Oracle® Communications Tekelec HLR Router

Installation Guide for HP Hardware

Release 4.1

E56461, Revision 2

June 2016

Oracle® Communications HLR Router 4.1 Initial Installation and Configuration Guide for HP Hardware

CAUTION: Before installing any system, please access My Oracle Support (MOS) and review any Technical Service Bulletins (TSBs) that relate to these procedures.

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

Refer to ***Appendix L*** - *Accessing My Oracle Support (MOS),* for more information on contacting Oracle Customer Care.

TABLE OF CONTENTS

List of Tables

List of Figures

1. INTRODUCTION

1.1 Purpose and Scope

This document describes how to install the Tekelec HLR Router 4.1 product on DL 360 (Gen6) or DL380 (Gen 9) hardware within a customer network. It makes use of AppWorks network installation and is intended to cover the initial network configuration steps for a NOAM, Query Server, SOAM and MP server which include switch configuration (Cisco 4948 E-F switches), and validation of initial configuration.

This document describes the HLR Router product SW installation on the DL 360 (Gen6) or DL380 (Gen 9) Server deployed using Cisco 4948E-F switches. It does not cover hardware installation, site survey, customer network configuration, IP assignments, customer router configurations, or the configuration of any device outside of the HLRR cabinet. The document TR007612 Ref [4] shows networking details for the HLRR 4.1 system. Users needing familiarity with these areas of interest should refer sources cited in **Section 1.2, References**.

1.2 References

[1] *TEKELEC Acronym Guide, MS005077*

[2] *Site Survey (Domestic US), SS005955 (AC), SS005956 (DC)*

[3] *Hardware Verification Plan, VP005629*

[4] *Network Interconnect: HLR Router 4.1, E74584-01*

[5] *Platform 6.5 Configuration Procedure Reference, 909-2249-001*

[6] *HP Solutions Firmware Upgrade Pack Release Notes, Release 2.x.x, (Min 2.2.9)*

[7] *HP Solutions Firmware Upgrade Pack Upgrade Guide, Release 2.x.x, (Min 2.2.9)*

[8] *Manufacturing Acceptance Test Procedure Subscriber Data Management Rack Mount Servers, 820-6641-01*

[9] *HLR Router Network Implementation Guide, WI006024*

[10] *C-Class Platform Passwords (Password Dragon) TR006061 (Oracle Restricted)*

1.3 Acronyms and Terminology

This table provides an alphabetized list of acronyms used throughout this document:

Acronym	Meaning
CSV	Comma Separated Values
DR	Disaster Recovery
HLR	Home Location Register
HLRR	Home Location Register Router
IMI	Internal Management Interface
ISL	Inter-Switch-Link
NE	Network Element
NOAM	Network Operations, Administration, Maintenance & Provisioning
iLO	HP Integrated Lights-Out
IPM	Initial Product Manufacture – the process of installing TPD or TVOE on hardware platform
Management Server	HP ProLiant DL360 G6 or DL380 G9 server used to host PMAC application in a virtual machine, to configure Cisco 4948E switches, and to serve other configuration purpose. This server is deployed with a quad serial card and is connected to both switches.
PMAC	Platform Management & Configuration
PMAC Application	PMAC is an application that provides platform-level management functionality for HP G6 system, such as the capability to manage and provision platform components of the system so it can host applications.
RMS	Rack Mount Server
SOAM	Systems Operations, Administration & Maintenance
TPD	Tekelec Platform Distribution (Linux OS)
TVOE	Tekelec Virtual Operating Environment
VIP	Virtual IP
VM	Virtual Machine
XMI	External Management Interface

Table 1 – Acronyms and Terminology

1.4 My Oracle Support (MOS)

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

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

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

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

MOS is available 24 hours a day, 7 days a week, 365 days a year.

1.5 Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at **1-800-223-1711** (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*.

The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

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

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

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

1.6 Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training: *http://education.oracle.com/communication*

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site: *www.oracle.com/education/contacts*

1.7 Locating Product Documentation on the Oracle Help Center Site

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

1. Access the OHC site at http://docs.oracle.com.
2. Click Industries.
3. Under the Oracle Communications subheading, click the Oracle Communications documentation link.
4. The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
5. Click the Product and then the Release Number. A list of the entire documentation set for the selected product and release appears.
6. To download a file to your location, right-click the PDF link, select Save target as (or similar command based on your browser), and save to a local folder.

1.8 Assumptions

This installation procedure assumes the following;

- The user has reviewed the Customer specific HLR Router Network Implementation Guide [[9] and has received assigned values for all requested information related to NOAM, Query Server, SOAM and MP installation.
- The user has taken assigned values from the Customer specific HLR Router Network Implementation Guide [9] and used them to compile XML files (see Appendix D for each NOAM and SOAM site's NE prior to attempting to execute this procedure.
- The user conceptually understands HLR Router topology and network configuration as described in the HLR Router Network Implementation Guide [9].
- The user has at least an intermediate skill set with command prompt activities on an Open Systems computing environment such as Linux or TPD.

1.9 XML Files (for installing NE)

The XML files compiled for installation of the each of the NOAM and SOAM site's NE must be maintained and accessible for use in Disaster Recovery procedures. The Oracle's Professional Services Engineer (PSE) will provide a copy of the XML files used for installation to the designated Customer Operations POC. The customer is ultimately responsible for maintaining and providing the XML files to Oracle's Customer Care Center (MOS) See Appendix L, if needed for use in Disaster Recovery operations.

1.10 How to use this Document

Although this document is primarily to be used as an initial installation guide, its secondary purpose is to be used as a reference for Disaster Recovery procedures. When executing this document for either purpose, there are a few points which help to ensure that the user understands the author's intent. These points are as follows;

- Before beginning a procedure, completely read the instructional text (it will appear immediately after the Section heading for each procedure) and all associated procedural WARNINGS or NOTES.
- Before execution of a STEP within a procedure, completely read the left and right columns including any STEP specific WARNINGS or NOTES.
- If a procedural STEP fails to execute successfully, STOP and contact Oracle's Customer Care Center (MOS) See Appendix L, for assistance before attempting to continue.

2. PRE-INSTALLATION SETUP

2.1 Installation Requirements

The following items/settings are required in order to perform installation for HP DL360 and DL380 based HLRR hardware:

- A laptop or desktop computer equipped as follows;
  - 10/100 Base-TX Ethernet Interface.
  - Administrative privileges for the OS.
  - An approved web browser (currently Microsoft Internet Explorer 7.0, 8.0, or 9.0 with support for JavaScript and cookies)
- An IEEE compliant 10/100 Base-TX Ethernet Cable, RJ-45, Straight-Through.
- USB flash drive with at least 4GB of the available space.
- TPD "root and admusr" user password.

NOTE: *When using the iLO for SSH connectivity, supported terminal Emulations are* ***VT100 or higher*** *(i.e. VT-102, VT-220, VT-320).*

2.2 Physical Connections

A connection to the VGA/Keyboard ports on the DL 360 (Gen6) or HP DL380 (Gen 9) rear panel or a connection to the iLO is required to initiate and monitor the progress of HLRR installation procedures.

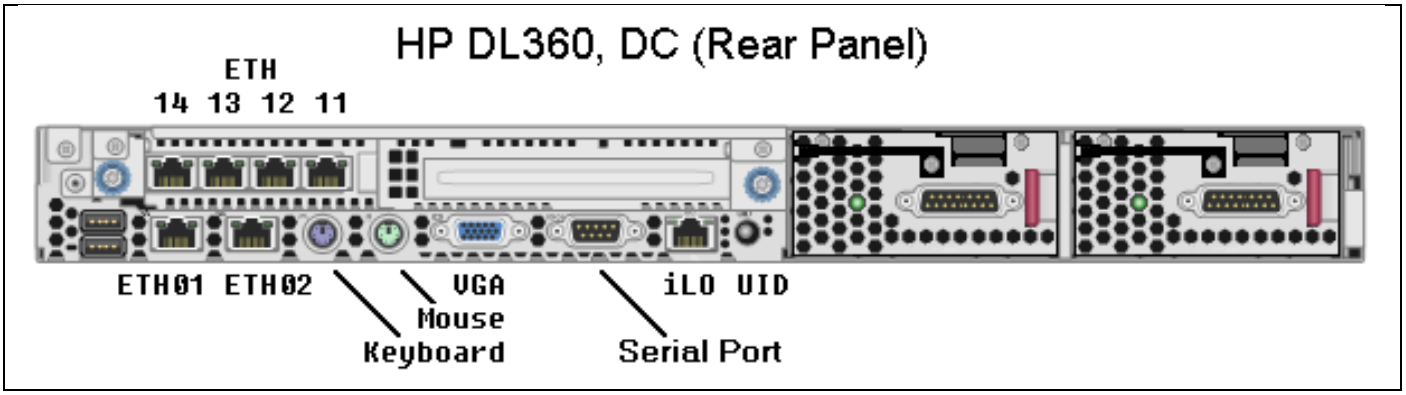


Figure 1 - HP DL360 (Gen6), DC (Rear Panel)

2.3 Access Alternatives for Application Install

This procedure may also be executed using one of the access methods described below:

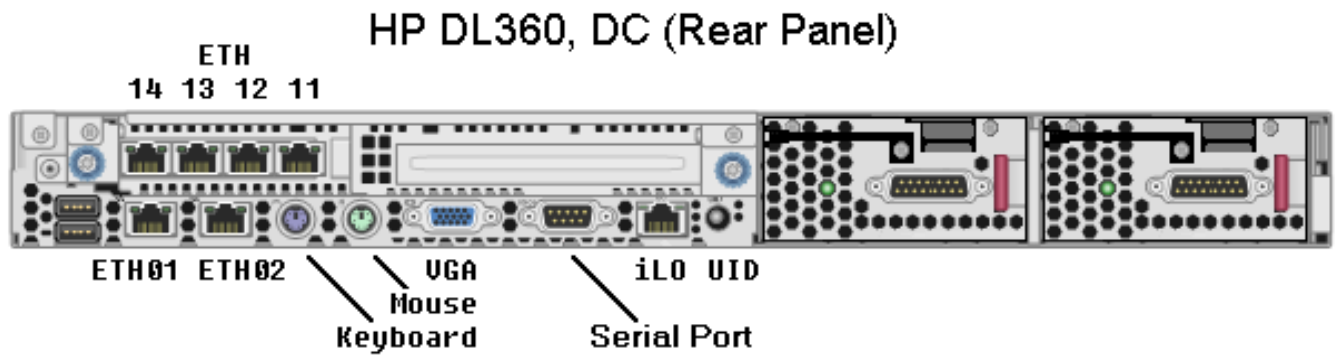


Figure 2 - HP DL360 (Gen6), DC (Rear Panel)

One of the **Access Methods** shown to the right may be used to initiate and monitor HLRR installation. **NOTE:** *Methods 3 & 4 may only be used on an HP DL360 with an iLO that has been previously configured with a statically assigned IP address. It is not intended for use with a new, out-of-the-box server.*	☐	**Method 1)** VGA Monitor and PS2 Keyboard.
	☐	**Method 2)** Laptop + epiphan SYSTEMS INC. KVM2USB Switch. http://www.epiphan.com/products/frame-grabbers/kvm2usb/
	☐	**Method 3)** iLO VGA Redirection Window, IE8, Ethernet cable. (See **Appendix A**)
	☐	**Method 4)** iLO access via SSH, terminal program, Ethernet cable.

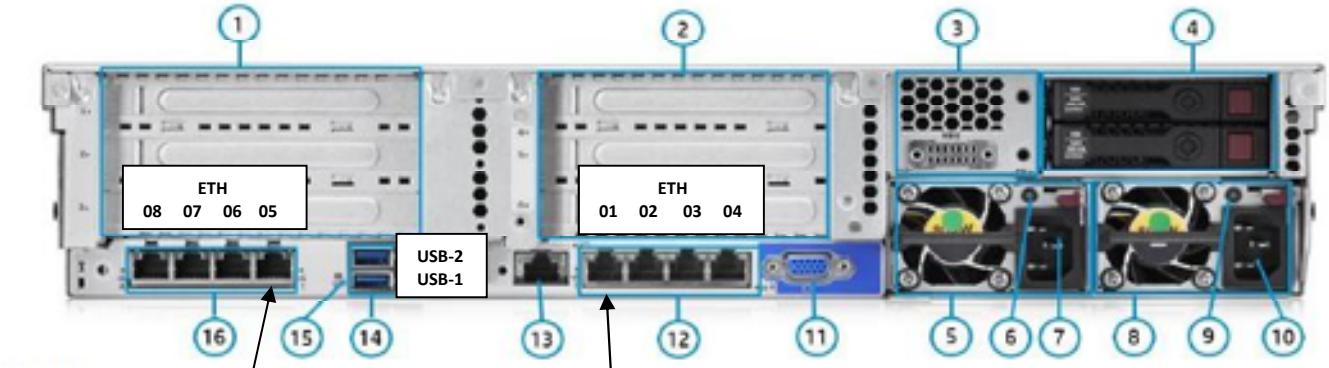


Figure 3 - HP DL380 (Gen9), DC (Rear Panel)

4-Port NIC Expansion Slot 0
Ethernet Ports
Eth05-Eth08

Internal 4-Port NIC
Ethernet Ports
Eth01-Eth04

1. PCI Slots (Slots 1-3 top to bottom, riser shipped standard)
2. PCI Slots (Slots 4-6top to bottom, requires second riser card, and second processor)
3. Optional serial port
4. Optional rear 2 SFF HDD (supported in 24 SFF or 12 LFF front end)
5. HP Flexible Slot Power Supply bay 1 (800w shown)
6. Power supply Power LED
7. Power supply Power connection
8. HP Flexible Slot Power Supply bay 2 (800w shown)
9. Power supply Power LED
10. Power supply Power connection
11. VGA connector
12. Embedded 4 x 1GbE Network Adapter
13. Dedicated iLO connector
14. USB 3.0 connectors (2)
15. Unit ID LED
16. Optional FlexibleLOM ports (Shown: 4 x 1GbE)

One of the **Access Methods** shown to the right may be used to initiate and monitor HLRR installation.

NOTE: *Methods 3 & 4 may only be used on an HP DL380 with an iLO that has been previously configured with a statically assigned IP address. It is not intended for use with a new, out-of-the-box server.*

☐ **Method 1)** VGA Monitor and USB Keyboard.

☐ **Method 2)** Laptop + epiphan SYSTEMS INC. KVM2USB Switch.
http://www.epiphan.com/products/frame-grabbers/kvm2usb/

☐ **Method 3)** iLO VGA Redirection Window, IE8, Ethernet cable. (See **Appendix A**)

☐ **Method 4)** iLO access via SSH, terminal program, Ethernet cable.

2.4 Activity Logging

All activity while connected to the system should be logged using a convention which notates the **Customer Name**, **Site/Node** location, **Server hostname** and the **Date**. All logs should be provided to Oracle for archiving post installation.

NOTE: *Parts of this procedure will utilize a VGA Monitor (or equivalent) as the active terminal. It is understood that logging is not possible during these times. The user is only expected to provide logs for those parts of the procedures where direct terminal capture is possible (i.e. SSH, serial, etc.).*

3. FIRMWARE AND BIOS SETTINGS

Prior to upgrading the Firmware of the DL360 and DL380 servers the CMOS Clock, BIOS Settings, and iLO IP Address needed to be configured. These configuration procedures are defined in **Appendix B, G, and H** of this document.

Several procedures in this document pertain to the upgrading of firmware on DL360 and DL380 servers and Cisco 4948 E-F switches that are part of the Platform 7.0.x configuration.

The required firmware and documentation for upgrading the firmware on HP hardware systems and related components are distributed as the HP *Solutions Firmware Upgrade Pack.* The minimum firmware release required for Platform 7.0.x is *HP Solutions Firmware Upgrade Pack 2.2.9 or higher*. If a firmware upgrade is needed, the current GA release of the *HP Solutions Firmware Upgrade Pack* should be used.

Each version of the *HP Solutions Firmware Upgrade Pack* contains multiple items including media and documentation. If an HP FUP 2.x.x version newer than the Platform 7.0.x minimum of HP FUP 2.2.9 is used, then the *HP Solutions Firmware Upgrade Guide* should be used to upgrade the firmware. Otherwise, the HP Solutions Firmware Upgrade Guide, Release 2.x.x should be used.

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

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

Refer to the Release Notes of the *[6] HP Solutions Firmware Upgrade Pack Release Notes, Release 2.x.x, (Min 2.2.9)* to determine specific firmware versions needed.

Contact **My Oracle Support (MOS)** for more information on obtaining the HP Firmware Upgrade Packs.

3.1 Configure the CMOS Clock, BIOS Settings, and iLO IP Address and Upgrade Firmware

The following procedure explains the steps needed to configure the CMOS Clock, BIOS Settings, and iLO IP Address of the DL360/DL80 RMS servers and upgrade the firmware. (If needed).

Procedure 1. Configure the CMOS Clock, BIOS Settings, and iLO IP Address and Upgrade Firmware

S T E P #	The following procedure explains the steps needed to configure the CMOS Clock, BIOS Settings, and iLO IP Address of the DL360/DL80 RMS servers and upgrade the firmware. (If needed). Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support **Appendix L -** MY ORACLE SUPPORT (MOS) and ask for assistance.	
1 ☐	**Configure RMS Server.**	Connect to the RMS Server using a VGA Display and USB Keyboard. **For HP DL 360 (G6) Server execute:** **Appendix B.** HP DL360 Configure CMOS Clock, BIOS Settings, and iLO IP Address **For HP DL 380 (G9) Servers execute:** **Appendix G.** Configure the HP DL380 Server CMOS Clock/BIOS Settings **Appendix H.** Configure the iLO/iLOM IP Address on DL380 Servers (iLO4)
2 ☐	**RMS Server:** Verify/Upgrade Firmware	Follow the appropriate procedure for the ProLiant DL360(G6) or DL380(G9) hardware type to verify and upgrade the HP server firmware using the procedures in [7] HP Solutions Firmware Upgrade Pack Upgrade Guide, Release 2.x.x, (Min 2.2.9) Check-off the associated Check Box in step 3 as the RMS server's CMOS Clock, BIOS Settings, and iLO IP Address has been configured and firmware is updated:

Procedure 1. Configure the CMOS Clock, BIOS Settings, and iLO IP Address and Upgrade Firmware

3 ☐	**RMS Server:** CMOS Clock, BIOS Settings, and iLO IP Address have been configured and firmware updated	Check-off the associated **Check Box** as the RMS server's CMOS Clock, BIOS Settings, and iLO IP Address has been configured and firmware is updated: **Primary Site:** ☐ RMS-1: _____ ☐ RMS-2: _____ ☐ RMS-3: _____ ☐ RMS-4: _____ ☐ RMS-5: _____ ☐ RMS-6: _____ ☐ RMS-7: _____ ☐ RMS-8: _____ ☐ RMS-9: _____ ☐ RMS-10: _____ **Disaster Recover Site: (Optional)** ☐ RMS-1: _____ ☐ RMS-2: _____ ☐ RMS-3: _____ ☐ RMS-4: _____ ☐ RMS-5: _____ ☐ RMS-6: _____ ☐ RMS-7: _____ ☐ RMS-8: _____ ☐ RMS-9: _____ ☐ RMS-10: _____
4 ☐	**Optional: Repeat on the Disaster Recovery RMS servers.**	

4. INSTALLATION

This section contains the installation overview, and includes information about required materials, strategies, and SNMP configuration. Note that IPM refers to installing TVOE on the target system. TVOE is used when virtualization is needed (e.g., for the PMAC and the NOAM/SOAM/QS/MPs). Customers are required to download all software from the Oracle Software Delivery Cloud (OSDC). A readme file which provides instructions for the customer to create required bootable USBs using the .usb file will be included with the software, also see Appendix I of this document. Please obtain required bootable USBs from the customer representative.

4.1 Required Materials

- One (1) USB of TPD 7.x, release specified by Release Notes.
- One (1) USB of PMAC 6.x, release specified by Release Notes.
- One (1) USB of TVOE 3.0, release specified by Release Notes.
- One (1) USB of HLRR 4.1.x and all configuration files
- Passwords for root and admusr users on the local system.
- Access to the iLO Terminal or direct access to the server VGA port.
- HP Solutions Firmware Upgrade Pack Upgrade Guide, Release 2.x.x, (Min 2.2.9) (the latest version should be used if an upgrade is to be performed; otherwise version 2.2.9 is the minimum).
- A 4GB or larger USB Flash Drive is required.
- NAPD and all relevant configuration materials for ALL sites involved. This includes host IP addresses, site network element XML files, and netConfig configuration files.
- Keyboard and monitor for configuring iLO addresses.

4.2 Installation Strategy

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

The following list summarizes this process.

1. An overall installation requirement is established. This data that should be collected:
- The total number of sites and what type of hardware will be used.
- The number of servers at each site and their role(s)
- Establish the number of rack mounted servers at each site
- What time zone should be used across the entire collection of application sites?
- Will SNMP traps be viewed at the application level, or will an external NMS be used (or both)

2. A site survey is conducted to determine exact networking and site details. Additionally, IP networking options must be well understood, and IP address allocations collected from the customer and placed in the NAPD, in order to complete switch and network configurations.

4.3 SNMP Configuration

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

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

- HLRR Application Servers (NOAM, SOAM, MPs of all types)
- HLRR Auxiliary Components (Switches, TVOE hosts, and PMAC)

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

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

The following components; PMAC (App), Switches (4948E-F), and TVOE for all HLRR Servers should have their SNMP trap destinations set to the local NOAM VIP and the customer NMS, if available.

Note: All the entities **MUST** use the same Community String during configuration of the NMS server.

Note: SNMP community strings i.e. (Read Only or Read Write SNMP community strings) should be the same for all the components like OAM/MP servers, PMACs, TVOEs and external NMS.

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

4.4 NTP Strategy

The following set of general principals' capture the recommendations for NTP configuration of HLRR.

Principle 1 – NOAM/SOAM's TVOE Hosts should synchronize to the customer's NTP network
The NOAM/SOAM's TVOE Hosts should synchronize to the customer's NTP network using three separate NTP sources as a minimum. See *Figure 2: Site NTP Topology* for clarification.

Principle 2 – Provide a robust pool of sources
The pool of customer NTP server references should be of stratum 3 or above, accurate and highly reliable. If possible both local site server and backup remote site servers should be provided. Three or more customer NTP sources are required.

Principle 3 - Virtual (NOAM/SOAM/MP) guests should synchronize to their TVOE hosts
When virtualization is used in the product deployment, virtual guests (NOAM/SOAM/MP) should use their TVOE hosts as their NTP references. See *Figure 2: NTP Topology* for clarification.

Principle 4 - MP TVOE hosts should use their SOAM's TVOE hosts
MP TVOE hosts should use their SOAM's TVOE hosts and the PMAC's TVOE host as the third NTP source. See *Figure 2: Site NTP Topology* for clarification.

Principle 5 - Virtual guests should not be used as NTP servers
Avoid specifying virtual guests as NTP references. Guest emulated clocks have been shown to result in poor NTP server behavior

Principle 6 - Prefer local references
When references from multiple sites or networks are used on one server, the "prefer" keyword should be applied to the local references.

Principle 7 - Ensure connectivity
Care should be taken to ensure that all NTP references are reachable through the appropriate networking configuration. In particular firewall rules must be correctly specified to allow NTP clients to connect to their specified references.

