset** the PC's 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/MP/IPFE CONSOLE ACCESS

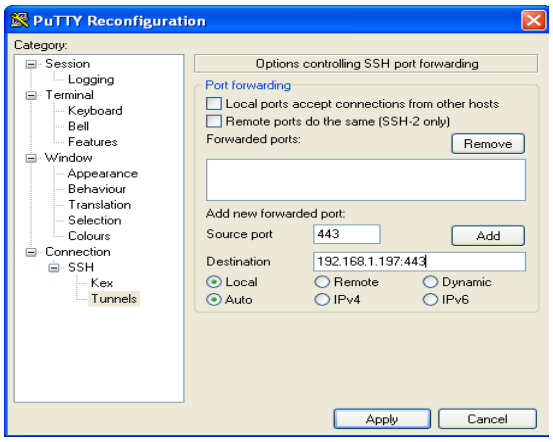
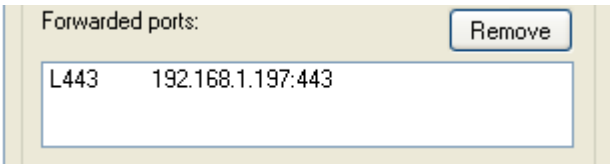
This procedure describes how to log into the PM&C/NOAMP/SOAMP/MP/IPFE console from the TVOE Host.

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 Management 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 blade 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 blade. **NOTE:** This procedure assumes that you have obtained the control network IP address for the first NOAMP server. That variable will be refered to as *NOAMP-Control-IP* in thiese instructions.	
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. **This procedure is now complete**

APPENDIX H. MANUAL TIMEZONE SETTING PROCEDURE

Procedure H.1 Timezome Setting

STEP		
	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 I 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.**
4 ☐	**Reboot the Server**	`# init 6`

APPENDIX I. 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 J. 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 4.1 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)

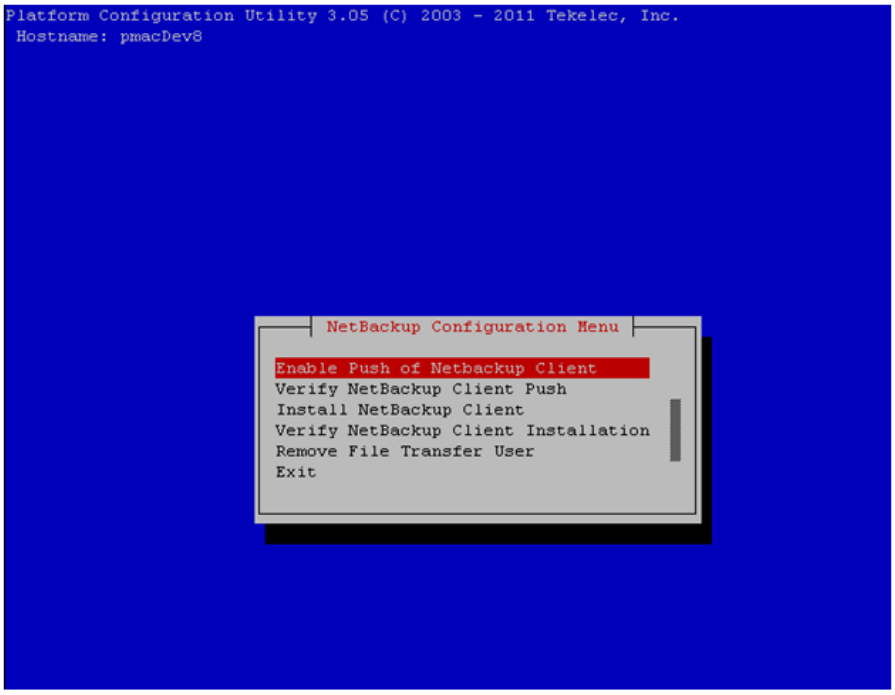
Prerequisites:
• Application server platform installation has been completed.
• Site survey has been performed to determine the network requirements for the application server, and interfaces have been configured.
• NetBackup server is available to copy, sftp, the appropriate NetBackup Client software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