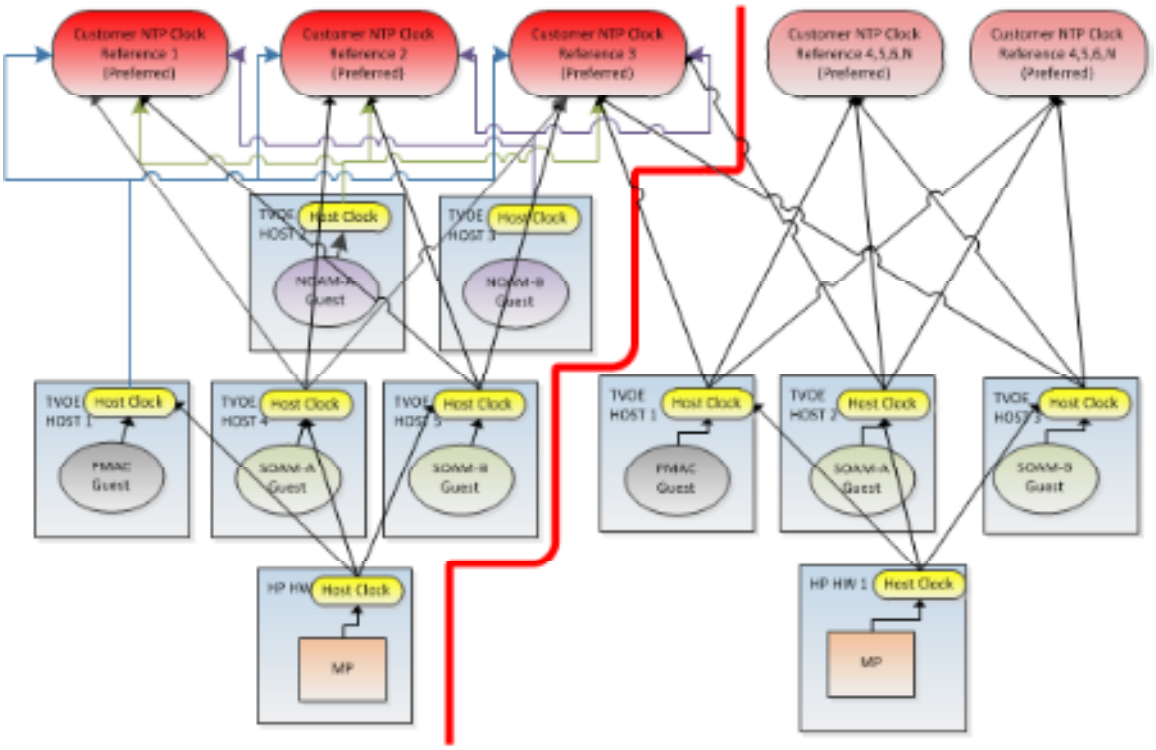


Figure 2: Site NTP Topology

4.5 Overview of HLRR Networks

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

Network Name	Default VLAN ID*	Routable	Description
Control	1	No	Network used by PMAC to IPM the servers/blades/VMs. Refer to the NAPD for site-specific IP information. (IPs are assigned via by the PMAC using DHCP)
Management	2	Yes	Network used for iLO interfaces and Management Also used to provide remote access to the TVOE and PMAC servers.
XMI	3	Yes	Network used to provide access to the HLRR entities (GUI, ssh), and for inter-site communication
IMI	4	No	Network used for intra-site communication
XSI-1	5	Yes	Network used for HLRR Signaling Traffic
XSI-2	6	Yes	Network used for HLRR Signaling Traffic
XSI-3**	7	Yes	Network used for HLRR Signaling Traffic
XSI-4**	8	Yes	Network used for HLRR Signaling Traffic

* The VLAN ID assignments are site and deployment specific.
** Optional

5. INSTALLING HLR ROUTER ON THE CUSTOMER NETWORK

This section contains the software installation procedures, including preparation and configuration information for a HLRR site. The procedures in this section are expected to be executed in the order presented in this document. If a procedural STEP fails to execute successfully, STOP and contact My Oracle Support by referring to **My Oracle Support (MOS)**.

Sudo - Platform 7.0.x introduces a new non-root user 'admusr'. As a non-root user, many commands --when run as admusr-- now require the use of 'sudo'. Using sudo will require a password with the first command, as well as intermittently over a period of time. Therefore, if a prompt for the "[sudo] password:" appears, the user should re-enter the admusr login password.

5.1 HLR Router Installation Matrix

Installing the HLR Router product is a task which requires multiple installations of varying types. The matrix below provides a guide to the user as to which procedures are to be performed on which site types. The user should be aware that this document only covers the necessary configuration required to complete product install. Refer to the online help or contact Oracle's Customer Care Center (MOS) See Appendix L, with post installation configuration options.

NOTE: *Although the NOAM sites are fully redundant by function, we must distinguish between them during installation due to procedural changes based on the installation sequence. The user should be aware that any reference to the "NOAM" site refers to the 1st installation of a NOAM pair on the customer network while references to the "DR NOAM" site refers to the 2nd NOAM pair to be installed.*

Server Type		PROCEDURES TO PERFORM										
		1-3	4-8	9	10-11	12	13	14	15	16	17	18-19
☐	Management Server	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
☐	Cisco Switches	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
☐	PMAC	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
☐	NOAM-A	✗	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
☐	NOAM-B	✗	✗	✗	✓	✓	✗	✓	✗	✓	✗	✗
☐	DR NOAM	✓	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗
☐	SOAM	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✗
☐	MP	✗	✗	✗	✓	✓	✗	✓	✓	✗	✗	✓
☐	Query Server	✗	✗	✗	✓	✓	✗	✓	✗	✓	✗	✗

Table 2 - HLR Router Installation Matrix

HLR Router Installation: List of Procedures

Table 3 - HLR Router Installation: List of Procedures

6. SOFTWARE INSTALLATION PROCEDURE

6.1 Install TVOE on First RMS (PMAC Host)

This procedure will install TVOE 3.0.x on the Management Server

Requirments: Procedure 1. Configure the CMOS Clock, BIOS Settings, and iLO IP Address and Upgrade Firmware

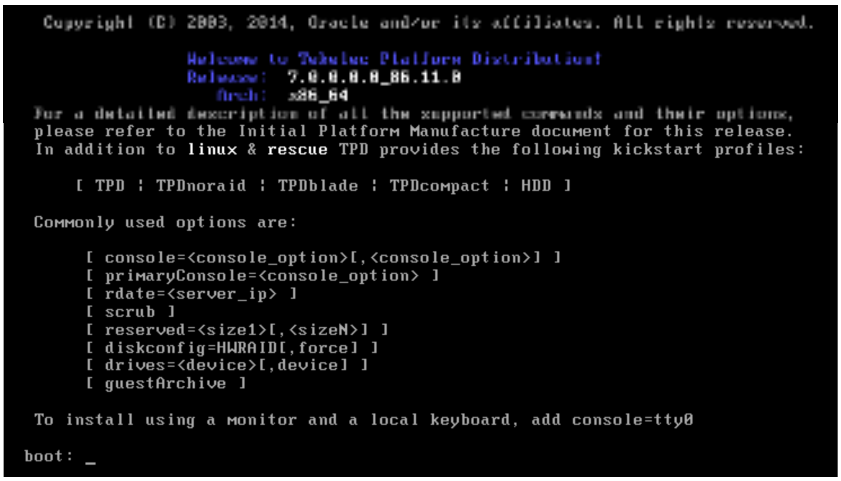
Needed material: TVOE 3.0.x Media (USB or CD/DVD)

This section describes the process of installing TVOE on the first rack mount server. Throughout this section, the first RMS server refers to the server that shall host the PMAC VM.

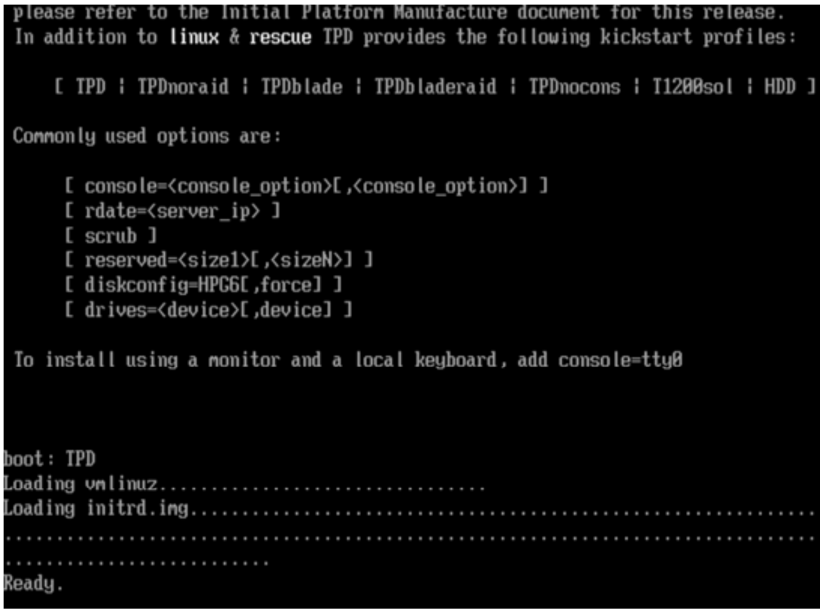
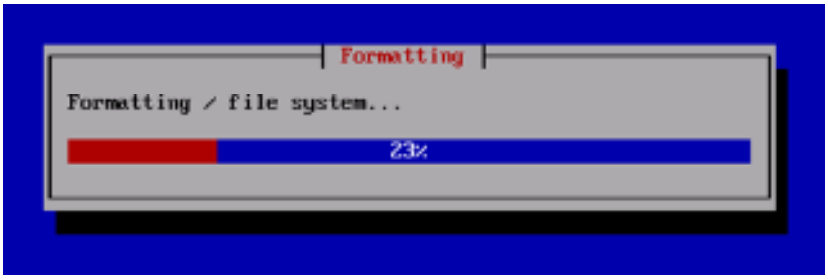
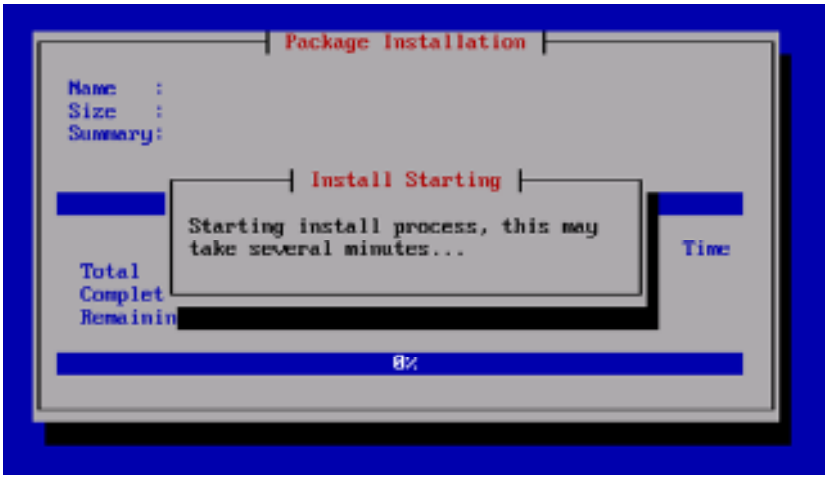
Procedure 2. Install TVOE on First RMS (PMAC Host)

S T E P #	This procedure explains the steps needed to install TVOE 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 My Oracle Support **Appendix L -** MY ORACLE SUPPORT (MOS) and ask for assistance.	
1 ☐	**RMS Server:** Insert TVOE Media into Server	Insert the OS IPM media (CD/DVD or USB) into the CD/DVD tray/USB slot of the rack mount server. Refer to **Appendix I** for creating a bootable USB. Alternatively, ISO can be mounted using Virtual media as well. Refer to **Appendix F.**
2 ☐	**Power Cycle Server**	Power cycle the server by holding the power button in until the button turns amber, then release. Wait 5 seconds, then press the power button and release it again to power on the system.
3 ☐	**Select Boot Method**	For some servers you must select a boot method so that the server does not boot directly to the hard drive. For HP rack mount servers, hit **F11** when prompted to bring up the boot menu and select the appropriate boot method.

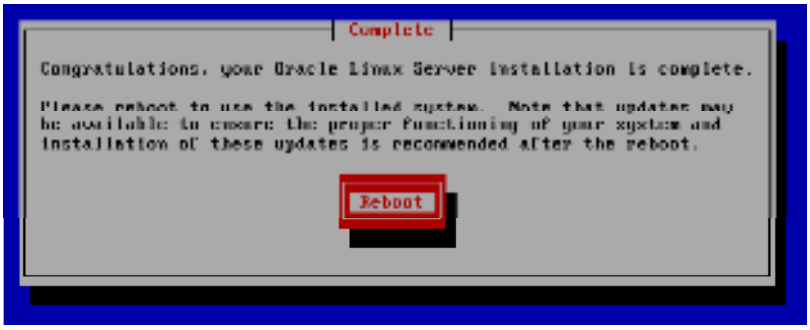
Procedure 2. Install TVOE on First RMS (PMAC Host)

5 ☐	**RMS Server:** 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=HWRAID,force console=tty0**

Procedure 2. Install TVOE on First RMS (PMAC Host)

6 ☐	**RMS Server:** Monitor the IPM Installation	The IPM process takes about **30 minutes**, you will see several messages and screens in the process. The following screens will be displayed:   

Procedure 2. Install TVOE on First RMS (PMAC Host)

7 ☐	**RMS Server:** Install Complete-Reboot	Once the IPM is complete, you will be prompted to press Enter as shown below to reboot the server. Remove the disk or USB from the server or unmount the TPD image from the iLO and press **Enter** to reboot the server.  After a few minutes and multiple reboots, the the server boot sequence will start and eventually display that it is booting the new IPM (TVOE) load.  **Note:** A successful IPM platform installation process results in a user login prompt.
8 ☐	**Optional:** TVOE DR RMS-1 server	**Optional:** Repeat this procedure for the Disaster Recovery RMS-1Server.
THIS PROCEDURE HAS BEEN COMPLETED		

6.2 Configure Management Server Network (All Sites)

This procedure will configure the Network on the TVOE/Management Server

Requirements: Procedure 2. Install TVOE on First RMS (PMAC Host) 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 MY ORACLE SUPPORT AND ASK FOR ASSISTANCE.

Procedure 3: Configure Management Server Network

<table>
<tr><th>Step</th><th>Procedure</th><th>Result</th></tr>
<tr><td>1. ☐</td><td>Access the HP server's console.</td><td>Connect to the HP server's console using one of the access methods described in Section 2.3.</td></tr>
<tr><td>2. ☐</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.
<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):
bond0
<TVOE_Control_Bridge_Interface></td></tr>
<tr><td>Management (XMI)</td><td>management</td><td>Fill in the appropriate value:
bond1
<TVOE_Management_Bridge_Interface></td></tr>
<tr><td>imi</td><td>imi</td><td>Fill in the appropriate value:
bond 0.4
<TVOE_IMI_Bridge_Interface></td></tr>
</table></td></tr>
</table>

Procedure 3: Configure Management Server Network

Step	Procedure	Result
3. ☐	**TVOE Management server iLO:** *Verify the Control Network*	Verify the control network bridge is running: $ **sudo netAdm query --type=Bridge --name=control** Bridge Name: control On Boot: yes Protocol: none IP Address: 192.168.1.x Netmask: 255.255.255.0 Promiscuous: no Hwaddr: d8:9d:67:1c:bc:84 MTU: 1500 Delay: 4 Bridge Interface: bond0 Bond0 is created by default when TVOE is installed on the server so the control bridge should have been configured; if so then skip to the next step. If bond0 is missing create the control network bond0 and assign eth01 and eth02 to it: ***Example:*** $ **sudo netAdm add --device==bond0 --onboot=yes --type=Bonding --mode=active-backup --miimon=100** Interface bond0 added $ **sudo netAdm set --device=eth01 --type=Ethernet --master=bond0 --slave=yes --onboot=yes** Interface eth01 updated $ **sudo netAdm set --device=eth02 --type=Ethernet –-master=bond0 --slave=yes --onboot=yes** Interface eth02 updated $ **sudo netAdm add --type=Bridge --name=control --bootproto=dhcp --onboot=yes --bridgeInterfaces=bond0** Verify the control network bridge is now running: $ **sudo netAdm query --type=Bridge --name=control** Bridge Name: control On Boot: yes Protocol: none IP Address: 192.168.1.x Netmask: 255.255.255.0 Promiscuous: no Hwaddr: d8:9d:67:1c:bc:84 MTU: 1500 Delay: 4 Bridge Interface: bond0

Procedure 3: Configure Management Server Network

Step	*Procedure*	*Result*
4. ☐	**TVOE Management Server iLO:** *Add the Internal Network Management interface bridge on bond0.4*	Create the imi network bridge: $ **sudo netAdm add --device=bond0.4** Interface bond0.4 added $ **sudo netAdm add --name=imi --type=Bridge --bridgeInterface=bond0.4** Setting up the bridge and unsetting network info Interface bond0.4 was updated. Bridge imi added! Verify the imi network bridge is running: $ **sudo netAdm query --type=Bridge --name=imi** Bridge Name: imi On Boot: yes Protocol: none IP Address: Netmask: Promiscuous: no Hwaddr: d8:9d:67:1c:bc:84 MTU: Delay: 4 Bridge Interface: bond0.4

Procedure 3: Configure Management Server Network

Step	Procedure	Result
5. ☐	**DL360 Servers Only** **TVOE Management Server iLO:** *Add the External Management Interface (XMI) bridge on bond 1 = eth11 + eth12*	**Execute this step for DL360 servers only. For DL380 servers skip to step 6.** Add the management network: $ **sudo netAdm add --device=bond1** Interface bond1 added $ **sudo netAdm set --device=eth11 --master=bond1 --slave=yes --onboot=yes --bootproto=none** Interface eth11 was updated. Interface eth11 updated $ **sudo netAdm set --device=eth12 --master=bond1 --slave=yes --onboot=yes --bootproto=none** Interface eth12 was updated. Interface eth12 updated $ **sudo netAdm add --name=management --type=Bridge --bridgeInterface=bond1** Setting up the bridge and unsetting network info Interface bond1 was updated. Bridge management added! Verify that the external management bridge (XMI) has been configured: $ **sudo netAdm query --type=Bridge --name=management** Bridge Name: management On Boot: yes Protocol: none IP Address: Netmask: Promiscuous: no Hwaddr: ac:16:2d:99:45:84 MTU: 1500 Delay: 4 stp: on Bridge Interface: bond1

Procedure 3: Configure Management Server Network

Step	Procedure	Result
6. ☐	**DL380 Servers Only** **TVOE Management Server iLO:** *Add the External Management Interface (XMI) bridge on bond 1 = eth05 + eth06*	**Execute this step for DL380 servers only. For DL360 servers return to step 5.** Add the management network: $ **sudo netAdm add --device=bond1** Interface bond1 added $ **sudo netAdm set --device=eth03 --master=bond1 --slave=yes --onboot=yes --bootproto=none** Interface eth03 was updated. Interface eth03 updated $ **sudo netAdm set --device=eth04 --master=bond1 --slave=yes --onboot=yes --bootproto=none** Interface eth04 was updated. Interface eth04 updated $ **sudo netAdm add --name=management --type=Bridge --bridgeInterface=bond1** Setting up the bridge and unsetting network info Interface bond1 was updated. Bridge management added! Verify that the external management bridge (XMI) has been configured: $ **sudo netAdm query --type=Bridge --name=management** Bridge Name: management On Boot: yes Protocol: none IP Address: Netmask: Promiscuous: no Hwaddr: ac:16:2d:99:45:84 MTU: 1500 Delay: 4 stp: on Bridge Interface: bond1

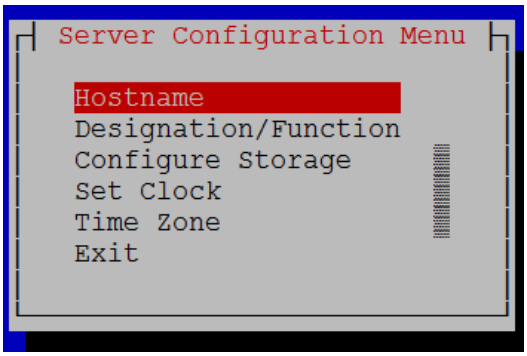
Procedure 3: Configure Management Server Network

Step	Procedure	Result
7. ☐	**TVOE Management Server iLO:** *Assign IP address to the XMI management network*	Set XMI management bridge IP address: **Note:** The output below is for illustrative purposes only. The NAPD information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure. ***Syntax:*** $ **sudo netAdm set --name=management --type=Bridge --address=<XMI Management_ip address> --netmask=<netmask>** ***Example:*** $ **sudo netAdm set --name=management --type=Bridge --address=10.240.37.2 --netmask=255.255.255.224** Interface bond1 was updated. Setting up the bridge and unsetting network info Interface bond1 was updated. Bridge management updated! Verify the management network bridge by running the following command: $ **sudo netAdm query --type=Bridge --name=management** Bridge Name: management On Boot: yes Protocol: none IP Address: 10.240.37.2 Netmask: 255.255.255.224 Promiscuous: no Hwaddr: ac:16:2d:99:45:84 MTU: 1500 Delay: 4 stp: on Bridge Interface: bond1

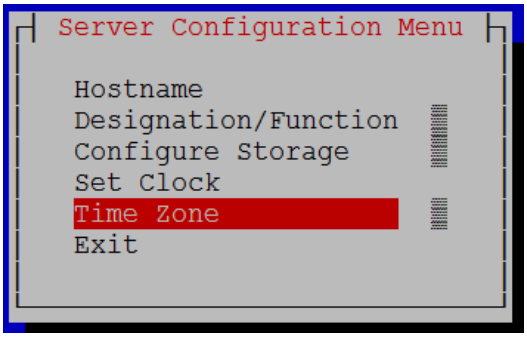
Procedure 3: Configure Management Server Network

Step	Procedure	Result
8. ☐	**TVOE Management Server iLO:** *Assign gateway IP address to the default route*	Add the default route on the management network. **Note:** The output below is for illustrative purposes only. The NAPD information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure. ***Syntax:*** $ **sudo netAdm add --route=default --gateway=<mgmt_gateway_address> --device=<TVOE_Managament_Bridge>** ***Example:*** $ **sudo netAdm add --route=default --gateway=10.250.43.161 --device=management** Route to management added Verify the management network by running the following command $ **sudo netAdm query --route=default --device=management** Routes for TABLE: main and DEVICE: management * NETWORK: default GATEWAY: 10.250.43.161
9. ☐	**TVOE Management Server iLO:** *Assign IP address to the control network*	Set the control network bridge IP address: **$ sudo netAdm set --type=Bridge --name=control --bootproto=none --address=192.168.1.4 --netmask=255.255.255.0** Interface bond0 was updated. Setting up the bridge and unsetting network info Interface bond0 was updated. Bridge control updated! Verify the control network bridge has been configured with IP address: **$ sudo netAdm query --type=Bridge --name=control** Bridge Name: control On Boot: yes Protocol: none IP Address: 192.168.1.4 Netmask: 255.255.255.0 Promiscuous: no Hwaddr: 98:4b:e1:74:d5:78 MTU: Delay: Bridge Interface: bond0

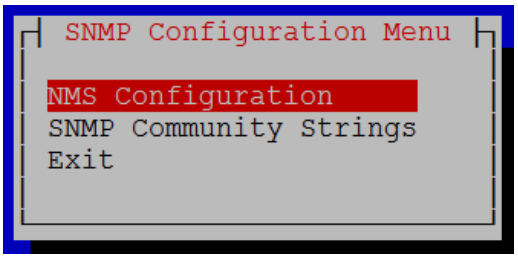
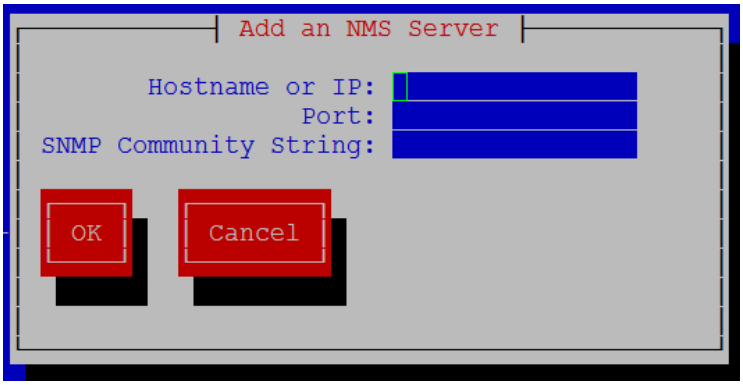
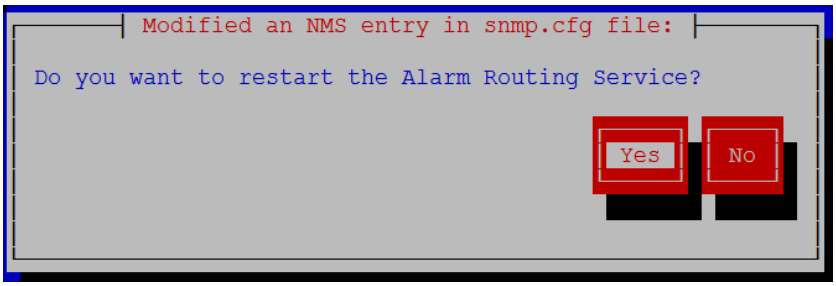
Procedure 3: Configure Management Server Network

Step	Procedure	Result
10. ☐	**TVOE Management Server iLO:** *Setup Syscheck*	***Note**: syscheck must be configured to monitor bonded interfaces.* Replace "bondedInterfaces" with "bond0" or "bond0,bond1" if segregated networks are used: $ **sudo syscheckAdm net ipbond --set --var=DEVICES --val=bond0,bond1** $ **sudo syscheckAdm net ipbond -enable** $ **sudo syscheck -v net ipbond**
11. ☐	**TVOE Management Server iLO:** *Set Hostname*	Set the server hostname: $ **sudo su – platcfg** **1.** Navigate to **Server Configuration ➤ Hostname**  **2.** Select Edit **3.** Set TVOE Management Server hostname **4.** Press OK. **5.** Navigate out of Hostname

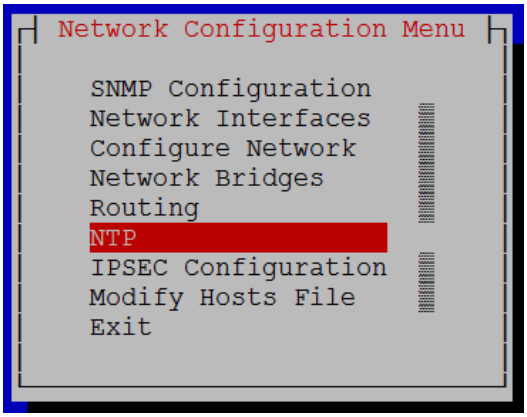
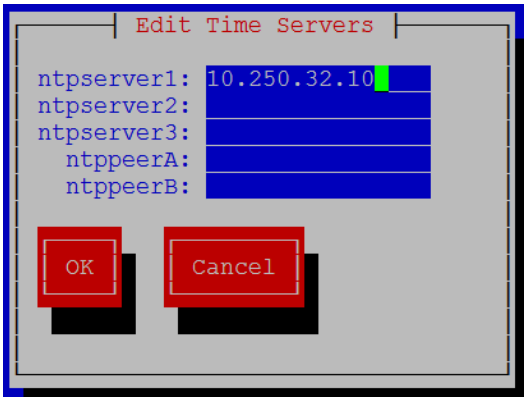
Procedure 3: Configure Management Server Network

Step	*Procedure*	*Result*
12. ☐	**TVOE Management Server iLO***:* *Set Time Zone and/or Hardware Clock*	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. **4.** Press OK. **5.** Navigate out of Server Configuration

Procedure 3: Configure Management Server Network

Step	Procedure	Result
13. ☐	**TVOE Management Server iLO:** *Configure SNMP trap destination* *See the NAPD documention for SNMP specifics.*	Configure SNMP trap destination: **1.** Navigate to **Network Configuration ➤ SNMP Configuration ➤ NMS Configuration**.  **2.** Select **Edit** and then choose 'Add a New NMS Server'. **3.** The 'Add an NMS Server' page will be displayed.  **4.** Complete the form by entering NMS server IP, Port (default port is 162) and community string provided by the customer about the SNMP trap destination. **5.** Select **OK** to finalize the configuration. **6.** The 'NMS Server Action Menu' will now be displayed. **7.** Select **Exit**. The following dialogue will then be presented:  **8.** Select **Yes** and then wait a few seconds while the Alarm Routing Service is restarted. **9.** At that time the SNMP Configuration Menu will be presented. ***Note**: All alarm information will then be sent to the NMS located at the destination.*

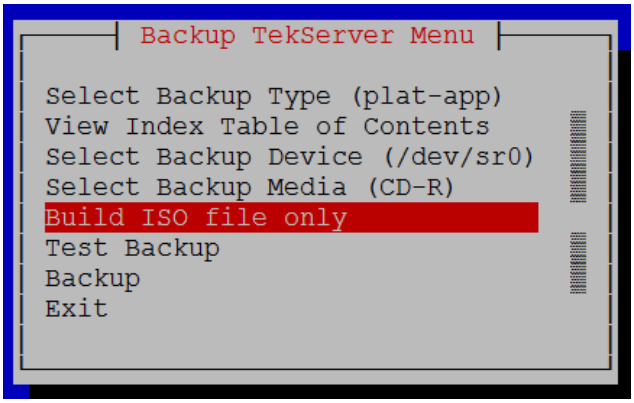
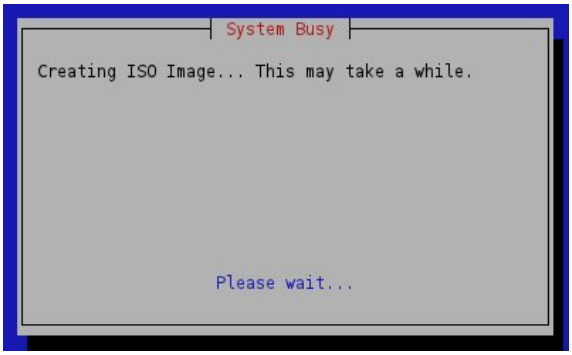
Procedure 3: Configure Management Server Network

Step	Procedure	Result
14. ☐	**TVOE Management Server iLO:** *Configure NTP*	Configure NTP servers: **1.** Navigate to **Network Configuration ➤ NTP.**  **2.** Set NTP server IP address to point to the customer provided NTP servers (3 NTP Servers are required). See paragraph **4.4 NTP Strategy** for more information on NTP deployment.  **3.** Press OK. **4.** Navigate out of Network Configuration **5.** Exit platcfg.
15. ☐	**TVOE Management Server iLO:** *Set server time*	Set time based on NTP server: $ **sudo service ntpd stop** $ **sudo ntpdate ntpserver1** $ **sudo service ntpd start**

Procedure 3: Configure Management Server Network

Step	*Procedure*	*Result*
16. ☐	**TVOE Management Server iLO*:*** *Reboot the server*	Reboot the server: $ **sudo init 6** Wait until the reboot completes and re-login with TVOE admusr credentials.
17. ☐	**TVOE Management Server iLO:** *Verify server health*	Verify server health: $ **sudo alarmMgr -alarmStatus** ***Note**: This command should return no output on a healthy system. If any alarms are reported, please stop and contact Oracle's Customer Care Center before continuing.*

Procedure 3: Configure Management Server Network

Step	Procedure	Result
18. ☐	**TVOE Management Server iLO:** *Perform a TVOE backup*	Login as platcfg user. The platcfg main menu will be shown $ **sudo su – platcfg** **1.** Navigate to **Maintenance ➤Backup and Restore ➤Backup Platform (CD/DVD)** **2.** The 'Backup TekServer Menu' page will now be shown.  **3.** Select **Build ISO file only**. ***Note****: Creating the ISO image may happen so quickly that this screen may only appear for an instant.*  **4.** After the ISO is created, platcfg will return to the Backup TekServer Menu as shown in step 2. **5.** The ISO has been created and is located in the /var/TKLC/bkp/ directory. An example filename of a backup file that was created is: *"hostname1307466752-plat-app-201104171705.iso"* **6.** Exit platcfg.

Procedure 3: Configure Management Server Network

Step	*Procedure*	*Result*
19. ☐	**Customer Server SSH:** *Copy backup image to the customer server*	Login to the customer server and copy backup image to the customer server where it can be safely stored.
20. ☐	*Configure the DR RMS-1 server networking.*	**Optional: Repeat this procedure for the Disaster Recovery RMS-1 Server.**
THIS PROCEDURE HAS BEEN COMPLETED		

6.3 Deploy PMAC on Management Server (All Sites)

This procedure will deploy PMAC 6.0.x on the TVOE Host

Prerequisite:

- **Procedure 2. Install TVOE on First RMS (PMAC Host)** has been completed.
- **Procedure 3: Configure Management Server Network** has been completed.

Needed material:

- **PMAC 6.0.x 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 My Oracle Support and ask for assistance.

Procedure 4. PMAC Deployment

Step	Procedure	Result
1. ☐	**1st RMS iLO/iLOM:** Login and Launch the Integrated Remote Console	Log in to iLO/iLOM; follow **Appendix A** Accessing the iLO VGA Remote Console Window for instructions on how to access the iLO/iLOM . **https://<management_server_iLO_ip>**

Procedure 4. PMAC Deployment

2. ☐	**TVOE iLO/iLOM:** Mount the PMAC Media to the TVOE Server	Use one of the following 2 options to mount the PMAC Media: Option 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/sdd1/872-2586-101-6.0.0_57.3.0-pmac-x86_64.iso Use the output of the previous command to populate the next command **$ sudo mount -o loop /media/sdb1/872-2586-101-6.0.0_57.3.0-pmac-x86_64.iso /mnt/upgrade** Option 2: If using an ISO image, run the following to mount it: **$ sudo mount -o loop ISO_FILENAME.iso /mnt/upgrade** Next Validate the PMAC media by executing the following commands: **$ cd /mnt/upgrade/upgrade** **$ sudo .validate/validate_cd** Validating cdrom... UMVT Validate Utility v2.2.2, (c)Tekelec, June 2012 Validating <device or ISO> Date&Time: 2012-10-25 10:07:01 Volume ID: tklc_872-2441-106_Rev_A_50.11.0 Part Number: 872-2441-106_Rev_A Version: 60.11.0 Disc Label: PM&C Disc description: PM&C The media validation is complete; the result is: PASS CDROM is Valid **Note:** If the media validation fails, the media is not valid and should not be used.

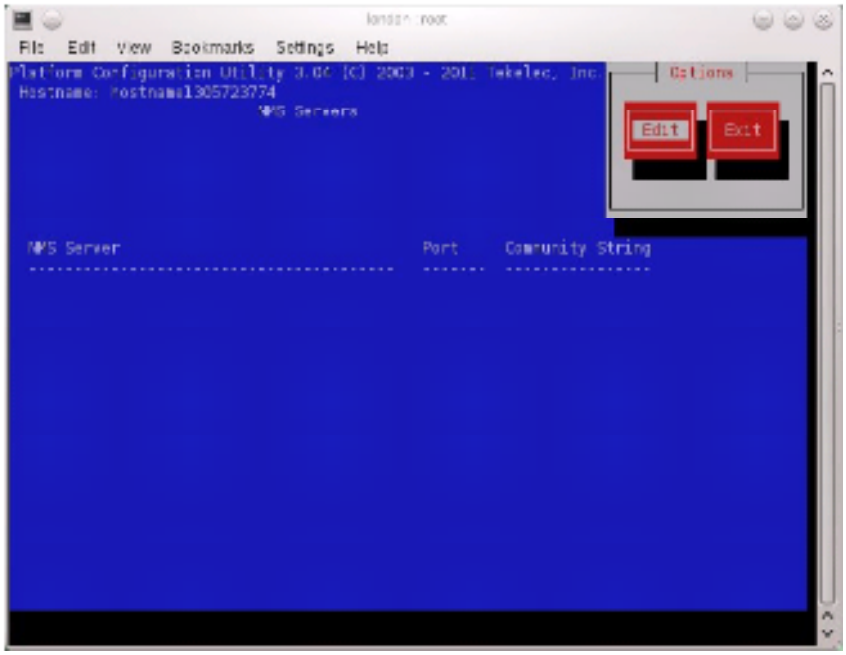
Procedure 4. PMAC Deployment

3. ☐	**TVOE iLO/iLOM:** Deploy PM&C Refer to the NAPD documentation for this networking information.	Using the pmac-deploy script, deploys the PMAC instance using the configuration captured during the site survey. **$ cd /mnt/upgrade/upgrade** **$ sudo ./pmac-deploy --guest=<PMAC _Name>** **--hostname=<PMAC_Name> --controlBridge=<TVOE_Control_Bridge>** **--controlIP=<PMAC_Control_ip_address>** **--controlNM=<PMAC_Control_netmask>** **--managementBridge=<PMAC_Management_Bridge>** **--managementIP=<PMAC_Management_ip_address>** **--managementNM=<PMAC_Management_netmask/prefix>** **--routeGW=<PMAC_Management_gateway_address>** **--ntpserver=<TVOE_Management_server_ip_address>** **--isoimagesVolSizeGB=20** For example: **$ sudo ./pmac-deploy --guest=pmac --hostname=pmac --controlBridge=control --controlIP=192.168.1.1 --controlNM=255.255.255.0 --managementBridge=management --managementIP=10.240.241.118 --managementNM=255.255.255.0 --routeGW=10.240.241.1 --ntpserver=10.240.241.105 --isoimagesVolSizeGB=20** The PMAC 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**: This step takes between **5 and 10 minutes**.
4. ☐	**TVOE iLO/iLOM:** Unmounts the Media	The media should auto-unmount, if it does not, unmount the media using the following command: **$ cd /** **$ sudo /bin/umount /mnt/upgrade** Remove the media from the drive.

Procedure 4. PMAC Deployment

5. ☐	**TVOE iLO/iLOM:** SSH into the Management Server	Using an SSH client such as putty, ssh to the TVOE host as ***admusr***. Login using **virsh**, and wait until you see the login prompt : **$ sudo /usr/bin/virsh list** Id Name State ---------- 2 PMAC running **$ sudo /usr/bin/virsh console <PMAC>** [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 PMAC:** Verify the PMAC is configured correctly on first boot	Establish an SSH session to the PMAC, login as ***admusr***. Run the following command (there should be no output): **$ sudo /bin/ls /usr/TKLC/plat/etc/deployment.d/**
7. ☐	**TVOE iLO/iLOM:** Error doing verification, if error is outputted	If an error was made use the following command to delete the PMAC Guest and then re-deploy the guest again: **$ sudo guestMgr --remove <PMAC_Name>**
8. ☐	**Virtual PMAC:** Set the PMAC time zone	Determine the Time Zone to be used for the PMAC. **Note:** Valid time zones can be found in **Appendix E.** **$ sudo set_pmac_tz.pl <time zone>** Example: $ sudo set_pmac_tz.pl Ect/UTC Verify that the time zone has been updated: **$ sudo date**

Procedure 4. PMAC Deployment

9. ☐	**Virtual PMAC:** Set SNMP	Set SNMP by running the following: **$ sudo su – platcfg** Navigate to **Network Configuration -> SNMP Configuration -> NMS Configuration.**  Select **Edit** and then choose **Add a New NMS Server**. The ***'Add an NMS Server'*** page will be displayed. 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. 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. Exit platcfg.
10. ☐	**Virtual PMAC:** Reboot the server	Reboot the server by running: **$ sudo init 6**
11. ☐	Deploy PMAC on DR Management server	**Optional:** Repeat this procedure for the Disaster Recovery Manageement Server.
THIS PROCEDURE HAS BEEN COMPLETED		

6.4 Configure PMAC Application (All Sites)

This procedure will provide PMAC configuration using the web interface.

Requirements: Procedure 4. PMAC Deployment has been completed.

Note: The installer must be knowledgeable of the network configuration. If you make a mistake, then click "Cancel" button and try again. The finish step may take longer time because it reconfigures the network and attempts to connect may fail.

Note: After you have completed an initialization, the network parameters can no longer be changed through the GUI.

Note: If you need to reset any of the network information, you must run this command in the PMAC shell: "**sudo pmacadm resetProfileConfig**". This command will delete the existing configuration and allow you to run through the initialization wizard again.

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

IF THIS PROCEDURE FAILS, CONTACT MY ORACLE SUPPORT AND ASK FOR ASSISTANCE.

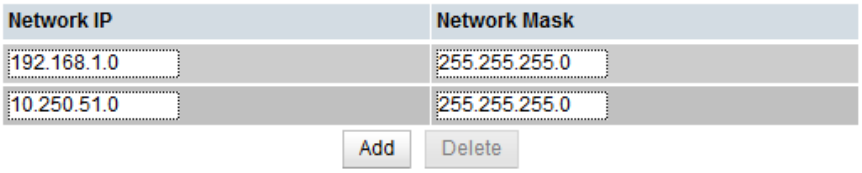
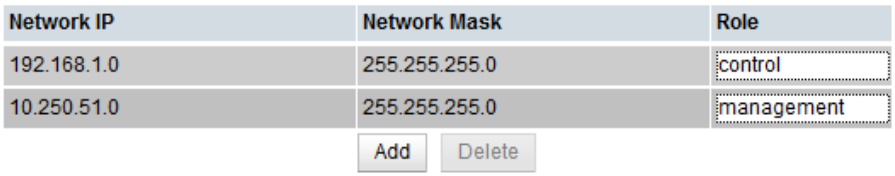
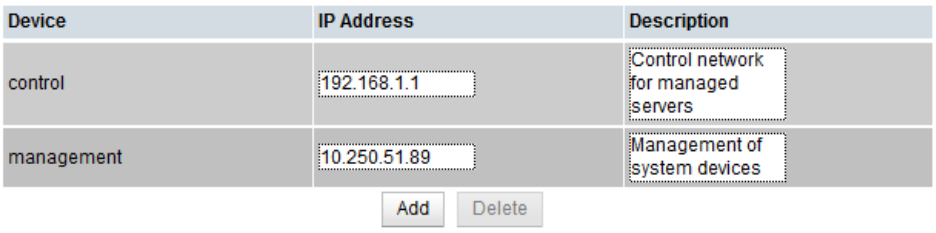
Procedure 5: Configure PMAC Application

Step	Procedure	Result
12. ☐	**PMAC GUI:** *Login to PMAC GUI*	Open web browser and enter: **http://<pmac_management_network_ip>** Login as **pmacadmin** user. 

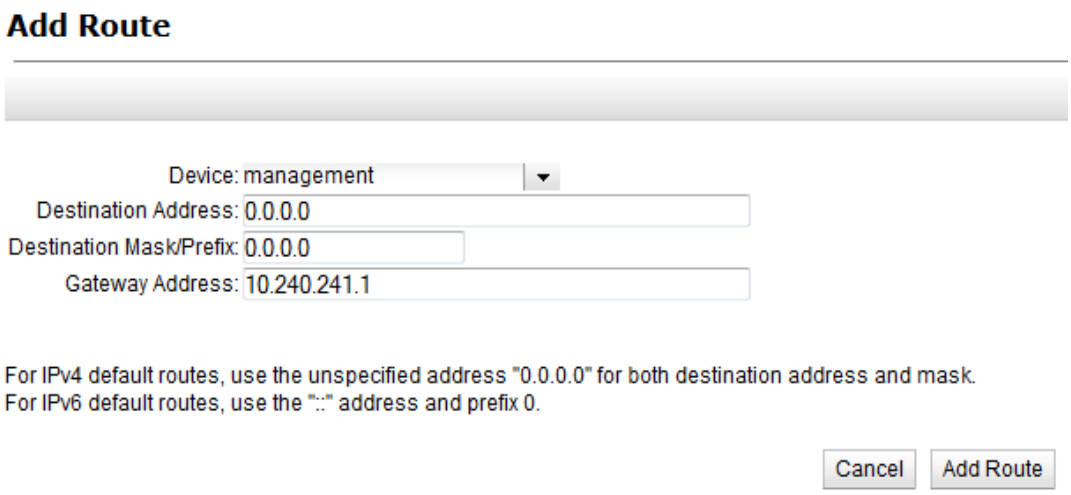
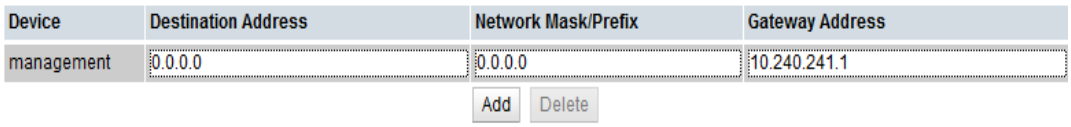
Procedure 5: Configure PMAC Application

Step	Procedure	Result
13. ☐	**PMAC GUI:** **Administration → PMAC Configuration → Feature Configuration** *Select a profile*	The first time that the PMAC GUI is opened, an initialization screen appears and will look similar to the screen shown below: Profiles File Name | Name | Comment | Version TVOE | PM&C TVOE Guest | Manage systems from a TVOE hosted PM&C | 6.0.0 [Initialize] Select the TVOE profile and click on **"Initialize"** button, the following screen will be displayed: Feature | description | Role | Enabled DEVICE.NETWORK.NETBOOT | Network device PXE initialization | management | ☑ DEVICE.NTP | PM&C as a time server | management | ☑ PMAC.MANAGED | Remote management of PM&C server | management | ☐ PMAC.REMOTE.BACKUP | Remote server for backup | management | ☐ PMAC.NETBACKUP | NetBackup client | management | ☐ [Add Role] [Apply] Set the Role to **management** for all features. Also make sure that the enable checkbox is checked for the following features only: 1. DEVICE.NETWORK.NETBOOT 2. DEVICE.NTP Click on **"Apply"** button to initialize the PMAC feature configuration. ***Note:*** *If you have missed the network initialization process, you will need to click on* ***"Apply"*** *button, then navigate to this GUI page* ***Administration → PMAC Configuration → Network Configuration*** *and click on the* ***"Reconfigure"*** *button.*

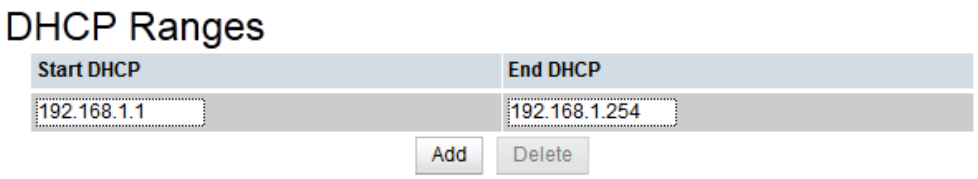
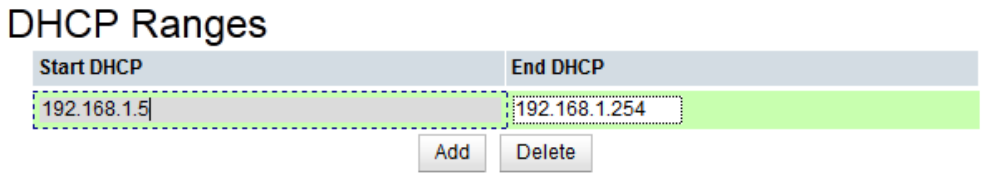
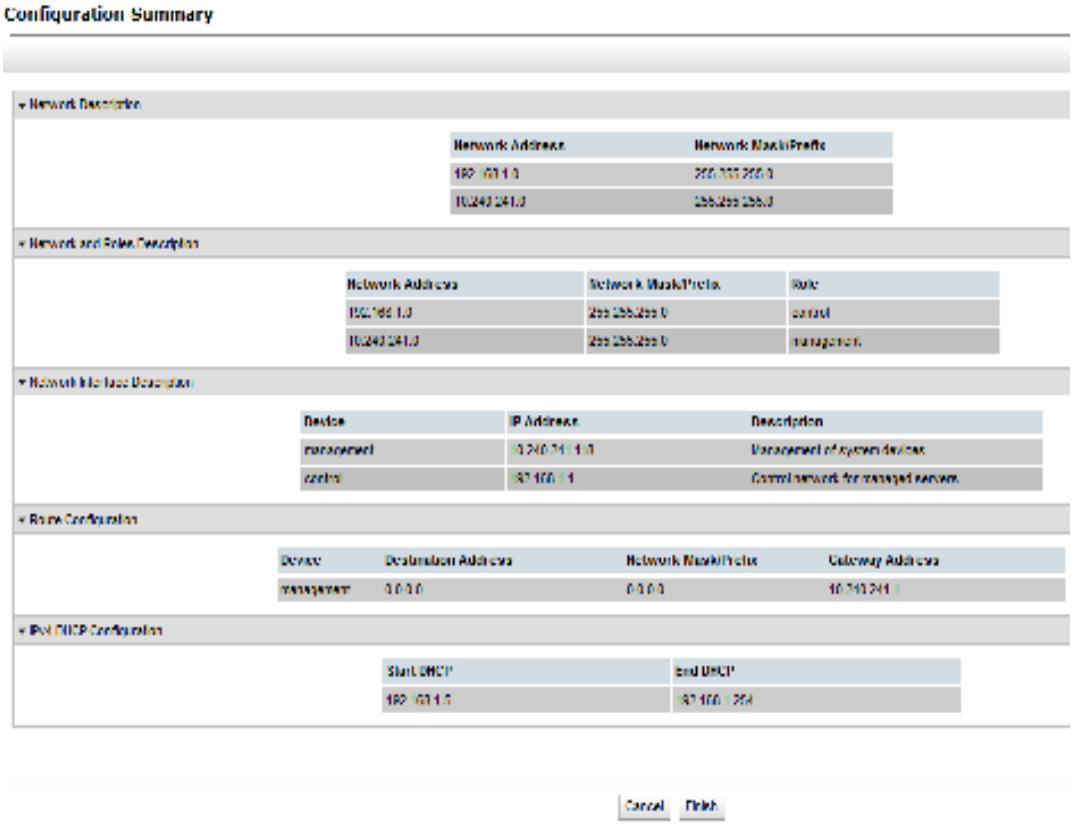
Procedure 5: Configure PMAC Application

Step	Procedure	Result
14. ☐	**PMAC GUI:** *Network Description*	You will see this default screen similar to:  Enter the Network IPs and Netmasks for the control (192.168.1.0) and Management Network (XMI Network). Click on **"Next"** button.
15. ☐	**PMAC GUI:** *Network Roles*	You will see this default screen similar to:  Verify the Roles and update if necessary by clinking on the Role field and selecting the correct role from the pull-down menu. The 192.168.1.0 network should be control and management network should have the XMI network ip address from the NAPD. Click on **"Next"** button.
16. ☐	**PMAC GUI:** *Network Interface*	You will see this default screen similar to:  Enter the XMI IP addresses of the PMAC in the management field and a control address of 192.168.1.1 in the control field. Click on **"Next"** button.