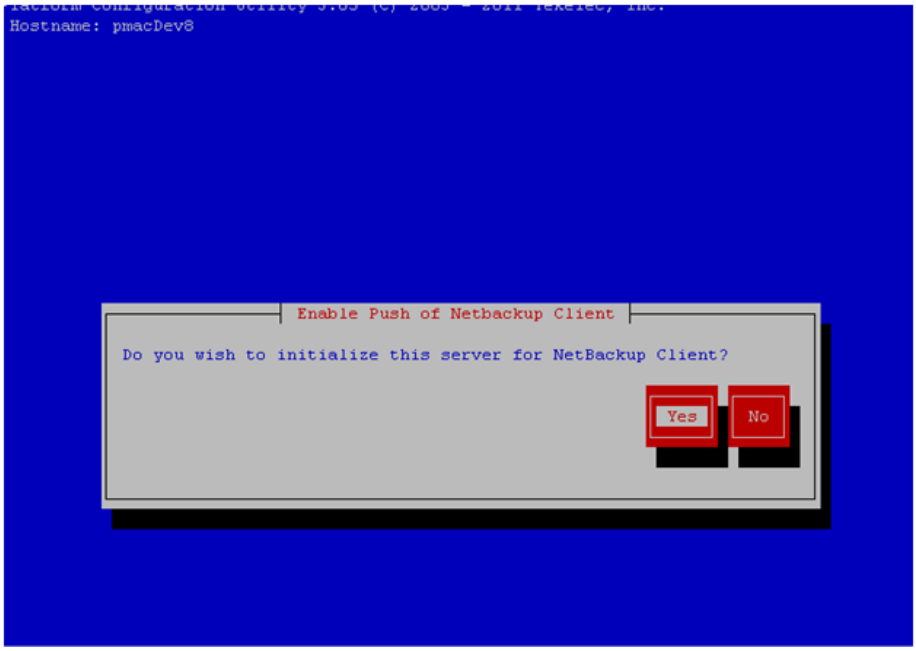
```
# su - platcfg
```

- Navigate to **NetBackup Configuration**



3. Application server iLO: Enable Push of NetBackup Client

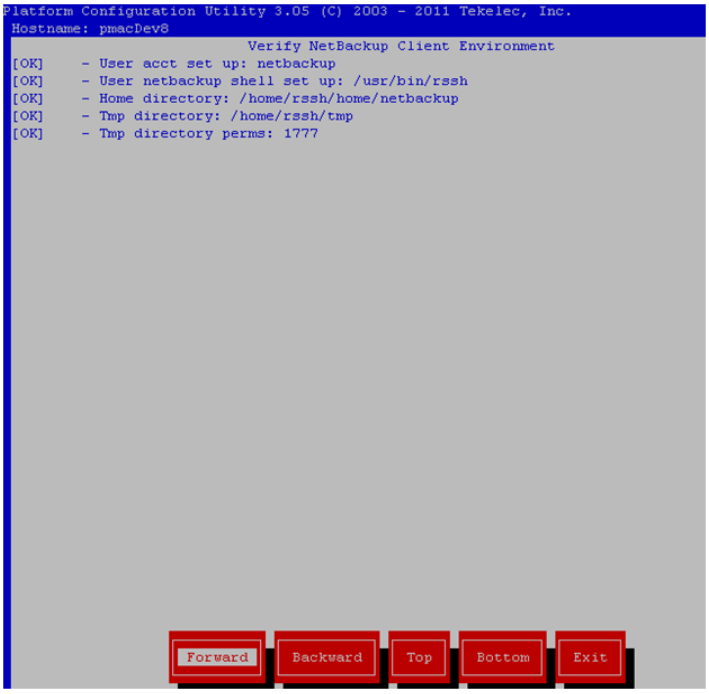
- Navigate to **NetBackup Configuration ➢ Enable Push of NetBackup Client**