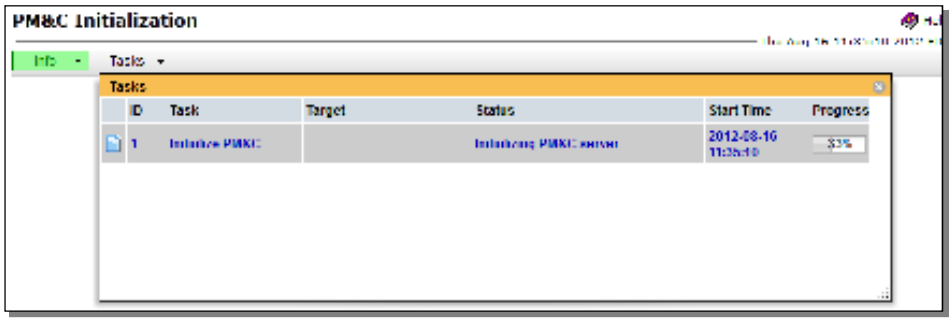
Procedure 5: Configure PMAC Application

Step	Procedure	Result
17. ☐	**PMAC GUI:** *Network Route*	You will see this default screen similar to: Click on the **Add** button to display the Add Route Screen:  Select Management in the Device Field. Enter 0.0.0.0 in the Destination Address Field. Enter 0.0.0.0 in the Destination Mask/Prefix Field. Enter the XMI Network Gateway Address in the Gateway Address Field. Click on the **Add Route** button to commit changes. Verify the route was entered correctly:  Click on **"Next"** button when done.

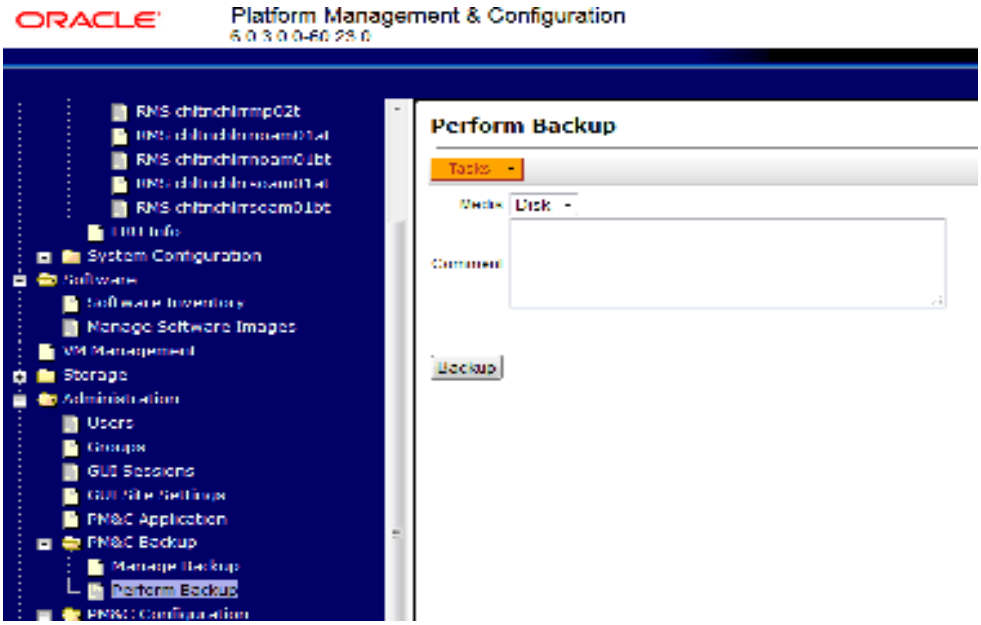
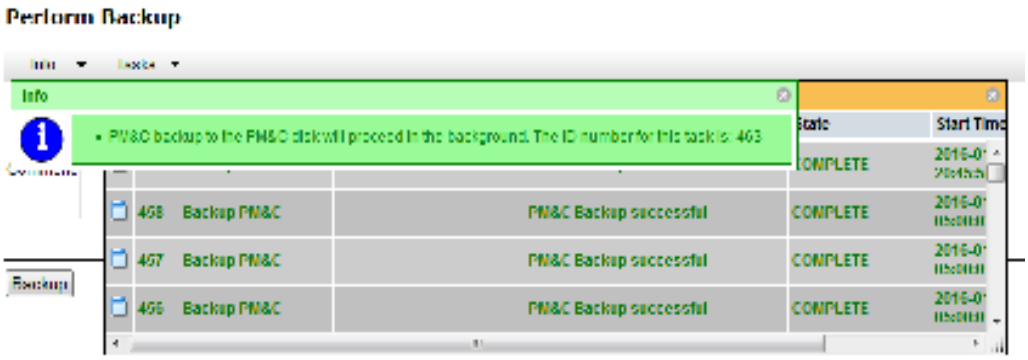
Procedure 5: Configure PMAC Application

Step	Procedure	Result
18. ☐	**PMAC GUI:** *DHCP Ranges*	You will see this default screen similar to:  Set the Starting address to 192.168.1.5 and the Ending address to 192.168.1.254.  Click on **"Next"** button when done.
19. ☐	**PMAC GUI:** *Summary Settings*	The following Configuration Summary screen will be displayed.  Verify the values are all correct then click the **"Finish"** button when done.

Procedure 5: Configure PMAC Application

Step	Procedure	Result
20. ☐	**PMAC GUI:** *Complete the configuration*	The following summary screen will be displayed, click on Tasks to view the Initialization Progress  Navigate to GUI page **"Main Menu → Task Monitoring"** for status of PMAC Initialization task. ID | Task | Target | Status | Running Time | Start Time | Progress 1 | Initialize PM&C | | PM&C initialized | 0:00:25 | 2012-08-16 11:35:10 | 100% Wait till the Progress bar turns green, that signifies that the PMAC Initialization was successful.
21. ☐	**PMAC GUI:** *Set the PMAC Application GUI Site Settings*	Navigate to GUI page: **Main Menu → Administration → GUI Site Settings** Set the "**Site name**" field to a descriptive name Set the "**Welcome Message**" field that is displayed upon login. Verify values, and click **"Update Settings"** button when done

Procedure 5: Configure PMAC Application

Step	Procedure	Result
22. ☐	**Virtual PMAC SSH:** *Perform PMAC application backup and save backup file*	Perform PMAC application backup from the PMAC GUI: Navigate to GUI page: **Main Menu → Administration → Perform Backup**  Click the **Backup** button to backup PMAC. Observe that the backup starts and is successful by monitoring the Info and Task screens:  ***Note:*** *The PMAC backup 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.* The PMAC backup must be moved to a remote server. Transfer (sftp, scp, rsync, or preferred utility) the PMAC backup file to an appropriate remote server.
23. ☐	**Optional:** PMAC on DR Management server	**Optional:** Repeat this procedure for the Disaster Recovery PMAC Server.
THIS PROCEDURE HAS BEEN COMPLETED		

6.5 Add Cabinet to PMAC System Inventory (All Sites)

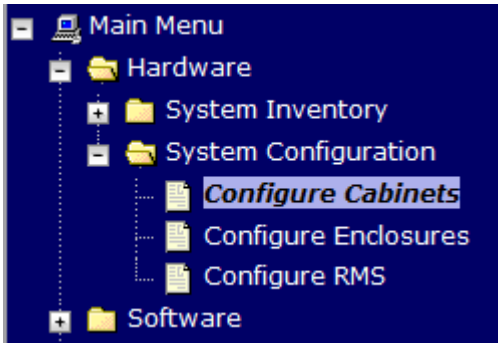
This procedure provides instructions to add a cabinet to the PMAC system inventory.

Requirements: Procedure 5: Configure PMAC Application has been completed.

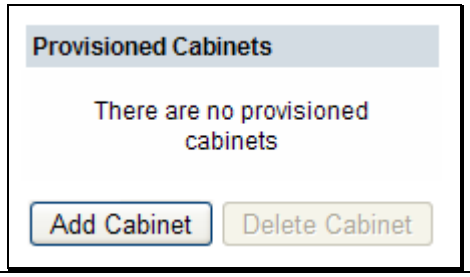
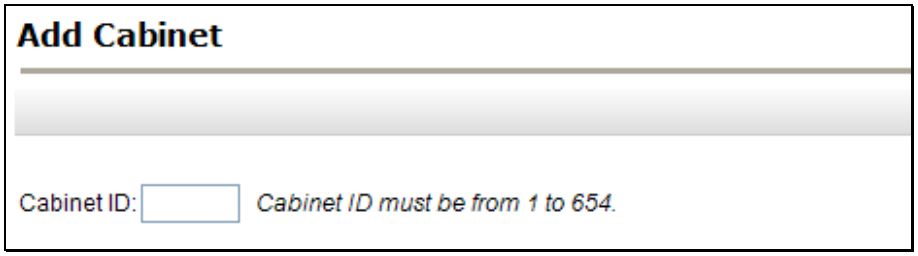
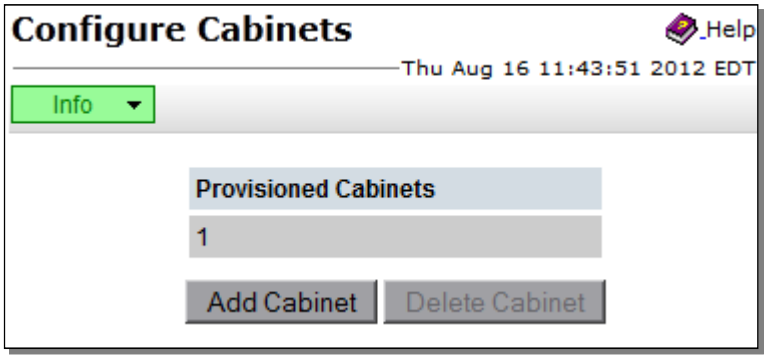
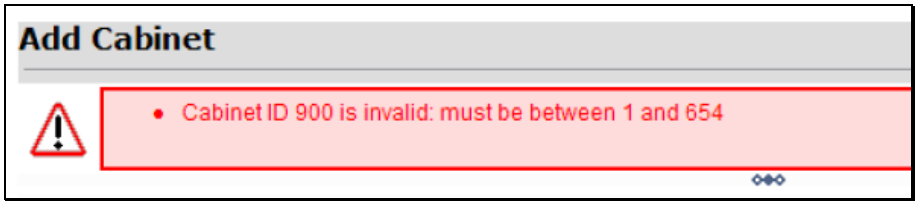
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

IF THIS PROCEDURE FAILS, CONTACT MY ORACLE SUPPORT AND ASK FOR ASSISTANCE.

Procedure 6: Add Cabinet to PMAC System Inventory

Step	Procedure	Result
1. ☐	**PMAC GUI:** *Login to PMAC GUI*	Open web browser and enter: **http://<pmac_management_network_ip>** Login as **pmacadmin** user. 
2. ☐	**PMAC GUI:** *Configure Cabinets*	Navigate to this GUI page: **Main Menu → Hardware → System Configuration → Configure Cabinets**. 

Procedure 6: Add Cabinet to PMAC System Inventory

Step	Procedure	Result
3. ☐	**PMAC GUI:** *Navigate to Configure Cabinet*	On the Configure Cabinets panel click on "**Add Cabinet"** button 
4. ☐	**PMAC GUI:** *Enter Cabinet ID*	Enter the value for CabinetID and press **Add Cabinet**. 
5. ☐	**PMAC GUI:** *Check Errors*	If no error is reported to the user, you will see the following:  Or you will see an error message: 
6. ☐	DR PMAC server	**Optional:** Repeat this procedure on the Disaster Recovery PMAC Server.
THIS PROCEDURE HAS BEEN COMPLETED		

6.6 Add Rack Mount Servers to PMAC System Inventory (All Sites)

This procedure provides instructions to add a Rack-Mount Server (RMS) to the PMAC system inventory. This procedure must be run for every physical server – not for every "logical" server that runs in a VM on a physical server.

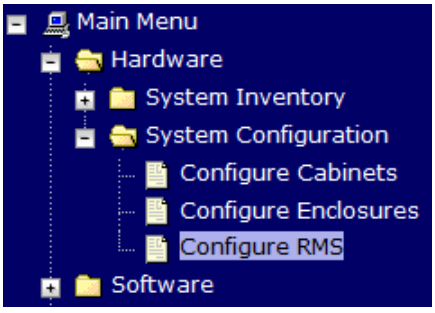
Requirements: Procedure 6: Add Cabinet to PMAC System Inventory has been completed.

Note: The installer must be knowledgeable of the network. If you make mistake, hit cancel and try again. The finish step may take longer time because it reconfigures the network and attempts to connect may fail.

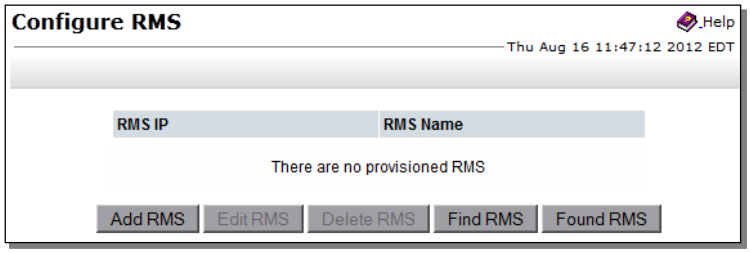
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

IF THIS PROCEDURE FAILS, CONTACT MY ORACLE SUPPORT AND ASK FOR ASSISTANCE.

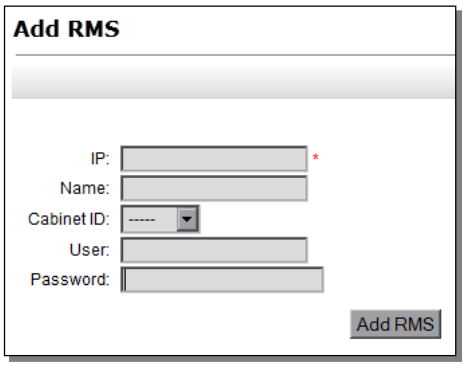
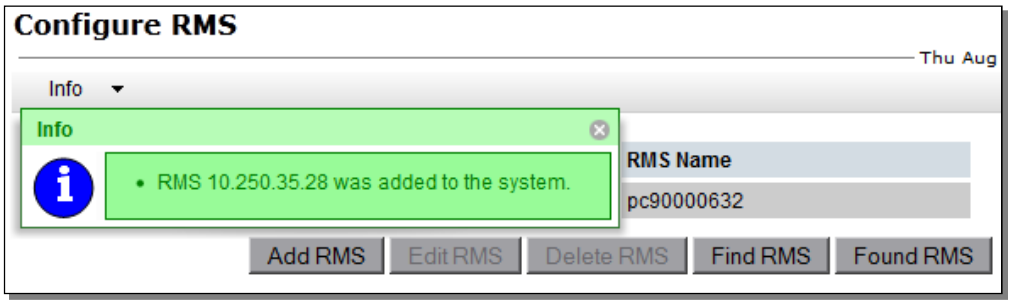
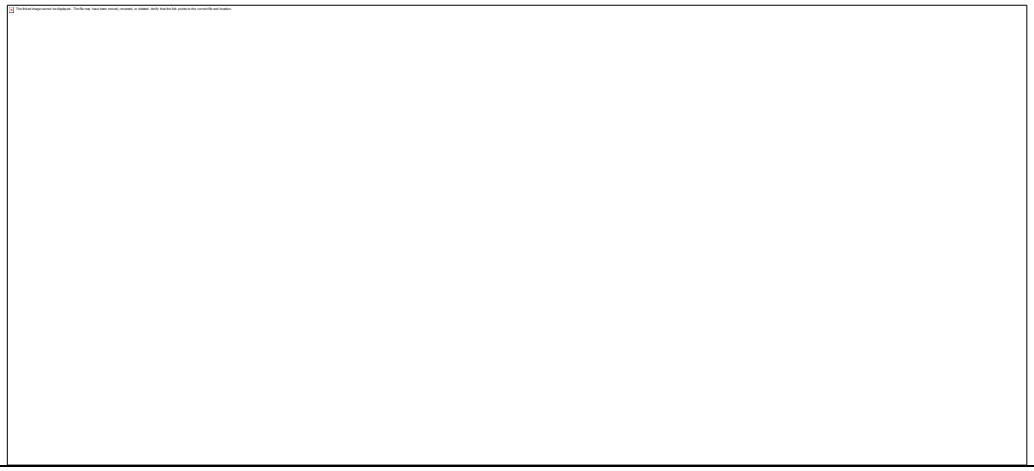
Procedure 7: Add Rack Mount Servers to PMAC System Inventory

Step	Procedure	Result
1. ☐	**PMAC GUI:** *Login to PMAC GUI*	Open web browser and enter: **http://<pmac_management_network_ip>** Login as **pmacadmin** user. 
2. ☐	**PMAC GUI:** Configure RMS	Navigate to this GUI page: **Main Menu → Hardware → System Configuration → Configure RMS** 

Procedure 7: Add Rack Mount Servers to PMAC System Inventory

Step	Procedure	Result
3. ☐	**PMAC GUI:** *Add RMS*	On the Configure Cabinets panel click on **Add RMS**  • Check-off the associated **Check Box** as the RMS server is added: **Primary Site:** ☐ RMS-1: _____ ☐ RMS-2: _____ ☐ RMS-3: _____ ☐ RMS-4: _____ ☐ RMS-5: _____ ☐ RMS-6: _____ ☐ RMS-7: _____ ☐ RMS-8: _____ ☐ RMS-9: _____ ☐ RMS-10: _____ **Disaster Recover Site: (Optional)** ☐ RMS-1: _____ ☐ RMS-2: _____ ☐ RMS-3: _____ ☐ RMS-4: _____ ☐ RMS-5: _____ ☐ RMS-6: _____ ☐ RMS-7: _____ ☐ RMS-8: _____ ☐ RMS-9: _____ ☐ RMS-10: _____

Procedure 7: Add Rack Mount Servers to PMAC System Inventory

Step	Procedure	Result
4. ☐	**PMAC GUI:** *Enter RMS Information*	Enter the RMS Name, management port (iLO) IP Address, iLO user, and iLO password of the rack mount server. Select the cabinet ID. Then press **Add RMS**. 
5. ☐	**PMAC GUI:** *Check Errors*	If no error is reported to the user, you will see the following:  Or you will see an error message: 
6. ☐	**Repeat Steps 2-5 of this procedure for each rack mount server to be added.**	

Procedure 7: Add Rack Mount Servers to PMAC System Inventory

Step	Procedure	Result
7. ☐	Add RMS on DR PMAC server	**Optional:** Repeat this procedure on the Disaster Recovery PMAC Server.
THIS PROCEDURE HAS BEEN COMPLETED		

6.7 Add Software Images to PMAC Server (All Sites)

This procedure will provide PMAC configuration using the web interface.

Needed material:

- TVOE 3.0.x Media (64-bit)
- TPD 7.0.x Media (64-bit)
- HLRR 4.1.x Application Media (64-bit)
- PMAC 6.x.x Media (64-bit)
- HP Misc Firmware 2.x.x (Min 2.2.9) ISO
- HP Hardware Firmware 2.x.x (Min 2.2.9) ISO
- <pmacftpusr_password> (Refer to TR006061 Password Dragon [10] for this value).

Requirements: Procedure 4. PMAC Deployment has been completed

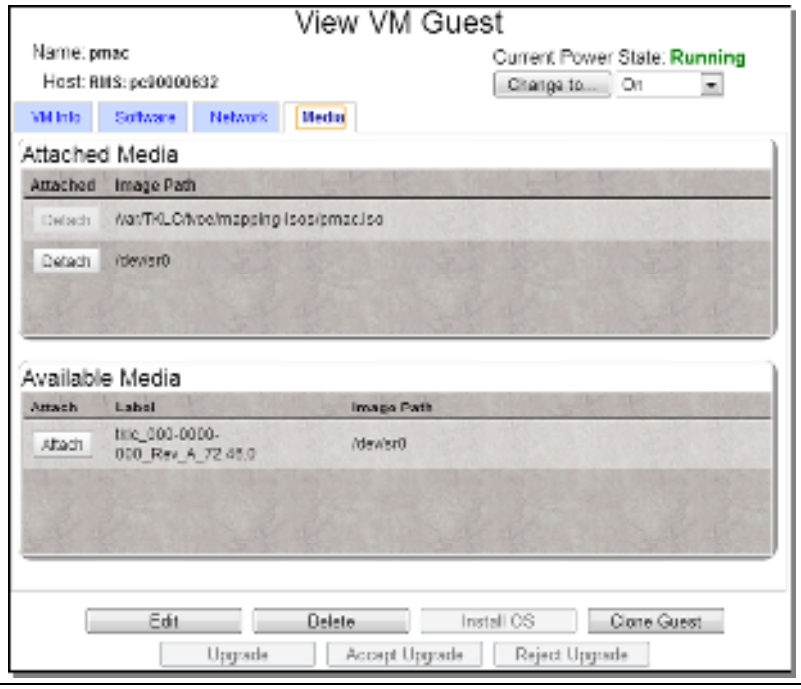
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

IF THIS PROCEDURE FAILS, CONTACT MY ORACLE SUPPORT AND ASK FOR ASSISTANCE.

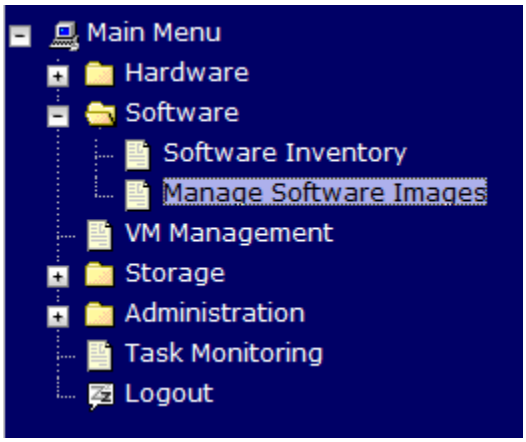
Procedure 8: Add Software Images to PMAC Server

Step	Procedure	Result
1. ☐	Load TVOE ISO image to PMAC server	There are three ways to make an TVOE ISO image available to PMAC: • Insert the CD containing TVOE ISO image into the removable media drive of the management (PMAC) server (DL360 Server Only). • Insert the USB containing TVOE ISO image into the management (PMAC) server (DL380 or DL360 Server. • Use **sftp** to transfer the iso image to the PMAC server in the **/var/TKLC/smac/image/isoimages/home/smacftpusr/** directory as pmacftpusr user: 1. Change into the directory where your TVOE ISO image is located 2. Using **sftp**, connect to the PMAC management server **$ sftp pmacftpusr@<PMAC_management_network_ip>** $ Password: <pmacftpusr_password> 3. **$ put <image>.iso** 4. After the image transfer is 100% complete, close the connection **$ quit**

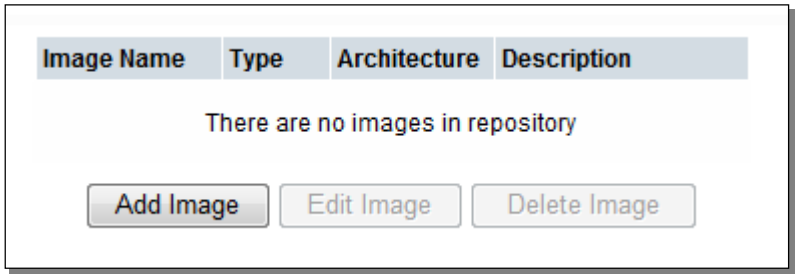
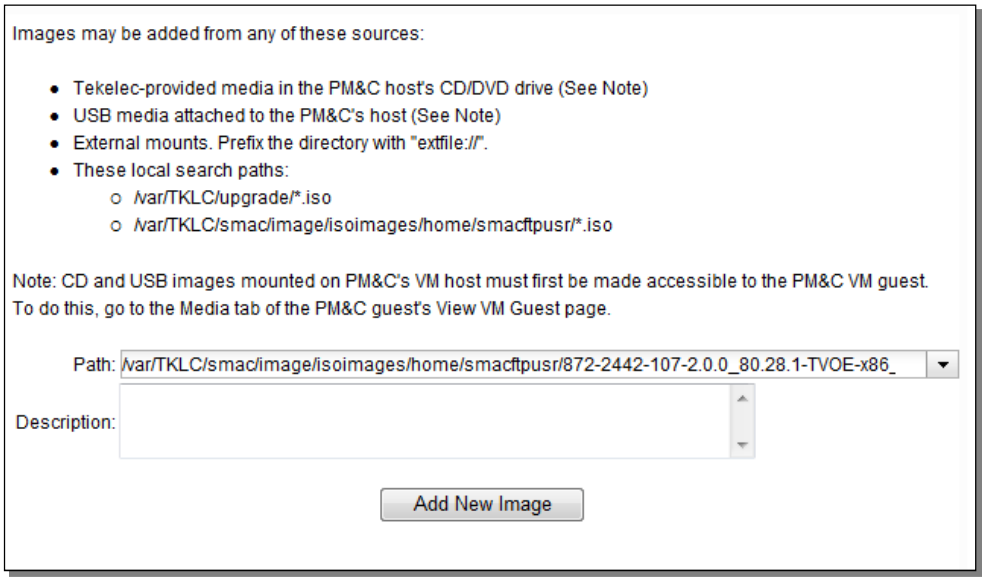
Procedure 8: Add Software Images to PMAC Server

Step	Procedure	Result
2. ☐	**PMAC GUI:** Login to PMAC GUI	Open web browser and enter: **http://<pmac_management_network_ip>** Login as **pmacadmin** user. 
3. ☐	**PMAC GUI:** Attach TVOE software image to the PMAC guest	If the image was transferred directly to the PMAC via sftp, then skip the rest of this step and continue with next step 4. If the image was supplied on a CD, continue with this step 3. 1. Navigate to this GUI page: **Main Menu → VM Management** 2. In the "**VM Entities**" list, select the PMAC guest. On the resulting "**View VM Guest**" page, select the "**Media**" tab. 3. Under the **Media** tab, find TVOE ISO image in the "**Available Media**" list, and click its "**Attach**" button. 4. After a pause, the image will appear in the "**Attached Media**" list. 

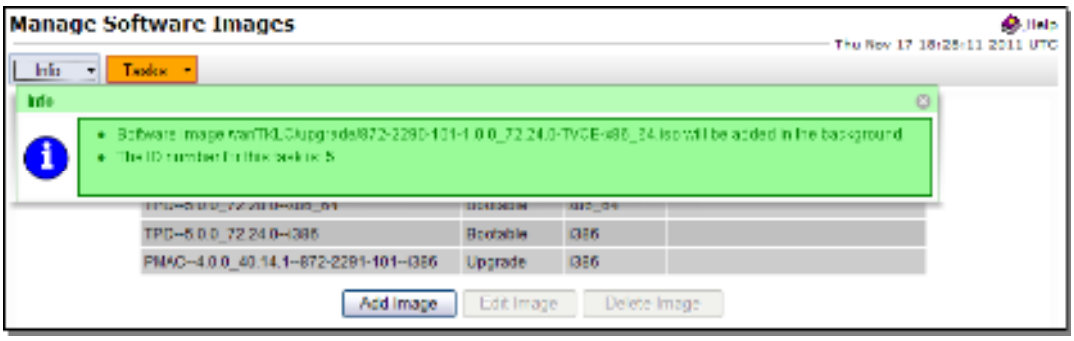
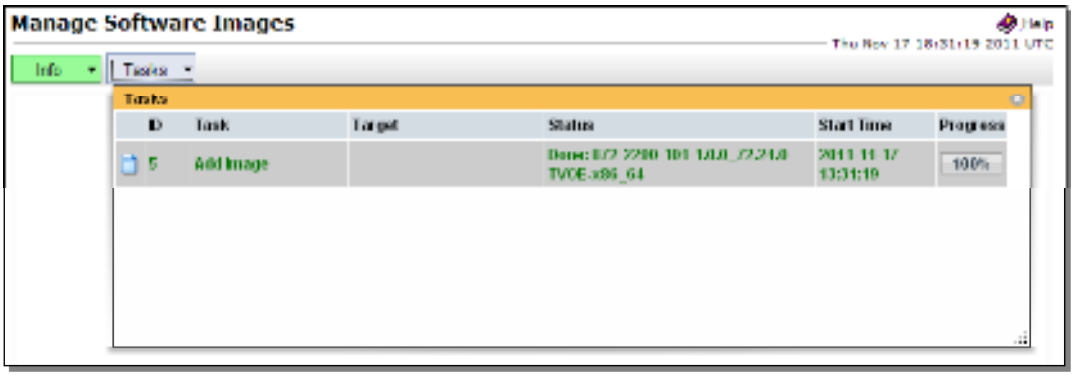
Procedure 8: Add Software Images to PMAC Server

Step	Procedure	Result
4. ☐	**PMAC GUI:** Navigate to Manage Software Images	Navigate to this GUI page: **Main Menu → Software → Manage Software Images** 

Procedure 8: Add Software Images to PMAC Server

Step	Procedure	Result
5. ☐	**PMAC GUI:** Add TVOE image	Press **"Add Image"** button. Use the dropdown to select the image.  If the image was supplied on a CD, then it will appear as a virtual device ("device://dev/sr…"). If the image was transferred to PMAC via sftp it will appear in the list as a local file "/var/TKLC/...".  Select the appropriate path, enter an appropriate image description and press **"Add New Image"** button.

Procedure 8: Add Software Images to PMAC Server

Step	Procedure	Result
6. ☐	**PMAC GUI:** Monitor the **Add Image** status	The **"Manage Software Images"** page is then re-displayed with a new background task entry in the table at the top of the page: 
7. ☐	**PMAC GUI:** Wait until the **Add Image** task finishes	1. When the task is complete, its text changes to green and its Progress column indicates "100%". 2. Check that the correct image name appears in the Status column: 
8. ☐	**PMAC GUI:** Detach the image from the PMAC guest	If the image was transferred directly to the PMAC via sftp, then skip the rest of this step and continue with step 9 (to load TPD image) or step 10 (to load HLRR image). If the image was supplied on a CD, continue with this step 8. 1. Return to the PMAC guest's "**Media**" tab as shown in Step 3, locate the image in the "**Attached Media**" list, and click its "**Detach**" button. 2. After a pause, the image will be removed from the "**Attached Media**" list. 3. This will release the virtual device for future use. 4. Remove the CD device from the Management Server.

Procedure 8: Add Software Images to PMAC Server

Step	Procedure	Result
9. ☐	**PMAC GUI:** Load TPD 7.0.x ISO image to PMAC server	To load TPD 7.0.x ISO image to the PMAC server by repeating steps 1 through 8 of this procedure.
10. ☐	**PMAC GUI:** Load HLRR 4.1.x ISO image to PMAC server	To load HLRR 4.1.x ISO image to the PMAC server by repeating steps 1 through 8 of this procedure.
11. ☐	**PMAC GUI:** Load PMAC 6.x.x ISO image to PMAC server	To load PMAC 6.x.x ISO to the PMAC server by repeating steps 1 through 8 of this procedure.
12. ☐	**PMAC GUI:** Load HP Misc Firmware 2.2.9 ISO image to PMAC server	To load HP Misc Firmware 2.x.x ISO to PMAC server by repeating steps 1 through 8 of this procedure.
13. ☐	**PMAC GUI:** Load HP Firmware 2.2.9 ISO image ISO image to PMAC server	Load HP Hardware Firmware 2.x.x ISO to PMAC server by repeating steps 1 through 8 of this procedure.
14. ☐	Add software to DR PMAC server	**Optional:** Repeat this procedure on the Disaster Recovery PMAC Server.
THIS PROCEDURE HAS BEEN COMPLETED		

6.8 Configure Cisco 4948E-F Aggregation Switches using netConfig (All Sites)

This procedure will configure 4948E-F frame switches with an appropriate IOS and configuration from PMAC on management server for use with the HP RMS setup as described in [4] Network Interconnect: HLR Router 4.1, TR007162.

Procedure Reference Tables: Steps within this procedure may refer to variable data indicated by text within "<>". Refer to this table for the proper value to insert depending on your system type.

If this procedure fails, contact My Oracle Support and ask for assistance.

Variable	Cisco 4948E-E
<Switch_IOS_image_file>	Fill in the appropriate value from [6] HP Solutions Firmware Upgrade Pack Release _____
<Switch_PROM_image_file>	Fill in the appropriate value from HP Solutions Firmware Upgrade Pack Release _____

NOTE: PMAC control network will be used for Switch management

Variable	Value
<switch_platform_username>	**platcfg**
<switch_platform_password>	Refer to TR006061 Password Dragon [10] for this value.
<switch_console_password>	**<Cisco Telnet Password>** Refer to TR006061 Password Dragon [10] for this value.
<switch_enable_password>	**<Cisco Enable Password>** Refer to TR006061 Password Dragon [10] for this value.
<management_server_mgmt_ip_address>	**192.168.1.4 (control IP of TVOE hosting PMAC)**
<pmac_mgmt_ip_address>	**192.168.1.1**
<switch_mgmt_id>	**1**
<switch1A_mgmt_ip_address>	**192.168.1.2**
<mgmt_Vlan_subnet_id>	**192.168.1.0**
<netmask>	**255.255.255.0**
<switch1B_mgmt_ip_address>	**192.168.1.3**
<switch_Internal_VLANS_list>	**1, 4**
<switch_mgmtVlan_id>	**1**
<management_server_mgmtInterface>	**control**
<management_server_iLO_ip>	Fill in the RMS hosting PMAC's iLO IP value
<serial console type>	**DL-380 uses USB = u DL 360 uses PCIe = c**

Variable	Value
<platcfg_password>	Refer to TR006061 Password Dragon [10] for this value.
<management_server_mgmtInterface>	**192.168.1.4**
<switch_backup_user>	admusr
<switch_backup_user_password>	Refer to TR006061 Password Dragon [10] for this value.

Needed materials:

- HP Solutions Firmware Upgrade Pack Release Notes, ref [6]
- HP Misc Firmware ISO specified in ref [6].
- Application specific documentation (documentation that is referred to this procedure)
- Template xml files are on the HLRR application ISO.

Requirements:

- **Procedure 2. Install TVOE on First RMS (PMAC Host)** has been completed
- **Procedure 4. PMAC Deployment** has been completed.
- **Procedure 5: Configure PMAC Application** 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, PLEASE CONTACT ORACLE'S CUSTOMER CARE CENTER FOR THE ASSISTANCE.

Procedure 9: Configure Cisco 4948E-F Frame Switches

Step	Procedure	Result
1. ☐	**TVOE Management Server:** Access the TVOE **Management Server** console.	Connect to the management server console using one of the access methods described in **Section 2.3.**
2. ☐	**TVOE Management Server :** Log into the server as the "**admusr**" user.	login as: **admusr** Password: ***<admusr_password>***
3. ☐	**TVOE Management Server:** Procedure pre-check - verify hardware type	Certain steps in this procedure require enabling and disabling Ethernet interfaces. This procedure supports DL360 and DL380 servers. The interfaces that are to be enabled and disabled are different for each server type. To determine the interface name, on the server, execute the following command: $ **sudo cat /proc/net/bonding/bond0 | grep Interface** Slave Interface: eth01 Slave Interface: eth02 Note the slave interface names of Ethernet interfaces to use in subsequent steps. If the output from the above command is not successful, refer back to the application documentation.

Procedure 9: Configure Cisco 4948E-F Frame Switches

Step	Procedure	Result
4. ☐	**TVOE Management Server:** Procedure pre-check – determine Platform version	On management server, determine the Platform version of the system by issuing the following command: **$ appRev** If the following is shown in the output, the Platform version is **7.0.x** : Install Time: Fri Dec 18 16:00:48 2015 Product Name: TVOE Product Release: 3.0.3.0.0_86.37.0 Base Distro Product: TPD Base Distro Release: 7.0.3.0.0_86.37.0 Base Distro ISO: TPD.install-7.0.3.0.0_86.37.0-OracleLinux6.7-x86_64.iso ISO name: TVOE-3.0.3.0.0_86.37.0-x86_64.iso OS: OracleLinux 6.7 If the command shows **Base Distro Release** version lower than 7.0 or fails to execute, stop this procedure and refer back to application procedures. It is possible the wrong version of TVOE/TPD is installed.
5. ☐	**TVOE Management Server:** Verify virtual PMAC is installed	PMAC is required to be installed prior to this procedure being attempted. Verify virtual PMAC was deployed on this management server by issuing the following command: $ **sudo virsh list --all** Id Name State ---------- 1 PMAC running 2 NOAM-A running If this command provides no output, it is likely that a virtual instance of PMAC is not installed. Refer to application documentation or contact Oracle's Customer Service.
6. ☐	**TVOE Management Server:** Login to the console of the virtual PMAC.	From TVOE management server, log into the console of the virtual PMAC instance found in step 5. **$ sudo virsh console <pmac_name>** 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: **admusr** Password: Last login: Fri May 25 16:39:04 on ttyS4 If this command fails, it is likely that a virtual instance of PMAC is not installed. Refer to application documentation or contact Oracle's Customer Service.

Procedure 9: Configure Cisco 4948E-F Frame Switches

Step	Procedure	Result
7. ☐	**Virtual PMAC:** Verify PMAC release version	Verify the PMAC release version. **$ appRev** If the following is shown in the output, the PMAC version is 6.0: Install Time: Fri Dec 18 19:47:57 2015 Product Name: PM&C Product Release: 6.0.3.0.0_60.23.0 Base Distro Product: TPD Base Distro Release: 7.0.3.0.0_86.37.0 Base Distro ISO: TPD.install-7.0.3.0.0_86.37.0-OracleLinux6.7-x86_64.iso ISO name: PM&C-6.0.3.0.0_60.23.0-x86_64.iso OS: OracleLinux 6.7 If the output does not contain "Product Name: PM&C" or does not contain a PM&C version of 6.0 or higher, then stop this procedure and refer back to the application instructions or contact Oracle's Customer Service.
8. ☐	**Virtual PMAC:** Set up netConfig repository with necessary ssh information.	$ **sudo /usr/TKLC/plat/bin/netConfig --repo addService name=ssh_service** Service type? (tftp, ssh, conserver, oa) **ssh** Service host? **192.168.1.1** Enter an option name <q to cancel>: **user** Enter the value for user: **admusr** Enter an option name <q to cancel>: **password** Enter the value for password: **<switch_backup_user_password>** Verify Password: **<switch_backup_user_password>** Enter an option name <q to cancel>: **q** Add service for ssh_service successful
9. ☐	**Virtual PMAC:** Use the following command and inspect the output, which will be similar to the one shown.	$ **sudo /usr/TKLC/plat/bin/netConfig --repo showService name=ssh_service** Service Name: ssh_service Type: ssh Host: 192.168.1.1 Options: password: C20F7D639AE7E7 user: admusr

Procedure 9: Configure Cisco 4948E-F Frame Switches

Step	Procedure	Result
10. ☐	**Virtual PMAC:** 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. $ **sudo /usr/TKLC/plat/bin/netConfig --repo addService name=tftp_service** Service type? (tftp, ssh, conserver, oa) **tftp** Service host? **192.168.1.1** Enter an option name (q to cancel): **dir** Enter a value for user dir: **/var/TKLC/smac/image/** Enter an option name(q to cancel): **q** Add service for tftp_service successful
11. ☐	**Virtual PMAC:** Check that you entered the tftp information correctly.	To check that you entered the tftp information correctly, use the following command: $ **sudo /usr/TKLC/plat/bin/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: 192.168.1.1 Options: dir: /var/TKLC/smac/image

Procedure 9: Configure Cisco 4948E-F Frame Switches

Step	Procedure	Result
12. ☐	**Virtual PMAC:** Run conserver setup command	**sudo /usr/TKLC/plat/bin/conserverSetup –<serial console type> -s <tvoe_control_server_ip>** **Note:** Serial Console Type Options: Quad Serial (DL360) = -c, USB (DL380) = -u An Example: $ **sudo /usr/TKLC/plat/bin/conserverSetup -u -s 192.168.1.4** Enter your platcfg username, followed by [ENTER]:**platcfg** Enter your platcfg password, followed by [ENTER]:**<platcfg_password>** Checking Platform Revision for local TPD installation... The local machine is running: Product Name: PM&C Base Distro Release: 7.0.3.0.0_86.1.0 Checking Platform Revision for remote TPD installation... The remote machine is running: Product Name: TVOE Base Distro Release: 7.0.3.0.0_86.2.0 Configuring switch 'switch1A_console' console server...Configured. Configuring switch 'switch1B_console' console server...Configured. Configuring iptables for port(s) 782...Configured. Configuring iptables for port(s) 1024:65535...Configured. Configuring console repository service... Repo entry for "console_service" already exists; deleting entry for: Service Name: console_service Type: conserver Host: 192.168.1.4 ...Configured. Slave interfaces for bond0: bond0 interface: eth01 bond0 interface: eth02 • If this command fails, contact My Oracle Support (MOS). • Verify the output of the script. • Verify that your Product Release is based on Tekelec Platform 7.0 (versions 7.0.x.x.x_x.x.x). • Note the slave interface names of bond interfaces (<ethernet_interface_1> and <ethernet_interface_2>) for use in subsequent steps.

Procedure 9: Configure Cisco 4948E-F Frame Switches

Step	Procedure	Result
13. ☐	**Virtual PMAC Server:** Mount the HP Misc Firmware ISO	For this step, be sure to use the correct IOS version specified by the [6] HP Solutions Firmware Upgrade Pack Release Notes, Release 2.x.x (Min 2.2.9) for the Cisco 4948E-F switches. From a PMAC console window, ssh to the TVOE management server ip address with the command: **ssh admusr@192.168.1.4** Login in to the TVOE host with the admusr password. Insert the HP Misc Firmware USB into a slot on the primary NOAM-A (management) server. And make the firmware available to the TVOE host with the commands: **$ sudo /bin/ls /media/*/*.iso** Example output: /media/sdb1/ FW2_MISC-2.2.9.0.0_10.44.0.iso **Note:** The HP Misc Firmware USB device is immediately added to the list of media devices once it is inserted into a USB slot on the TVOE Host server. **Note:** Note the device directory name under the media directory. This could be sdb1, sdc1, sdd1, or sde1, depending on the USB slot into which the media was inserted. Mount the HP Misc Firmware ISO with the following command: **sudo /bin/mount -o loop /media/<device directory>/<ISO Name>.iso /mnt/upgrade** For example: **$ sudo /bin/mount -o loop /media/sdb1/FW2_MISC-2.2.9.0.0_10.44.0.iso /mnt/upgrade**
14. ☐	**Virtual PMAC Server:** Copy Cisco 4948E-F Switch firmware to the PMAC's tftp_directory	For this step, be sure to use the correct IOS version specified by [6] HP Solutions Firmware Upgrade Pack Release Notes, Release 2.x.x (Min 2.2.9) for the Cisco 4948E-F switches. Exit the TVOE management server to return to the PMAC command console. Copy the firmware to PMAC's tftp_service directory and change the permissions of the file: **sudo /usr/bin/scp –r admusr@192.168.1.4:/mnt/upgrade/files/<4948E_ISO_image_filename> /var/TKLC/smac/image/** For example: **sudo /usr/bin/scp –r admusr@192.168.1.4:/mnt/upgrade/files/cat4500e-entservicesk9-mz.122-54.WO.bin /var/TKLC/smac/image/** Change the file permissions: **$ sudo /bin/chmod 644 /var/TKLC/smac/image/<4948E_ISO_image_filename >** For example: **$ sudo /bin/chmod 644 /var/TKLC/smac/image/cat4500e-entservicesk9-mz.122-54.WO.bin**

Procedure 9: Configure Cisco 4948E-F Frame Switches

Step	Procedure	Result
15. ☐	**TVOE Management Server**	From a PMAC console window, ssh to the TVOE management server ip address with the command: **ssh admusr@192.168.1.4** Login in to the TVOE host with the admusr password. Unmount the HP Misc Firmware USB with the commands: **cd /** **sudo umount /mnt/upgrade** Exit the TVOE management server to return to the PMAC command console. Remove the HP Misc Firmware USB from the NOAM-A management server.

Procedure 9: Configure Cisco 4948E-F Frame Switches

Step	Procedure	Result
16. ☐	**Virtual PMAC:** 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. **Note:** The model should be a Cisco 4948E-F. If you do not know, stop now and contact Oracle's Customer Care Center. $ **sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=switch1A --reuseCredentials** Device Vendor? **Cisco** Device Model? **4948E-F** What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management? **192.168.1.2/24** Is the management interface a port or a vlan? [vlan]: **[Enter]** What is the VLAN ID of the management VLAN? [2]: **1** What is the name of the management VLAN? [management]: **default** What switchport connects to the management server? [GE40]: **[Enter]** What is the switchport mode (access|trunk) for the management server port? [trunk]: **[Enter]** What are the allowed vlans for the management server port? [1,2]: **1,4** Enter the name of the firmware file [cat4500e-entservicesk9-mz.122-54.WO.bin]: <**IOS_filename**> Firmware file to be used in upgrade: **<IOS_filename>** Enter the name of the upgrade file transfer service: **tftp_service** File transfer service to be used in upgrade: **tftp_service** Should the init oob adapter be added (y/n)? **y** Adding consoleInit protocol for <switch_hostname> using oob... What is the name of the service used for OOB access? **console_service** What is the name of the console for OOB access? **switch1A_console** What is the platform access username? **platcfg** What is the device console password? **<switch_console_password>** Verify password: **<switch_console_password>** What is the platform user password? **<switch_platform_password>** Verify password: **<switch_platform_password>** What is the device privileged mode password? **<switch_enable_password>** Verify password: **<switch_enable_password>** Should the live network adapter be added (y/n)? **y** Adding cli protocol for switch1A using network... Network device access already set: **192.168.1.2** 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.