- 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)

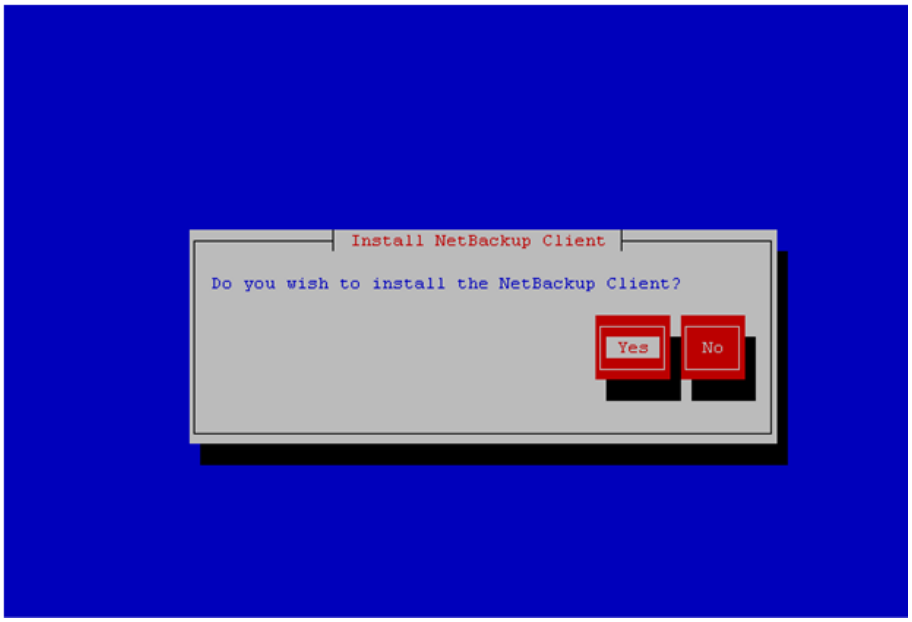
  ```
  # cd /usr/openv/netbackup/client/Linux/7.5
  ```

- 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

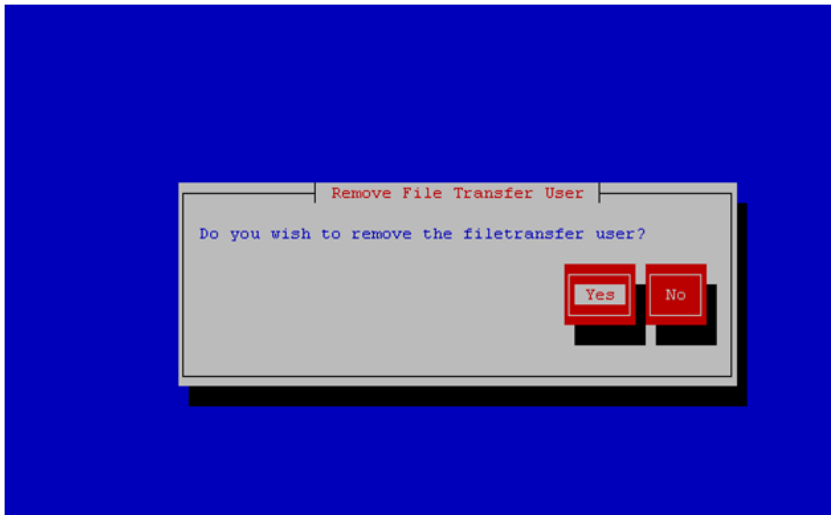
7. Application server iLO: Verify NetBackup CLient software installation on the application server.

- 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.