Procedure 9: Configure Cisco 4948E-F Frame Switches

Step	Procedure	Result
17. ☐	**Virtual PMAC:** Verify switch 1A configuration.	**sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=switch1A** **Example:** [admusr@chltnchlrrPMAC01 ~]$ **sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=switch1A** Device: switch1A Vendor: Cisco Model: 4948E-F FW Ver: (cat4500e-ENTSERVICESK9-M), Version 12.2(54)WO FW Filename: cat4500e-entservicesk9-mz.122-54.WO.bin FW Service: tftp_service Initialization Management Options mgmtIP: 192.168.1.2/24 mgmtInt: vlan mgmtVlan: 1 mgmtVlanName: default interface: GE40 mode: trunk allowedVlans: 1,4 Access: Network: 192.168.1.2 Access: OOB: Service: console_service Console: switch1A_console Init Protocol Configured Live Protocol Configured

Procedure 9: Configure Cisco 4948E-F Frame Switches

Step	Procedure	Result
18. ☐	**Virtual PMAC:** 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. **Note:** The model should be Cisco 4948E-F. If you do not know, stop now and contact Oracle's Customer Care Center. $ **sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=switch1B --reuseCredentials** Device Vendor? **Cisco** Device Model? **4948E-F** What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management? **192.168.1.3/24** Is the management interface a port or a vlan? [vlan]: **[Enter]** What is the VLAN ID of the management VLAN? [2]: **1** What is the name of the management VLAN? [management]: **default** What switchport connects to the management server? [GE40]: **[Enter]** What is the switchport mode (access|trunk) for the management server port? [trunk]: **[Enter]** What are the allowed vlans for the management server port? [1,2]: **1,4** Enter the name of the firmware file [cat4500e-entservicesk9-mz.122-54.WO.bin]: <**IOS_filename**> Firmware file to be used in upgrade: **<IOS_filename>** Enter the name of the upgrade file transfer service: **tftp_service** File transfer service to be used in upgrade: **tftp_service** Should the init oob adapter be added (y/n)? **y** Adding consoleInit protocol for <switch_hostname> using oob... What is the name of the service used for OOB access? **console_service** What is the name of the console for OOB access? **switch1B_console** What is the platform access username? **platcfg** What is the device console password? **<switch_console_password>** Verify password: **<switch_console_password>** What is the platform user password? **<switch_platform_password>** Verify password: **<switch_platform_password>** What is the device privileged mode password? **<switch_enable_password>** Verify password: **<switch_enable_password>** Should the live network adapter be added (y/n)? **y** Adding cli protocol for switch1B using network... Network device access already set: **192.168.1.3** 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 switch1A successfully added.

Procedure 9: Configure Cisco 4948E-F Frame Switches

Step	Procedure	Result
19. ☐	**Virtual PMAC:** Verify switch 1B configuration.	**sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=switch1B** **Example:** [admusr@chltnchlrrpmac01 ~]$ **sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=switch1B** Device: switch1B Vendor: Cisco Model: 4948E-F FW Ver: (cat4500e-ENTSERVICESK9-M), Version 12.2(54)WO FW Filename: cat4500e-entservicesk9-mz.122-54.WO.bin FW Service: tftp_service Initialization Management Options mgmtIP: 192.168.1.3/24 mgmtInt: vlan mgmtVlan: 1 mgmtVlanName: default interface: GE40 mode: trunk allowedVlans: 1,4 Access: Network: 192.168.1.3/24 Access: OOB: Service: console_service Console: switch1B_console Init Protocol Configured Live Protocol Configured

Procedure 9: Configure Cisco 4948E-F Frame Switches

Step	Procedure	Result
20. ☐	**Virtual PMAC:** Copy switch configuration files from HLRR application ISO to the PMAC server	Copy the 4948E-F switch configuration xml files from the HLRR application ISO to the PMAC server. **Note:** this step assumes that you have copied the HLRR application ISO into the PMAC software repository as directed in **Procedure 8: Add Software Images to PMAC Server**. Create temporary mount point: **$ sudo mkdir -p /mnt/disk** Mount the HLRR application ISO: **$ sudo mount -o loop /var/TKLC/smac/image/repository/<hlrr_application_iso> /mnt/disk** For example: **$ sudo mount -o loop /var/TKLC/smac/image/repository/EXHR-4.1.0_41.2.0-x86_64.iso /mnt/disk** Create temporary directory, change file permissions and CD into it: **$ sudo mkdir /tmp/temp** **$ sudo chmod 777 /tmp/temp** **$ cd /tmp/temp** Access the application RPM: **$ rpm2cpio /mnt/disk/Packages/TKLCexhr-4.1.0*.rpm | cpio -idmv** [output not shown] **$ cd /tmp/temp/usr/TKLC/exhr/xml/** Verify the xml files are in the directory: **$ ls -al** -r-xr-xr-x 1 root root 725 Dec 21 23:43 HLRR_NOAMP_NE.xml -r-xr-xr-x 1 root root 724 Dec 21 23:43 HLRR_SOAM_NE.xml -r-xr-xr-x 1 root root 4803 Dec 21 23:43 switch1A_HLRR_4948E_E-F_init.xml -r-xr-xr-x 1 root root 4803 Dec 21 23:43 switch1B_HLRR_4948E_E-F_init.xml -r-xr-xr-x 1 root root 10857 Dec 21 23:43 switch1A_HLRR_4948E_E-F_configure.xml -r-xr-xr-x 1 root root 10857 Dec 21 23:43 switch1B_HLRR_4948E_E-F_configure.xml

Procedure 9: Configure Cisco 4948E-F Frame Switches

Step	Procedure	Result
21. ☐	**Virtual PMAC:** Copy switch configuration and NE files from HLRR application ISO to the PMAC server and the change file permissions	Copy the xml files to PMAC's /usr/TKLC/exhr/xml/ directory: **$ sudo cp -p *.xml /usr/TKLC/smac/etc/switch/xml/** **Note:** If directory **/usr/TKLC/smac/etc/switch/xml** doesn't exist on the PMAC server, create it: **$ sudo mkdir -p /usr/TKLC/smac/etc/switch/xml** **$ sudo chmod 777 /usr/TKLC/smac/etc/switch/xml** Verify all the xml files were copied: **$ ls -al /usr/TKLC/smac/etc/switch/xml/** -r-xr-x--- 1 root root 725 Jan 29 16:02 HLRR_NOAMP_NE.xml -r-xr-x--- 1 root root 724 Jan 29 16:02 HLRR_SOAM_NE.xml -rw-rw-rw- 1 admusr admgrp 13944 Jan 28 18:47 switch1A_HLRR_4948E_E-F_configure.xml -rw-rw-rw- 1 admusr admgrp 1124 Jan 27 15:07 switch1A_HLRR_4948E_E-F_init.xml -rw-rw-rw- 1 admusr admgrp 13953 Jan 28 18:47 switch1B_HLRR_4948E_E-F_configure.xml -rw-rw-rw- 1 admusr admgrp 1124 Jan 27 16:06 switch1B_HLRR_4948E_E-F_init.xml Change file permissions to read/write using the following commands: **$ sudo chmod 666 /usr/TKLC/smac/etc/switch/xml/*.xml** Verify all the xml files permission were changed to read/write: **$ ls -al /usr/TKLC/smac/etc/switch/xml/** -rw-rw-rw- 1 root root 725 Jan 29 16:02 HLRR_NOAMP_NE.xml -rw-rw-rw- 1 root root 724 Jan 29 16:02 HLRR_SOAM_NE.xml -rw-rw-rw- 1 admusr admgrp 13944 Jan 28 18:47 switch1A_HLRR_4948E_E-F_configure.xml -rw-rw-rw- 1 admusr admgrp 1124 Jan 27 15:07 switch1A_HLRR_4948E_E-F_init.xml -rw-rw-rw- 1 admusr admgrp 13953 Jan 28 18:47 switch1B_HLRR_4948E_E-F_configure.xml -rw-rw-rw- 1 admusr admgrp 1124 Jan 27 16:06 switch1B_HLRR_4948E_E-F_init.xml Change out of the directory: **$ cd /** Remove the temporary directory: **$ sudo rm -rf /tmp/temp** Unmount the application ISO: **$ sudo umount /mnt/disk**

Procedure 9: Configure Cisco 4948E-F Frame Switches

Step	Procedure	Result
22. ☐	**Virtual PMAC:** Verify the 4928E-F's IOS image is on the system in the tftp_directory.	Verify the 4928E-F's IOS image is on the system in the tftp_directory and that the file permissions at set to read/write, read, read (644). **$ sudo /bin/ls -al /var/TKLC/smac/image/** [admusr@chltnchlrrpmac01 xml]$ sudo /bin/ls -al /var/TKLC/smac/image/ -rw-r--r-- admusr admgrp 25948874 Jul 2 2015 **cat4500e-entservicesk9-mz.122-54.WO.bin** If the file exists and it has the correct file permission, then continue to the next step. If the file does not exist or the file permissions are not correct, repeat steps 13 and 14 of this procedure to copy the file from the firmware media and set its permissions.
23. ☐	**Virtual PMAC:** Start the control network TFTP Process.	Start the control network TFTP Process with the command: **sudo /usr/sbin/in.tftpd -l -s --address=192.168.1.1 /var/TKLC/smac/image/** Verify that the process is running: **ps -ef | grep tftp** root 13433 1 0 Jan28 00:00:00 /usr/sbin/in.tftpd -l -s --address=192.168.1.1 /var/TKLC/smac/image/
24. ☐	**TVOE Management Server:** Manipulate host server physical interfaces.	Exit from the virtual PMAC console, by entering **< ctrl-] >** and you will be returned to the TVOE management server prompt. Ensure that the interface of the server connected to switch1A is the only interface up by performing the following commands: $ **sudo /sbin/ifup eth01** $ **sudo /sbin/ifdown eth02** **$ sudo netAdm set --type=Bridge --name=control --updateMAC**
25. ☐	**TVOE Management Server:** Login to the console of the virtual PMAC.	From TVOE management server, log into the console of the virtual PMAC instance from step 5. **$ sudo virsh console <pmac_name>** 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: **admusr** Password: Last login: Fri May 25 16:39:04 on ttyS4 If this command fails, it is likely that a virtual instance of PMAC is not installed. Refer to application documentation or contact Oracle's Customer Service.

Procedure 9: Configure Cisco 4948E-F Frame Switches

Step	Procedure	Result
26. ☐	**Virtual PMAC:** ***(switch console session)*:** Determine if switch1A PROM upgrade is required.	Determine if switch1A PROM upgrade is required. **Note:** ROM & PROM are intended to have the same meaning for this procedure Connect to switch1A, check the PROM version. Connect serially to switch1A by issuing the following command. $ **sudo /usr/bin/console -M 192.168.1.4 -l platcfg switch1A_console** Enter platcfg@pmac5000101's password: **<platcfg_password>** [Enter `^Ec?' for help] Press Enter Password: (**should be none)** Switch> **show version | include ROM** ROM: 12.2(44r)SG11 System returned to ROM by reload **Note:** If the console command fails, contact *My Oracle Support (MOS)*. Note the IOS image & ROM version for comparison in a following step. Check the version from the previous command against the version from [6] HP Solutions Firmware Upgrade Pack Release Notes, Release 2.x.x (Min 2.2.9). If the versions are different, perform the procedure in *Appendix J Upgrade Cisco 4948 PROM* to upgrade the PROM for switch1A.
27. ☐	**Virtual PMAC:** ***(switch console session)*:** Exit the switch console to the PMAC console.	Exit from the switch console by entering**<ctrl-e><c><.>** and you will be returned to the PMAC server prompt.
28. ☐	**Virtual PMAC:** Prepare switch1A to be initialized and configured.	Prepare switch1A to be initialized and configured. **$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A setFactoryDefault** Wait 10 minutes for the switch to complete its reboot process.
29. ☐	**Virtual PMAC:** Initialize switch1A	Initialize switch1A by issuing the following command: $ **sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch/xml/switch1A_HLRR_4948E_E-F_init.xml** Processing file: /usr/TKLC/smac/etc/switch/xml/ switch1A_HLRR_4948E_E-F_init.xml **Note:** This step takes about 5-10 minutes to complete. Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact *My Oracle Support (MOS)*. A successful completion of netConfig will return the user to the $ prompt.

Procedure 9: Configure Cisco 4948E-F Frame Switches

Step	Procedure	Result
30. ☐	**Virtual PMAC:** Retrieve switch1A hostname.	Use netConfig to get the hostname of the switch, to verify that the switch was initialized properly, and to verify that netConfig can connect to the switch. $ **sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getHostname** Hostname: switch1A
31. ☐	**Virtual PMAC:** Verify the switch is using the proper IOS image.	Verify the switch is using the proper IOS image that was copied into the tftp_service directory. Issue the following commands to verify the IOS release on switch1A: $ **sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getFirmware** Version: 122-54.XO License: entservicesk9 Flash: cat4500e-entservicesk9-mz.122-54.WO.bin
32. ☐	**Virtual PMAC:** Configure switch 1A.	Configure switch 1A by issuing the following commands: $ **sudo /usr/TKLC/plat/bin/netConfig** **--file=/usr/TKLC/smac/etc/switch/xml/switch1A_HLRR_4948E_E-F_configure.xml** Processing file: /usr/TKLC/smac/etc/switch/xml/ switch1A_HLRR_4948E_E-F_configure.xml **Note:** This may take 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 *My Oracle Support (MOS)*. A successful completion of netConfig will return the user to the $ prompt.
33. ☐	**TVOE Management Server:**	Exit from the virtual PMAC console, by entering **< ctrl-] >** and you will be returned to the TVOE management server prompt. Ensure that the interface of the server connected to switch1B is the only interface up by performing the following commands: $ **sudo /sbin/ifup eth02** $ **sudo /sbin/ifdown eth01** **$ sudo netAdm set --type=Bridge --name=control --updateMAC**

Procedure 9: Configure Cisco 4948E-F Frame Switches

Step	Procedure	Result
34. ☐	**TVOE Management Server:** Login to the console of the virtual PMAC.	From TVOE management server, log into the console of the virtual PMAC instance from step 5. **$ sudo virsh console <PMAC_name>** 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: **admusr** Password: Last login: Fri May 25 16:39:04 on ttyS4 If this command fails, it is likely that a virtual instance of PMAC is not installed. Refer to application documentation or contact *My Oracle Support (MOS)*.
35. ☐	**Virtual PMAC:** Determine if switch1B PROM upgrade is required.	Determine if switch1B PROM upgrade is required. **Note:** ROM & PROM are intended to have the same meaning for this procedure Connect to switch1A, check the PROM version. Connect serially to switch1A by issuing the following command. $ **sudo /usr/bin/console -M 192.168.1.4 -l platcfg switch1B_console** Enter platcfg@pmac5000101's password: **<platcfg_password>** [Enter `^Ec?' for help] Press Enter Password: **<switch_password>** Switch> **show version | include ROM** ROM: 12.2(44r)SG11 System returned to ROM by reload **Note:** If the console command fails, contact *My Oracle Support (MOS)*. Note the IOS image & ROM version for comparison in a following step. Check the version from the previous command against the version from [6] HP Solutions Firmware Upgrade Pack Release Notes, Release 2.x.x (Min 2.2.9). If the versions are different, perform the procedure in *Appendix J Upgrade Cisco 4948 PROM* to upgrade the PROM for switch1B.
36. ☐	**Virtual PMAC:** ***(switch console session)*:** Exit the switch console to the PMAC console.	Exit from the switch console by entering**<ctrl-e><c><.>** and you will be returned to the PMAC server prompt.

Procedure 9: Configure Cisco 4948E-F Frame Switches

Step	Procedure	Result
37. ☐	**Virtual PMAC:** Prepare switch1B to be initialized and configured.	Prepare switch1B to be initialized and configured. **$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B setFactoryDefault** Wait 10 minutes for the switch to complete its reboot process.
38. ☐	**Virtual PMAC:** Initialize switch1B	Initialize switch1B by issuing the following command: $ **sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch/xml/switch1B_HLRR_4948E_E-F_init.xml** Processing file: /usr/TKLC/smac/etc/switch/xml/ switch1B_HLRR_4948E_E-F_init.xml **Note:** This step takes about 5-10 minutes to complete. Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact *My Oracle Support (MOS)*. A successful completion of netConfig will return the user to the $ prompt.
39. ☐	**Virtual PMAC:** Retrieve switch1B hostname.	Use netConfig to get the hostname of the switch, to verify that the switch was initialized properly, and to verify that netConfig can connect to the switch. $ **sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getHostname** Hostname: switch1B
40. ☐	**Virtual PMAC:** Verify the switch is using the proper IOS image.	Verify the switch is using the proper IOS image copied to the tftp_service directory. Issue the following commands to verify the IOS release on switch1B: $ **sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getFirmware** Version: 122-54.XO License: entservicesk9 Flash: cat4500e-entservicesk9-mz.122-54.WO.bin
41. ☐	**Virtual PMAC:** Configure switch 1B.	Configure switch 1B by issuing the following commands: $ **sudo /usr/TKLC/plat/bin/netConfig --file=/usr/TKLC/smac/etc/switch/xml/switch1B_HLRR_4948E_E-F_configure.xml** Processing file: /usr/TKLC/smac/etc/switch/xml/ switch1B_HLRR_4948E_E-F_configure.xml **Note:** This may take 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 *My Oracle Support (MOS)*. A successful completion of netConfig will return the user to the prompt.

Procedure 9: Configure Cisco 4948E-F Frame Switches

Step	Procedure	Result
42. ☐	**Virtual PMAC:** Stop the Control TFTP process.	Verify the PID of the control TFTP 192.168.1.1 process: **ps -ef | grep tftp** root 3985 1 0 20:00 00:00:00 /usr/sbin/in.tftpd -l -s --address=10.240.241.118 /var/TKLC/smac/image/ root 3988 1 0 20:00 00:00:00 /usr/sbin/in.tftpd -l -s --address=255.255.255.255 /var/TKLC/smac/image/ root ***13433*** 1 0 Jan28 00:00:00 /usr/sbin/in.tftpd -l -s --address=192.168.1.1 /var/TKLC/smac/image/ Stop the control network TFTP Process: **$ sudo kill -9 <pid>** Verify the control TFTP process is stopped: **ps -ef | grep tftp** no output from the control TFTP 192.168.1.1 process should returned.
43. ☐	**TVOE Management Server:** Ensure that the interfaces of the server connected to switch1A and switch1B are up.	Exit from the virtual PMAC console, by entering **< ctrl-] >** and you will be returned to the TVOE management server prompt. Ensure that the interfaces of the server connected to switch1A and switch1B are up by performing the following commands: $ **sudo /sbin/ifup eth01** $ **sudo /sbin/ifup eth02** **$ sudo netAdm set --type=Bridge --name=control --updateMAC**
44. ☐	Configure the switches on DR Site	**Optional: Repeat this procedure on the Disaster Recovery System Switches.**
45. ☐	Perform *Appendix K Backup Cisco 4948E-F Aggregation Switch* for each switch configured in this procedure.	
THIS PROCEDURE HAS BEEN COMPLETED		

6.9 Install TVOE on all Rack Mount Servers (All Sites)

This procedure installs TVOE 3.0 on a Rack-Mount Server (RMS) to the PMAC system inventory.

Every physical server must have TVOE 3.0 installed on it. The Management Server hosts the PMAC and NOAM-A "logical" servers running in VMs. It should already have TVOE 3.0 installed on it, which was done in Procedure 2.

All other rack mount servers (RMS) need to have TVOE installed on them by using this procedure.

Note: You do not need to run this procedure for any "logical" server (or VM) that co-exists on the same RMS as the PMAC VM. For example, if PMAC and NOAM-A run on the same RMS, you do NOT need to run this procedure for RMS-1 (management server).

Requirements:

- **Procedure 6: Add Cabinet to PMAC System Inventory** has been completed.
- **Procedure 8: Add Software Images to PMAC Server** has been completed.

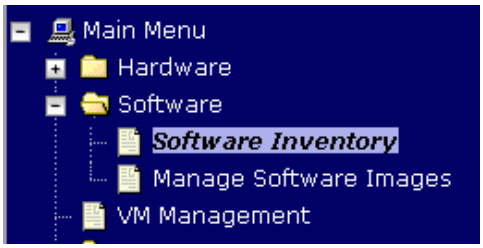
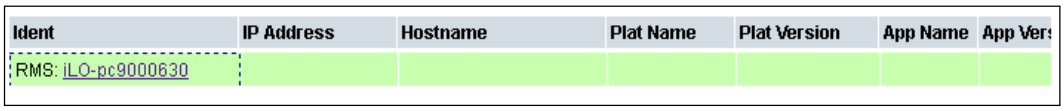
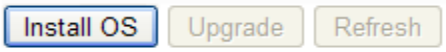
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

IF THIS PROCEDURE FAILS, CONTACT MY ORACLE SUPPORT AND ASK FOR ASSISTANCE.

Procedure10: Install TVOE on all Rack Mount Servers

Step	Procedure	Result
1. ☐	**PMAC GUI:** Login to PMAC GUI	Open web browser and enter: **http://<PMAC_management_network_ip>** Login as **pmacadmin** user. 

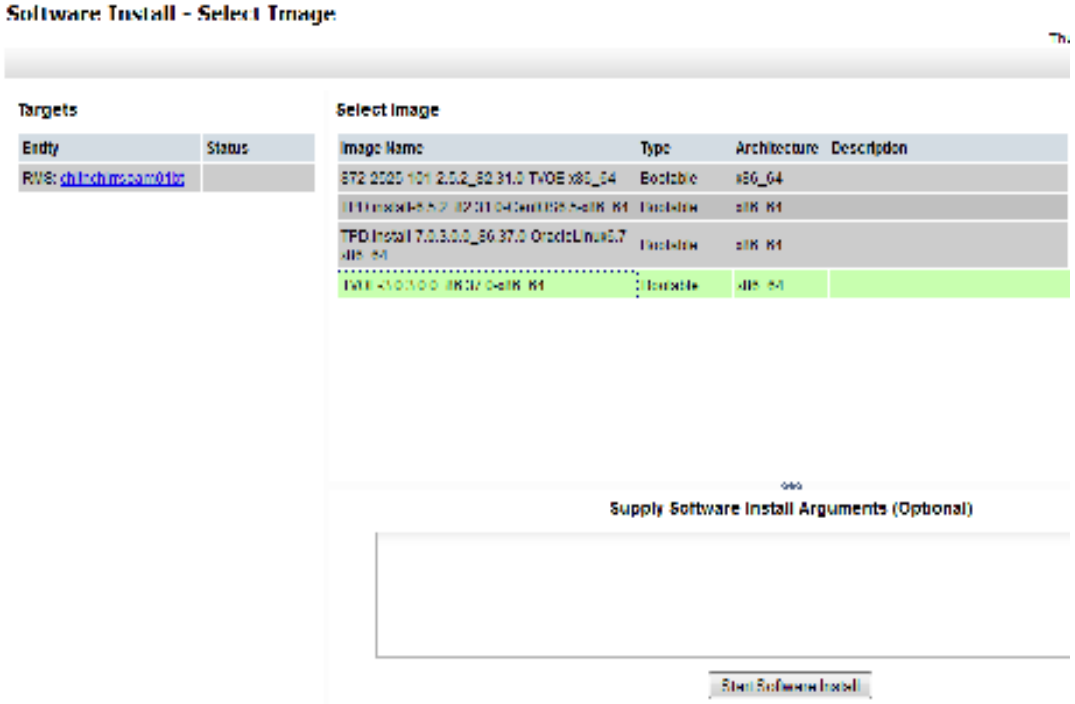
Procedure10: Install TVOE on all Rack Mount Servers

Step	Procedure	Result
2. ☐	**PMAC GUI:** Select server for TVOE 3.0 install **Attention! Do NOT run this step for the RMS that hosts the PMAC (Management Server)**	Navigate to the GUI page: **Software → Software Inventory**.  Select the RMS servers you want to IPM. If you want to install the same TVOE image to more than one RMS server, you may select multiple servers by clicking multiple rows individually. Selected rows will be highlighted in green.   Click on **Install OS** button Record the server name that is IPM'ed in the space provided step 3:

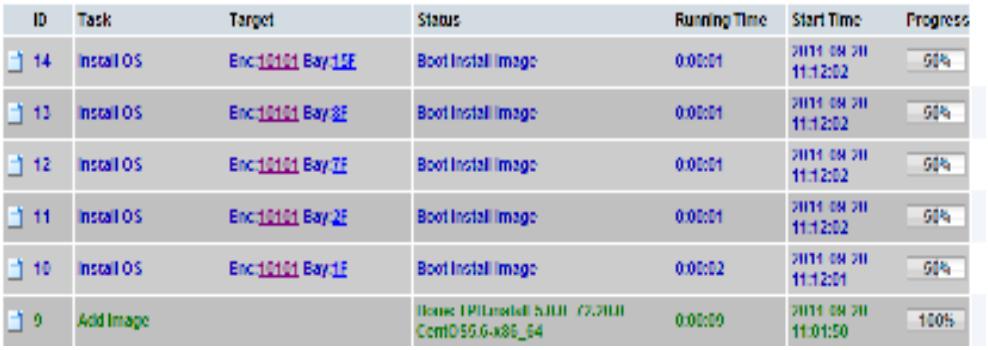
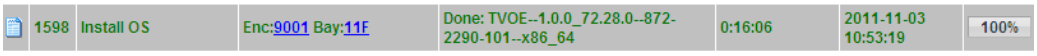
Procedure10: Install TVOE on all Rack Mount Servers

Step	Procedure	Result
3. ☐		Record the server name that is IPM'ed in the space provided below: **Primary Site:** ☐ RMS-2: _____ ☐ RMS-3: _____ ☐ RMS-4: _____ ☐ RMS-5: _____ ☐ RMS-6: _____ ☐ RMS-7: _____ ☐ RMS-8: _____ ☐ RMS-9: _____ ☐ RMS-10: _____ **Disaster Recovery Site:** ☐ RMS-2: _____ ☐ RMS-3: _____ ☐ RMS-4: _____ ☐ RMS-5: _____ ☐ RMS-6: _____ ☐ RMS-7: _____ ☐ RMS-8: _____ ☐ RMS-9: _____ ☐ RMS-10: _____

Procedure10: Install TVOE on all Rack Mount Servers

Step	Procedure	Result
4. ☐	**PMAC GUI:** Initiate TVOE 3.0 OS Install **Attention! Do NOT run this step for the RMS that hosts the PMAC (Management Server)**	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 TVOE 3.0 OS image to install on the selected server.  Click on **Start Software Install** button, then a confirmation window will pop up Click on **Ok** button to proceed with the install.

Procedure10: Install TVOE on all Rack Mount Servers

Step	Procedure	Result
5. ☐	**PMAC GUI:** Monitor OS Install and wait until complete **Attention! Do NOT run this step for the RMS that hosts the PMAC (Management Server)**	Navigate to this GUI page **Main Menu → Task Monitoring** to monitor the progress of the OS installation background task. A separate task will appear for each RMS.  When the installation is complete, the task will change to green and the Progress bar will indicate "100%".  Wait until all TVOE OS Installs are 100% complete and the procedure is finished.
6. ☐	**Repeat Steps 2-5 for each rack mount server.** **These steps can be run on multiple servers in parallel to save time.**	
7. ☐	**Optional: Repeat this procedure on the Disaster Recovery Servers.**	
THIS PROCEDURE HAS BEEN COMPLETED		

6.10 Configure TVOE Host's Network on all Rack Mount Servers (All Sites)

This procedure will configure Network on the Rack Mount Servers that will host HLR Router VMs.
It details the configuration for a single Rack Mount Server (RMS) and should be repeated for every RMS.

Requirements: Procedure10: Install TVOE on all Rack Mount Servers has been completed.

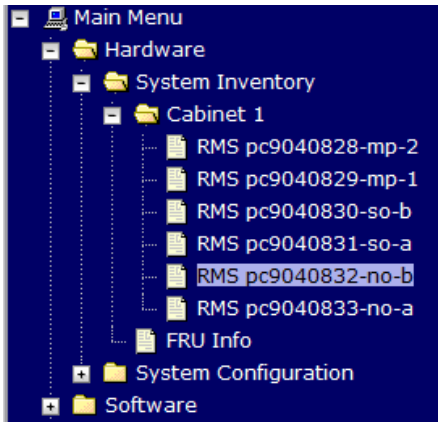
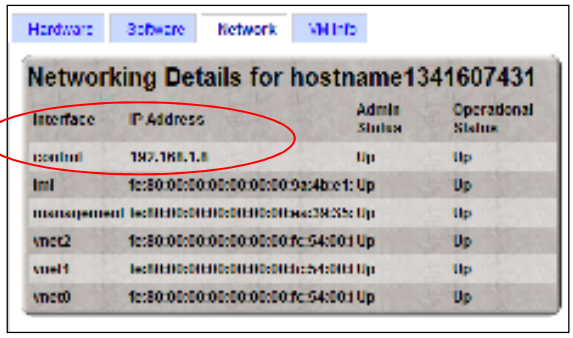
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

IF THIS PROCEDURE FAILS, CONTACT MY ORACLE SUPPORT AND ASK FOR ASSISTANCE.

Procedure 11: Configure TVOE Host's Network on all Rack Mount Servers

Step	Procedure	Result
1. ☐	**PMAC GUI:** *Login to PMAC GUI*	Open web browser and enter: **http://<PMAC_management_network_ip>** Login as **pmacadmin** user. 

Procedure 11: Configure TVOE Host's Network on all Rack Mount Servers

Step	Procedure	Result
2. ☐	**PMAC GUI:** *Find the Control Network IP address of RMS server* **Repeat this step for every RMS**	Navigate to the desired RMS server under the **Hardware → System Inventory** menu, as shown on example below. Select the desired RMS and navigate to the Network tab.   • Record each server's control IP in the space provided below: **Primary Site:** ☐ RMS-1: _____ ☐ RMS-2: _____ ☐ RMS-3: _____ ☐ RMS-4: _____ ☐ RMS-5: _____ ☐ RMS-6: _____ ☐ RMS-7: _____ ☐ RMS-8: _____ ☐ RMS-9: _____ ☐ RMS-10: _____ **Disaster Recovery Site:** ☐ RMS-1: _____ ☐ RMS-2: _____ ☐ RMS-3: _____ ☐ RMS-4: _____ ☐ RMS-5: _____ ☐ RMS-6: _____ ☐ RMS-7: _____ ☐ RMS-8: _____ ☐ RMS-9: _____ ☐ RMS-10: _____

Procedure 11: Configure TVOE Host's Network on all Rack Mount Servers

Step	Procedure	Result
3. ☐	**Management Server:** *SSH into the **Management Server***	Using an SSH client such as putty, ssh to the pmac_management_network_ip using admusr credentials.
4. ☐	**PMAC Server:** *Log into server as the "**admusr**" user.*	login as: **admusr** Password: ***<admusr_password>***
5. ☐	**PMAC Server:** *SSH into each RMS Server* **Attention! Do NOT run this step for RMS-1 which hosts the PMAC (Management Server)**	SSH to each RMS with admusr credentials using the <RMS Control IP Address> from Step 2 of this procedure. Check off each server from the list after steps 6-29 are completed: **Primary Site:** ☐ RMS-2: _____ ☐ RMS-3: _____ ☐ RMS-4: _____ ☐ RMS-5: _____ ☐ RMS-6: _____ ☐ RMS-7: _____ ☐ RMS-8: _____ ☐ RMS-9: _____ ☐ RMS-10: _____ **Disaster Recovery Site: (Optional)** ☐ RMS-2: _____ ☐ RMS-3: _____ ☐ RMS-4: _____ ☐ RMS-5: _____ ☐ RMS-6: _____ ☐ RMS-7: _____ ☐ RMS-8: _____ ☐ RMS-9: _____ ☐ RMS-10: _____

Procedure 11: Configure TVOE Host's Network on all Rack Mount Servers

Step	Procedure	Result
6. ☐	**RMS server:** *Verify/create the Control Network*	Verify the control network by running the following command: ***Note:*** *The output below is for illustrative purposes only, and shows the "control" bridge fully configured.* $ **sudo netAdm query --type=Bridge --name=control** Bridge Name: control On Boot: yes Protocol: none IP Address: 192.168.1.5 Netmask: 255.255.255.0 Promiscuous: no Hwaddr: d8:9d:67:1c:bc:84 MTU: 1500 Delay: 4 Bridge Interface: bond0 Bond0 is created by default when TVOE is installed on the server so the control bridge should have been configured; if so then skip to the next step. It bond0 is missing, create the control network bond0 and assign eth01 and eth02 to it: ***Example:*** $ **sudo netAdm add --device==bond0 --onboot=yes --type=Bonding --mode=active-backup --miimon=100** Interface bond0 added $ **sudo netAdm set --device=eth01 --type=Ethernet --master=bond0 --slave=yes --onboot=yes** Interface eth01 updated $ **sudo netAdm set --device=eth02 --type=Ethernet –-master=bond0 --slave=yes --onboot=yes** Interface eth02 updated $ **sudo netAdm add --type=Bridge --name=control --bootproto=dhcp --onboot=yes --bridgeInterfaces=bond0**

Procedure 11: Configure TVOE Host's Network on all Rack Mount Servers

Step	Procedure	Result
7. ☐	**RMS server:** *Add the Internal Network Management interface bridge on bond0.4*	Create Internal Management Interface bridge $ **sudo netAdm add –-device=bond0.4** Interface bond0.4 added $ **sudo netAdm add --name=imi –-type=Bridge --bridgeInterface=bond0.4** Interface bond0.4 updated Verify the imi network by running the following command $ **sudo netAdm query --type=Bridge --name=imi** Bridge Name: imi On Boot: yes Protocol: none IP Address: Netmask: Promiscuous: no Hwaddr: 98:4b:e1:74:26:4c MTU: Bridge Interface: bond0.4

Procedure 11: Configure TVOE Host's Network on all Rack Mount Servers

Step	Procedure	Result
8. ☐	**DL360 Servers Only** **RMS server:** *Add the External Management Interface (XMI) bridge on bond 1*	**Execute this step for DL360 servers only. For DL380 servers skip to step 9.** Create External Management Interface bridge $ **sudo netAdm add --device=bond1** Interface bond1 added $ **sudo netAdm set --device=eth11 --master=bond1 --slave=yes --onboot=yes --bootproto=none** Interface eth11 was updated. Interface eth11 updated $ **sudo netAdm set --device=eth12 --master=bond1 --slave=yes --onboot=yes --bootproto=none** Interface eth12 was updated. Interface eth12 updated $ **sudo netAdm add --name=management --type=Bridge --bridgeInterface=bond1** Setting up the bridge and unsetting network info Interface bond1 was updated. Bridge management added! Verify the management network by running the following command: $ **sudo netAdm query --type=Bridge --name=management** Bridge Name: management On Boot: yes Protocol: none IP Address: Netmask: Promiscuous: no Hwaddr: ac:16:2d:99:45:84 MTU: 1500 Delay: 4 stp: on Bridge Interface: bond1

Procedure 11: Configure TVOE Host's Network on all Rack Mount Servers

Step	Procedure	Result
9. ☐	**DL380 Servers Only** **RMS server:** *Add the External Management Interface (XMI) bridge on bond 1*	**Execute this step for DL380 servers only. For DL360 servers return to step 8.** Create External Management Interface bridge $ **sudo netAdm add --device=bond1** Interface bond1 added $ **sudo netAdm set --device=eth03 --master=bond1 --slave=yes --onboot=yes --bootproto=none** Interface eth03 was updated. Interface eth03 updated $ **sudo netAdm set --device=eth04 --master=bond1 --slave=yes --onboot=yes --bootproto=none** Interface eth04 was updated. Interface eth04 updated $ **sudo netAdm add --name=management --type=Bridge --bridgeInterface=bond1** Setting up the bridge and unsetting network info Interface bond1 was updated. Bridge management added! Verify the management network by running the following command: $ **sudo netAdm query --type=Bridge --name=management** Bridge Name: management On Boot: yes Protocol: none IP Address: Netmask: Promiscuous: no Hwaddr: ac:16:2d:99:45:84 MTU: 1500 Delay: 4 stp: on Bridge Interface: bond1

Procedure 11: Configure TVOE Host's Network on all Rack Mount Servers

Step	Procedure	Result
10. ☐	**RMS server:** *Assign IP address to the XMI/ management network*	Set XMI management bridge IP address: **Note:** The output below is for illustrative purposes only. The NAPD information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure. ***Syntax:*** $ **sudo netAdm set --name=management --type=Bridge --address=<XMI Management_ip address> --netmask=<netmask>** ***Example:*** $ **sudo netAdm set --name=management --type=Bridge --address=10.240.37.2 --netmask=255.255.255.224** Interface bond1 was updated. Setting up the bridge and unsetting network info Interface bond1 was updated. Bridge management updated! Verify the management network bridge by running the following command: $ **sudo netAdm query --type=Bridge --name=management** Bridge Name: management On Boot: yes Protocol: none IP Address: 10.240.37.2 Netmask: 255.255.255.224 Promiscuous: no Hwaddr: ac:16:2d:99:45:84 MTU: 1500 Delay: 4 stp: on Bridge Interface: bond1

Procedure 11: Configure TVOE Host's Network on all Rack Mount Servers

Step	Procedure	Result
11. ☐	**RMS server:** *Set management bridge default route*	Add the default route on the management network. **Note:** The output below is for illustrative purposes only. The NAPD information for this system will determine the network interfaces, (network devices, bonds, and bond enslaved devices), to configure. ***Syntax:*** $ **sudo netAdm add --route=default --gateway=<mgmt_gateway_address> --device=<TVOE_Managament_Bridge>** ***Example:*** $ **sudo netAdm add --route=default --gateway=10.250.43.161 --device=management** Route to management added Verify the management network by running the following command $ **sudo netAdm query --route=default --device=management** Routes for TABLE: main and DEVICE: management * NETWORK: default GATEWAY: 10.250.43.161
12. ☐	**DL360 RMS server:** *Add XSI1 bridge on MP* **Note: Only run this step on DL360 RMS servers that are hosting an MP**.	**This step is for DL360 RMS servers that are hosting an MP.** **If the server is a DL380 hosting an MP, then skip to step 14**. Create External Signaling Interface bridge xsi1: $ **sudo netAdm add –-name=xsi1 –-type=Bridge --bridgeInterface=eth13** Interface xsi1 added Verify the xsi1 network is running: $ **sudo netAdm query --type=Bridge --name=xsi1** Bridge Name: xsi1 On Boot: yes Protocol: none IP Address: Netmask: Promiscuous: no Hwaddr: e8:39:35:0f:42:ac MTU: Bridge Interface: eth13

Procedure 11: Configure TVOE Host's Network on all Rack Mount Servers

Step	Procedure	Result
13. ☐	**DL360 RMS server:** *Add XSI2 bridge on MP* **Note: Only run this step on DL360 RMS Servers that are hosting an MP.**	**This step is for DL360 RMS servers that are hosting an MP.** **If the server is a DL380 hosting an MP, then skip to step 14.** Create External Signaling Interface bridge xsi2: $ **sudo netAdm add –-name=xsi2 –-type=Bridge --bridgeInterface=eth14** Interface xsi2 added Verify the xsi2 network is running: $ **sudo netAdm query --type=Bridge --name=xsi2** Bridge Name: xsi2 On Boot: yes Protocol: none IP Address: Netmask: Promiscuous: no Hwaddr: e8:39:35:0f:42:ac MTU: Bridge Interface: eth14
14. ☐	**DL380 RMS server:** *Add XS1 bridge on MP* **Note: Only run this step on DL380 RMS servers that are hosting an MP.**	**This step is for DL380 RMS servers that are hosting an MP.** **If the server is a DL360 hosting an MP, then return to step 12.** Create External Signaling Interface bridge xsi1: $ **sudo netAdm add –-name=xsi1 –-type=Bridge --bridgeInterface=eth05** Interface xsi1 added Verify the xsi1 network is running: $ **sudo netAdm query --type=Bridge --name=xsi1** Bridge Name: xsi1 On Boot: yes Protocol: none IP Address: Netmask: Promiscuous: no Hwaddr: e8:39:35:0f:42:ac MTU: Bridge Interface: eth05

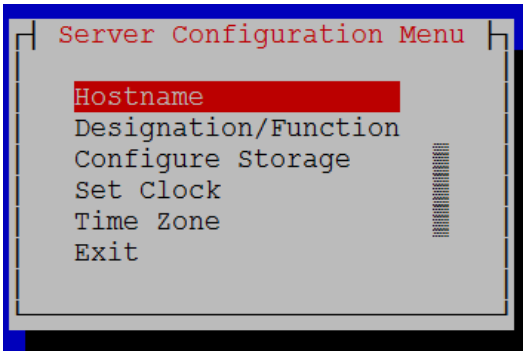
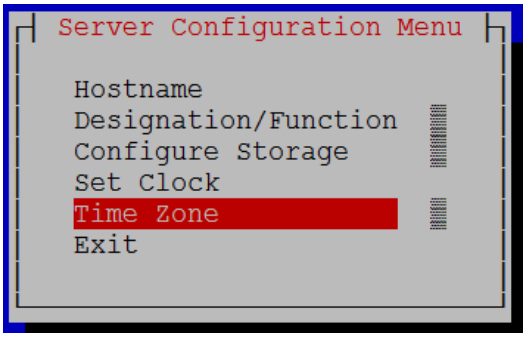
Procedure 11: Configure TVOE Host's Network on all Rack Mount Servers

Step	Procedure	Result
15. ☐	**DL380 RMS server:** *Add XSI2 bridge on MP* **Note: Only run this step on DL380 RMS Servers that are hosting an MP.**	**This step is for DL380 RMS servers that are hosting an MP.** **If the server is a DL360 hosting an MP, then return to step 12.** Create External Signaling Interface bridge xsi2: $ **sudo netAdm add –-name=xsi2 –-type=Bridge --bridgeInterface=eth06** Interface xsi2 added Verify the xsi2 network is running: $ **sudo netAdm query --type=Bridge --name=xsi2** Bridge Name: xsi2 On Boot: yes Protocol: none IP Address: Netmask: Promiscuous: no Hwaddr: e8:39:35:0f:42:ac MTU: Bridge Interface: eth06
16. ☐	**DL380 RMS server:** *Add XS3 bridge on MP* **Note: Only run this step on DL380 RMS servers that are hosting an MP.**	**Optional: XSI-3 (DL380 Only)** **This step is for DL380 RMS servers that are hosting an MP.** Create External Signaling Interface bridge xsi3: $ **sudo netAdm add –-name=xsi3 –-type=Bridge --bridgeInterface=eth07** Interface xsi4 added Verify the xsi3 network is running: $ **sudo netAdm query --type=Bridge --name=xsi3** Bridge Name: xsi3 On Boot: yes Protocol: none IP Address: Netmask: Promiscuous: no Hwaddr: e8:39:35:0f:42:ac MTU: Bridge Interface: eth07

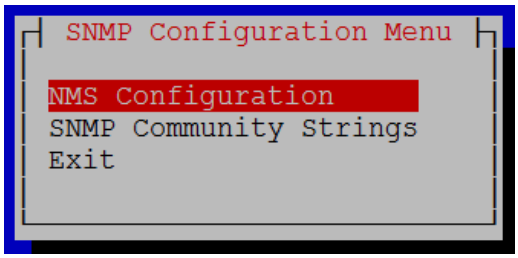
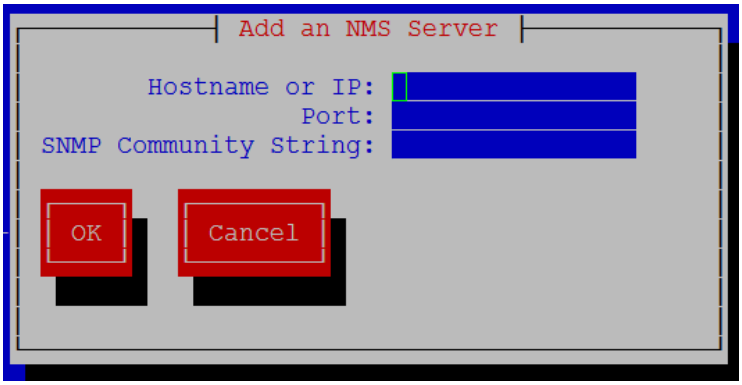
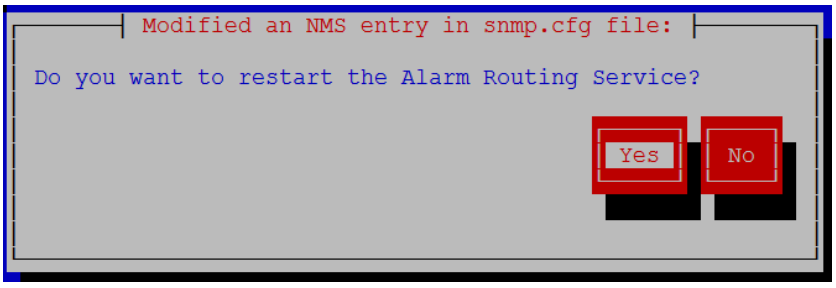
Procedure 11: Configure TVOE Host's Network on all Rack Mount Servers

Step	Procedure	Result
17. ☐	**DL380 RMS server:** *Add XS4 bridge on MP* **Note: Only run this step on DL380 RMS servers that are hosting an MP**.	**Optional: XSI-4 (DL380 Only)** **This step is for DL380 RMS servers that are hosting an MP.** Create External Signaling Interface bridge xsi4: $ **sudo netAdm add –-name=xsi4 –-type=Bridge --bridgeInterface=eth08** Interface xsi4 added Verify the xsi4 network is running: $ **sudo netAdm query --type=Bridge --name=xsi4** Bridge Name: xsi4 On Boot: yes Protocol: none IP Address: Netmask: Promiscuous: no Hwaddr: e8:39:35:0f:42:ac MTU: Bridge Interface: eth08
18. ☐	**RMS Server:** *Setup Syscheck*	***Note**: syscheck must be configured to monitor bonded interfaces.* Replace "bondedInterfaces" with "bond0" or "bond0,bond1" if segregated networks are used: $ **sudo syscheckAdm net ipbond --set --var=DEVICES --val=bond0,bond1** $ **sudo syscheckAdm net ipbond -enable** $ **sudo syscheck -v net ipbond**

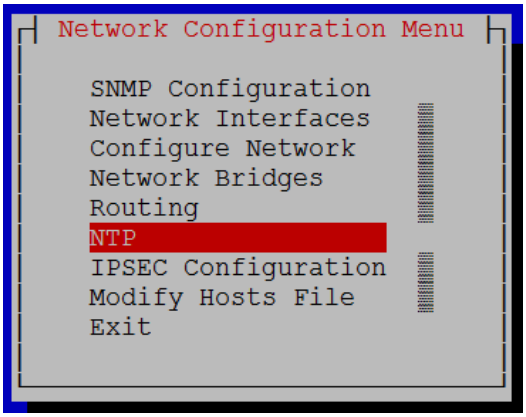
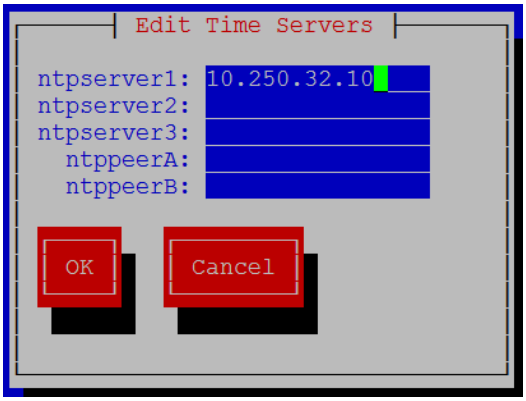
Procedure 11: Configure TVOE Host's Network on all Rack Mount Servers

Step	Procedure	Result
19. ☐	**RMS Server:** *Set Hostname*	Set the server hostname: $ **sudo su – platcfg** **1.** Navigate to **Server Configuration ➤ Hostname**  **2.** Select Edit **3.** Set TVOE Management Server hostname **4.** Press OK. **5.** Navigate out of Hostname
20. ☐	**RMS Server:** *Set Time Zone and/or Hardware Clock*	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. **4.** Press OK. **5.** Navigate out of Server Configuration

Procedure 11: Configure TVOE Host's Network on all Rack Mount Servers

Step	Procedure	Result
21. ☐	**RMS Server:** *Configure SNMP trap destination* *See the NAPD documention for SNMP specifics.*	Configure SNMP trap destination: **1.** Navigate to **Network Configuration ➤ SNMP Configuration ➤ NMS Configuration**.  **2.** Select **Edit** and then choose 'Add a New NMS Server'. **3.** The 'Add an NMS Server' page will be displayed.  **4.** Complete the form by entering NMS server IP, Port (default port is 162) and community string provided by the customer about the SNMP trap destination. **5.** Select **OK** to finalize the configuration. **6.** The 'NMS Server Action Menu' will now be displayed. **7.** Select **Exit**. The following dialogue will then be presented:  **8.** Select **Yes** and then wait a few seconds while the Alarm Routing Service is restarted. **9.** At that time the SNMP Configuration Menu will be presented. ***Note**: All alarm information will then be sent to the NMS located at the destination.*

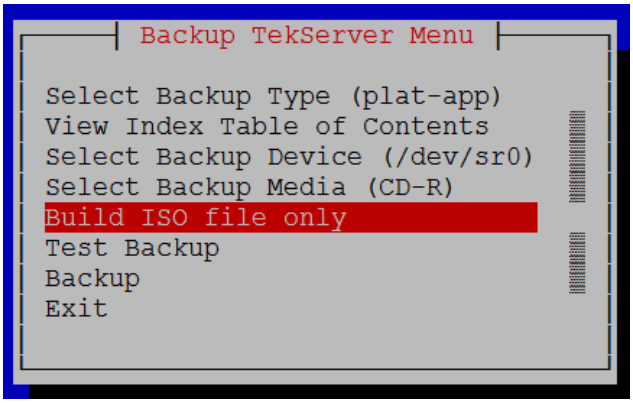
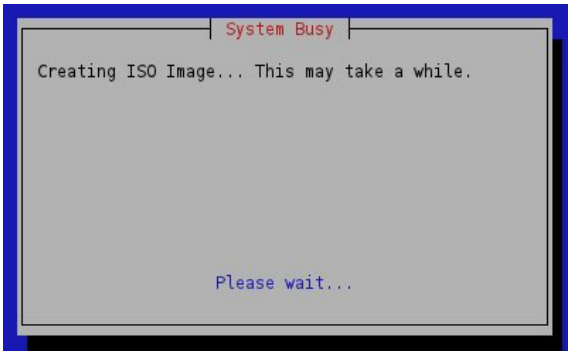
Procedure 11: Configure TVOE Host's Network on all Rack Mount Servers

Step	Procedure	Result
22. ☐	**RMS Server:** *Configure NTP*	Configure NTP servers: **1.** Navigate to **Network Configuration ➤ NTP.**  **2.** Set NTP server IP address to point to the customer provided NTP servers (**3 NTP Servers are required**). See paragraph **4.4 NTP Strategy** for more information on NTP deployment.  **3.** Press OK. **4.** Navigate out of Network Configuration **5.** Exit platcfg.
23. ☐	**RMS Server:** *Set server time*	Set time based on NTP server: $ **sudo service ntpd stop** $ **sudo ntpdate ntpserver1** $ **sudo service ntpd start**

Procedure 11: Configure TVOE Host's Network on all Rack Mount Servers

Step	Procedure	Result
24. ☐	**RMS Server:** *Reboot the server*	Reboot the server: $ **sudo init 6** Wait until the reboot completes and re-login with TVOE admusr credentials.
25. ☐	**RMS Server:** *Verify server health*	Verify server health: $ **sudo alarmMgr -alarmStatus** ***Note**: This command should return no output on a healthy system. If any alarms are reported, please stop and contact Oracle's Customer Care Center before continuing.*

Procedure 11: Configure TVOE Host's Network on all Rack Mount Servers

Step	Procedure	Result
26. ☐	**RMS Server:** *Perform a TVOE backup*	Login as platcfg user. The platcfg main menu will be shown $ **sudo su – platcfg** **1.** Navigate to **Maintenance ➤Backup and Restore ➤Backup Platform (CD/DVD)** **2.** The 'Backup TekServer Menu' page will now be shown.  **3.** Select **Build ISO file only**. ***Note**: Creating the ISO image may happen so quickly that this screen may only appear for an instant.*  **4.** After the ISO is created, platcfg will return to the Backup TekServer Menu as shown in step 2. **5.** The ISO has been created and is located in *the /var/TKLC/bkp/* directory. An example filename of a backup file that was created is: *"hostname1307466752-plat-app-201104171705.iso"* **6.** Exit platcfg.