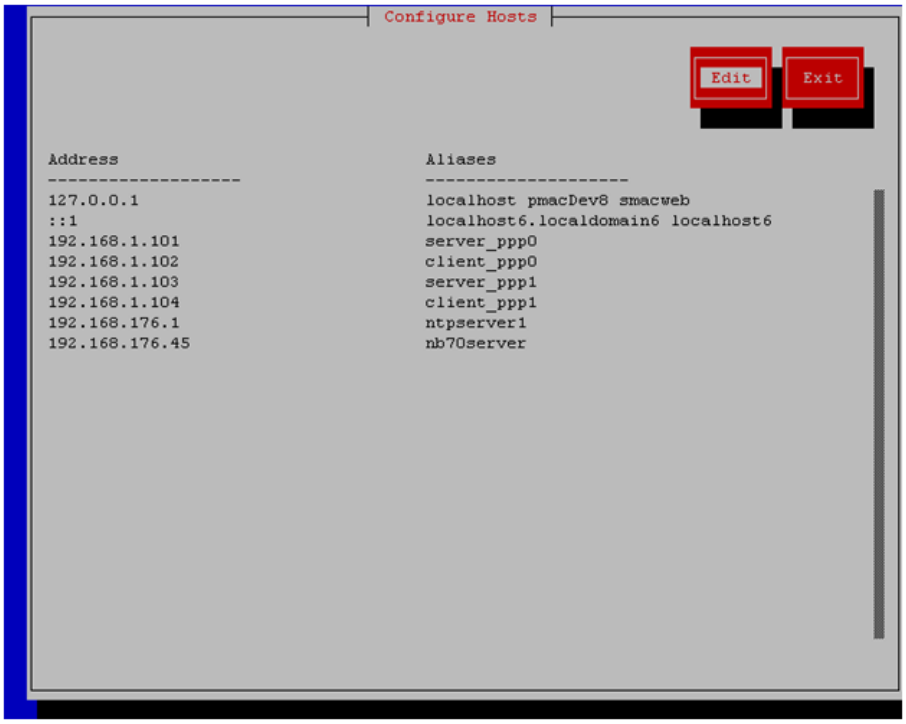
- List NetBackup servers hostname:

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

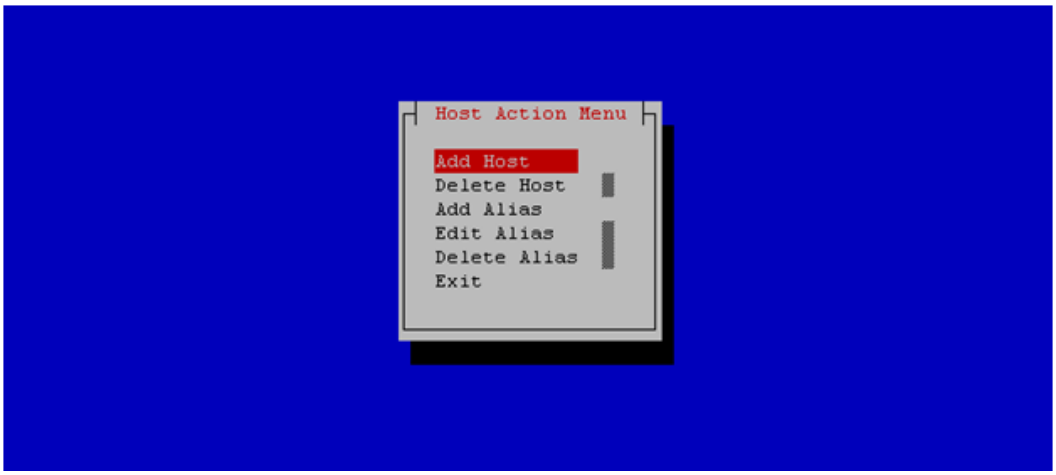
- Use platform configuration utility (platcfg) to update application hosts file with NetBackup Server alias.

```
# su - platcfg
```

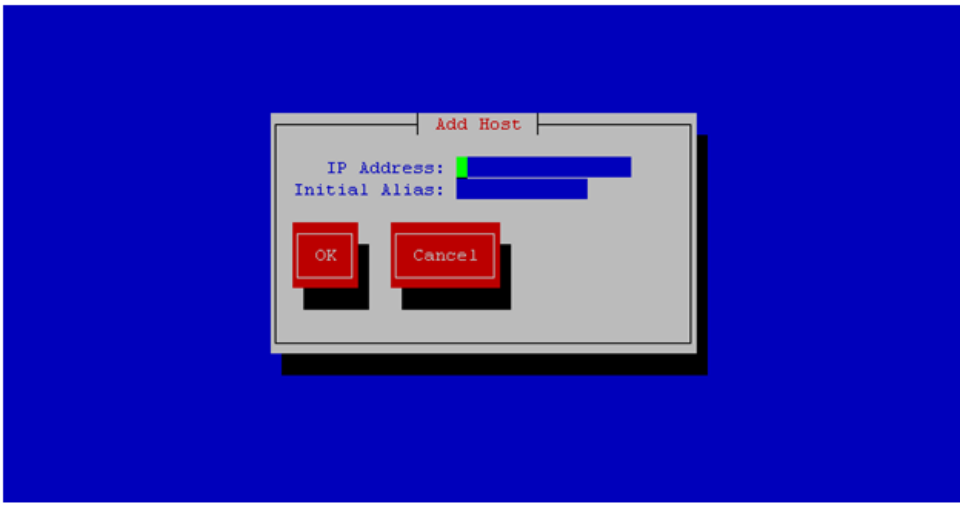
- Navigate to **Network Configuration ➢ Modify Hosts File**



- 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 K. 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 L. CREATING A BOOTABLE USB DRIVE

Procedure L.1 Creating a Bootable USB Drive on Windows

S T E P	**NOTE**: This procedure will create a Bootable USB drive from a .usb file	
1 ☐	**Insert USB Media**	Insert the USB Media into the USB Port
2 ☐	**Install Media Builder**	Download the Tekelec media builder tool from the Tekelec shared drive (m:\mbuilder) and follow the instructions on how to install it
3 ☐	**Copy the .USB file to your local machine**	Using sftp, copy the .usb image file to your local machine
4 ☐	**Use Media Builder to Create bootable USB**	Use the Media builder Tool to create a bootable USB drive from the .usb image file copied in step 3

Procedure L.2 Creating a Bootable USB Drive on Linux

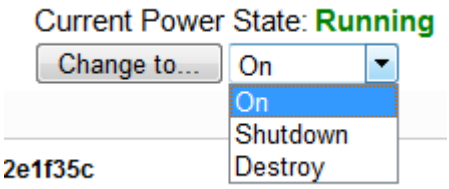
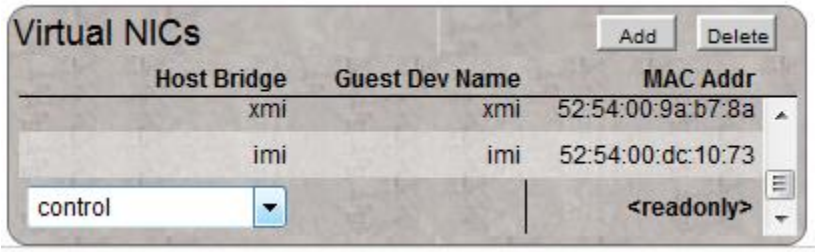
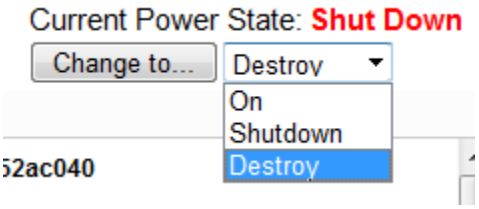
S T E P		
	NOTE: This procedure will create a Bootable USB drive from a .usb file on a Linux Machine	
1 ☐	**Insert USB Media**	Insert the USB Media into the USB Port. It should automatically be mounted under /media Obtain the path of the USB drive by running: `# ls /media` The output should be similar to the following: sdb1 Note down the path without the partition number (in this case, it would be /dev/sdb)
2 ☐	**Linux Machine**	Obtain theTVOE 2.0 **.usb** file and copy it onto the local linux machine (e.g. under /tmp)
3 ☐	**Copy the .USB file onto the USB drive**	Use the dd command to copy the .usb file onto the USB drive Note: Make sure you **do not** use the partition number when copying the file `# dd if=<path_to_usb_image> of=/dev/sdb oflag=direct`
4 ☐	**Remove USB drom Port**	Once the dd command is done, remove the USB drive from the USB port and delete the .usb file.

APPENDIX M. CONFIGURE ADDITIONAL SIGNALING INTERFACES ON AN MP

Procedure M.1 Configure Additional Signaling Interfaces on an MP

S T E P	This procedure will configure additional signaling interfaces on an MP **Prerequisite:** The DSR installation process is fully done **NOTE:** The additional signaling interfaces will be tagged onto the same device as the other signaling interfaces.	

1 ☐	**TVOE Host CLI:** Add the Signaling Interfaces	Log into the TVOE host via the iLO or ssh and configure an additional signaling (XSI) Network using option 1 **OR** option 2 below
		
		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.
		
		Option 1: Deployment with Aggregation switches:
		
		`# netAdm add --device=<TVOE_XSI3_Bridge_Interface> --onboot=yes`
		`Interface bond0.7 added`
		
		`# netAdm add --type=Bridge --name=xsi3 --onboot=yes --bridgeInterfaces=<TVOE_XSI3_Bridge_Interface>`
		`Interface bond0.7 was updated.`
		`Bridge xsi3 added!`
		
		Option 2: Deployment without Aggregation switches:
		
		`# netAdm add --device=<TVOE_XSI3_Bridge_Interface> --onboot=yes`
		`Interface bond2.<XSI3_VLAN_ID> added`
		
		`# netAdm add --type=Bridge --name=xsi3 --onboot=yes --bridgeInterfaces=<TVOE_XSI3_Bridge_Interface>`
		`Interface bond2.<XSI3_VLAN_ID> was updated.`
		`Bridge xsi3 added!`
		
		Repeat this step to add any additional signaling interfaces (e.g. xsi4).

2 ☐	**PM&C GUI:** Edit the MP Guest	1. Log into the pmac GUI by navigationg to **http://<pmac_management_ip>/** **2.** Navigate to **Main Menu -> VM Management** 3. Choose the TVOE host that is hosting the MP VM 4. Select the MP VM you wish to change 5. Change the power state of VM from **Running** to **Destroy** **(**Note: This will actually change the power state to "Shut Down")  6. Click on **Edit** 7. Under the "Virtual NICs", add the new signaling interfaces. If adding 2 interfaces, they would be as follows: (Note that all names are lowercase) • Host Bridge: **xsi3** Guest Dev: **xsi3** • Host Bridge: **xsi4** Guest Dev: **xsi4** 8. To add a new NIC, press the **Add** button, choose the proper host bridge from the drop-down box, then click over into the **Guest Dev Name** column and type in the name of guest interface. The following screenshot is just an example of the area you should be editing:  9. When you've finished adding the Virtual NICs, Click **Save** 10. Change the Power State of the VM from **Destroy** to **On**  11. Repeat for all other MP VMs you wish to edit.

3 ☐	**NO VIP GUI:** Configure newly added signaling interfaces	Execute the following procedures 1. Procedues 30 to add the new signaling network 2. Procedure 31 to configure the newly added signaling interfaces. 3. (OPTIONAL) Procedure 32 to add a default signaling route (only if the previously added interfaces have a default signaling route). 4. (OPTIONAL) Procedure 33 to add a VIP (only if the MPs are configured in Active/Standby Configuration).

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**.