Procedure 11: Configure TVOE Host's Network on all Rack Mount Servers

Step	Procedure	Result
27. ☐	**Customer Server SSH:** *Copy backup image to the customer server*	Login to the customer server and copy backup image to the customer server where it can be safely stored.
28. ☐	**Repeat Steps 5 -27 for each rack mount server.**	
29. ☐	**Optional: Repeat this procedure on the Disaster Recovery Servers.**	
THIS PROCEDURE HAS BEEN COMPLETED		

6.11 Create, IPM and Install Application on all Virtual Machines (All Sites)

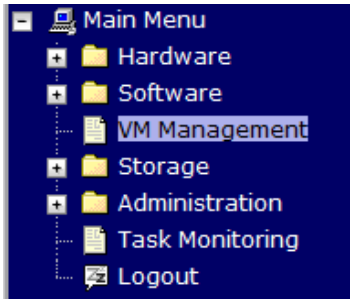
This procedure will create Virtual Machines (VMs) on the Rack Mount Servers, install the TPD operating system on each VM, and then install the HLRR 4.1 application on each VM. It details the create/IPM/install for a single VM and should be repeated for every VM.

Requirements: Procedure 11: Configure TVOE Host's Network on all Rack Mount Servers has been completed.

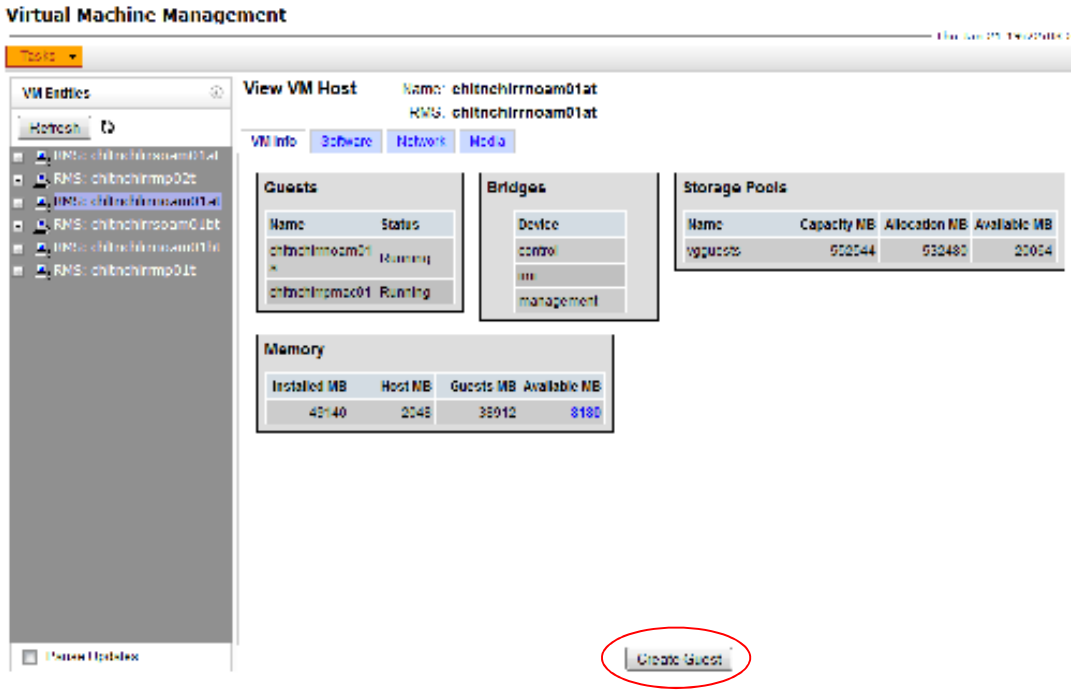
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

IF THIS PROCEDURE FAILS, CONTACT MY ORACLE SUPPORT AND ASK FOR ASSISTANCE.

Procedure 12: Create, IPM and Install Application on all Virtual Machines

Step	Procedure	Result
1. ☐	**PMAC GUI:** *Login to PMAC GUI*	Open web browser and enter: **http://<pmac_management_network_ip>** Login as **pmacadmin** user. 
2. ☐	**PMAC GUI:** *Navigate to VM Management menu*	Navigate to this GUI page: **Main Menu → VM Management** 

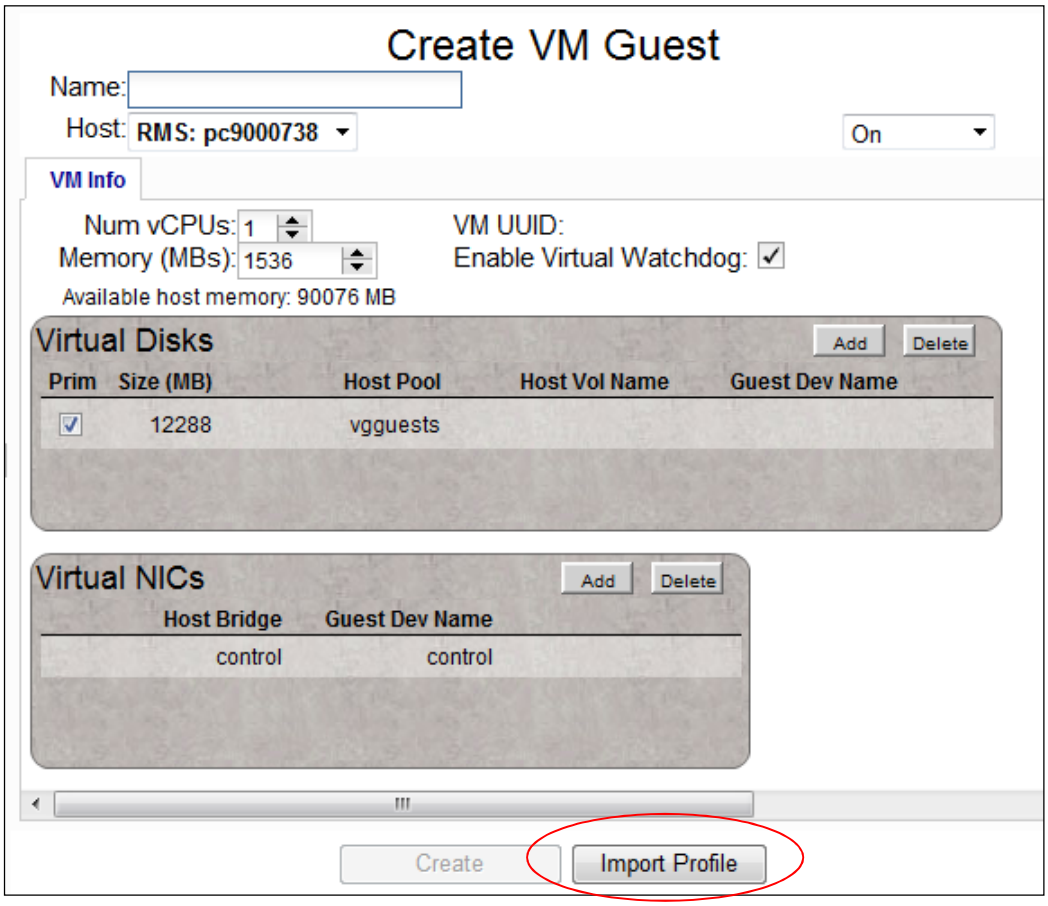
Procedure 12: Create, IPM and Install Application on all Virtual Machines

Step	Procedure	Result
3. ☐	**PMAC GUI:** *Select the desired Rack Mount Server (RMS) and create the VM Guest*	Select the TVOE rack mounted server from the "VM Entities" listing on the left side of the screen. The selected server's guest machine configuration will then be displayed.  Click on **Create Guest** button Record the **VM Guest Name** of each VM in the space provided in step 4.

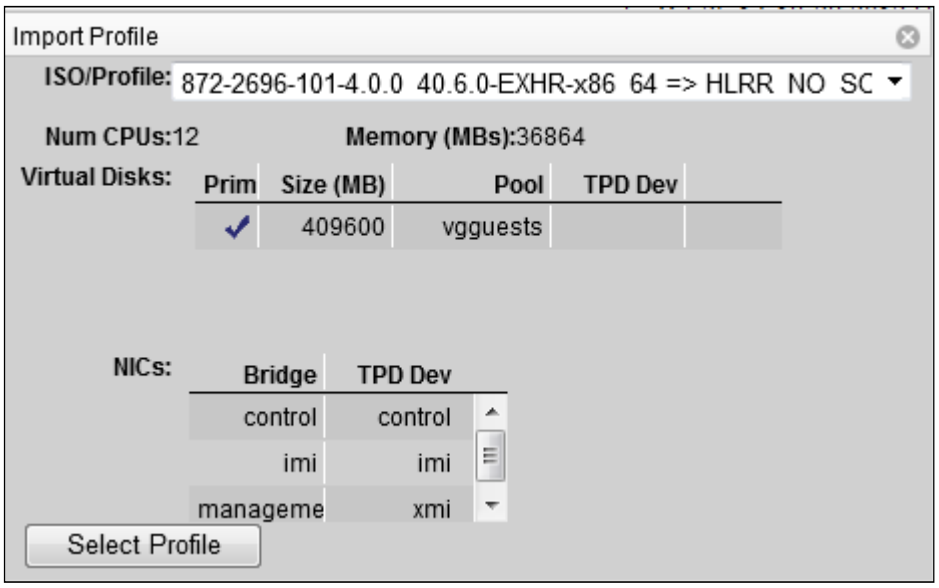
Procedure 12: Create, IPM and Install Application on all Virtual Machines

Step	Procedure	Result
4. ☐	*Check off each VM as it is completed.*	Check-off the associated **Check Box** as each VM is completed and record the **VM Guest Name** of each VM in the space provided. **Primary Site:** ☐ NOAM-A: _____ ☐ NOAM-B: _____ ☐ SOAM-A:_____ ☐ SOAM-B:_____ ☐ QS-1:_____ ☐ MP-1:_____ ☐ MP-2:_____ ☐ MP-3:_____ ☐ MP-4:_____ ☐ MP-5:_____ **Disaster Recovery Site: (Optional)** ☐ NOAM-A: _____ ☐ NOAM-B: _____ ☐ SOAM-A:_____ ☐ SOAM-B:_____ ☐ QS-1:_____ ☐ MP-1:_____ ☐ MP-2:_____ ☐ MP-3:_____ ☐ MP-4:_____ ☐ MP-5:_____

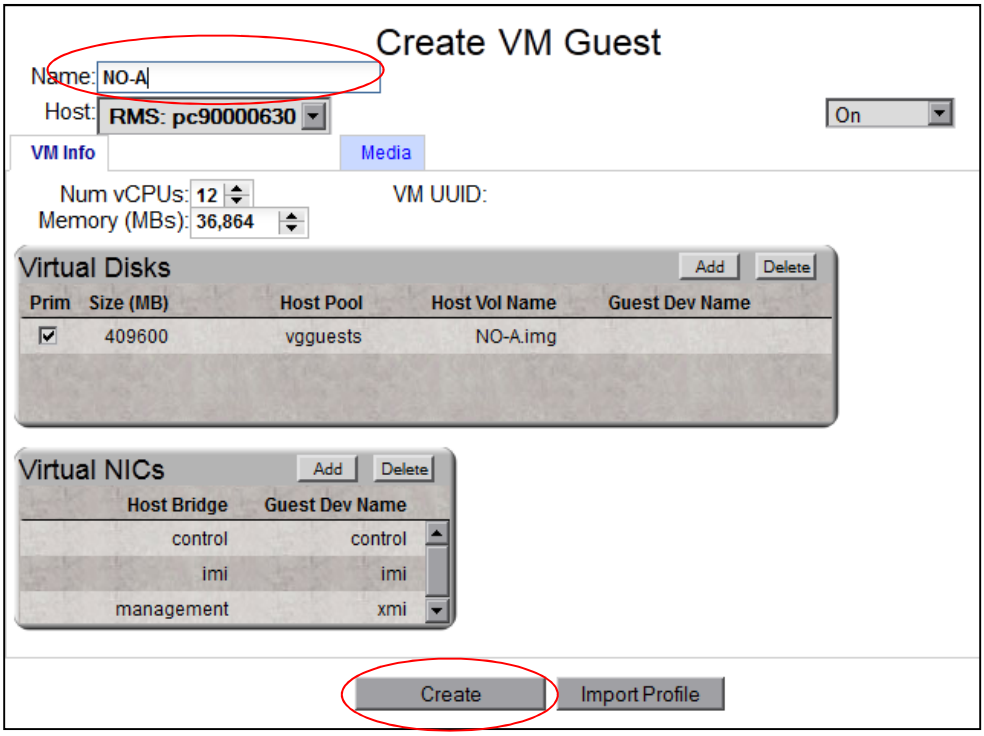
Procedure 12: Create, IPM and Install Application on all Virtual Machines

Step	Procedure	Result
5. ☐	**PMAC GUI:** *Click on the* ***Import Profile*** *dialogue button*	A **"Create VM Guest"** window is displayed that is similar to the below:  Click **"Import Profile"** button .

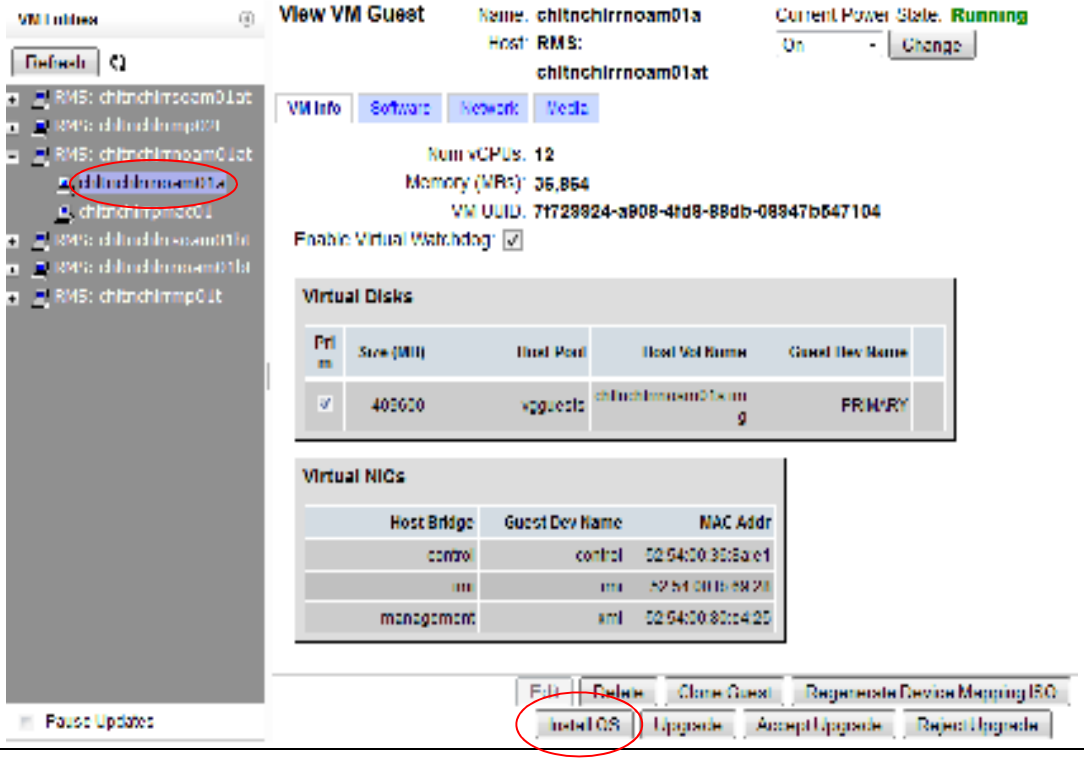
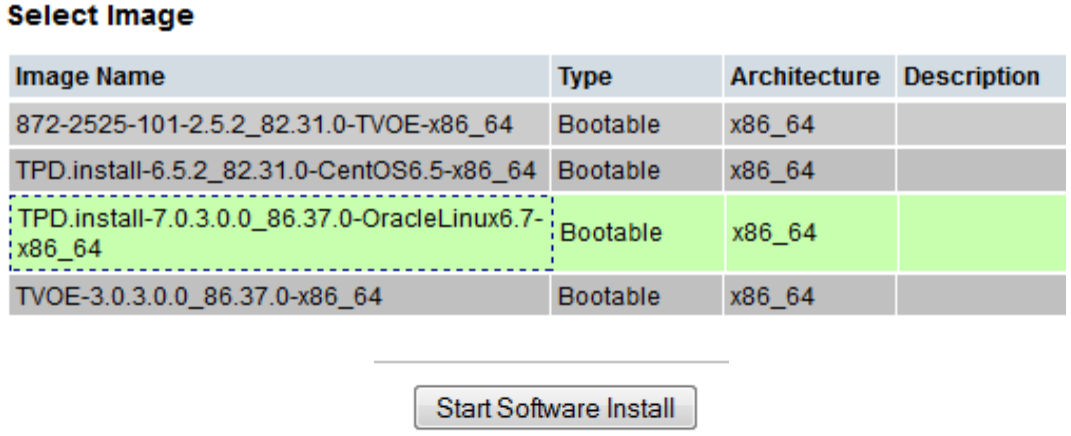
Procedure 12: Create, IPM and Install Application on all Virtual Machines

Step	Procedure	Result
6. ☐	**PMAC GUI:** *Select the desired* ***ISO/Profile*** *value*	Select the desired **ISO/Profile**. - If creating a VM for a NOAM, SOAM or Query Server, on a HP DL360, use the profile: "**EXHR-4.1.0_41.x.0-86_64=> HLRR_NO_SO_QS**" - If creating a VM for an MP server on a HP DL360, use the profile: "**EXHR-4.1.0_41.x.0-86_64=> HLRR_MP**" - If creating a VM for a NOAM, SOAM or Query Server, on a HP DL380 (Gen9), use the profile: "**EXHR-4.1.0_41.x.0-86_64=> HLRR_GEN9_NO_SO_QS**" - If creating a VM for an MP server on a HP DL380 (Gen9), use the profile: "**EXHR-4.1.0_41.x.0-86_64=> HLRR_GEN9_MP**"  Click on **Select Profile** button.

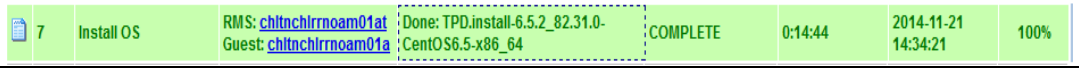
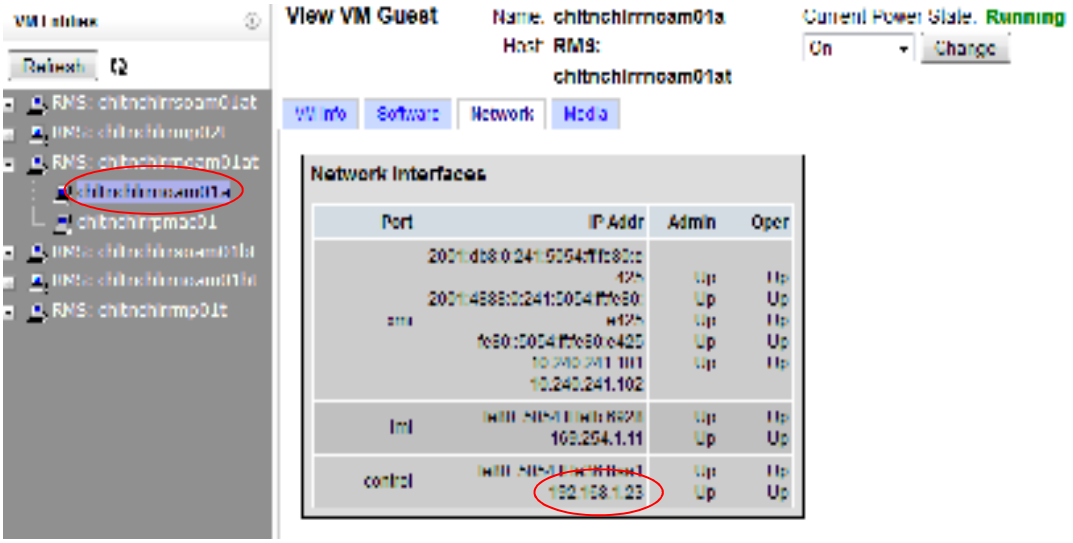
Procedure 12: Create, IPM and Install Application on all Virtual Machines

Step	Procedure	Result
7. ☐	**PMAC GUI:** *Override the VM Guest **Name** to make it unique for the site*	A "**Create VM Guest**" window is displayed that is similar to the below.  Override the **Name** field and change it to: NO-A, NO-B, QS-1, QS-2, SO-A, SO-B, MP-1 or MP-2. You could also include a location within the Name value such as NO-MRSVNC-A. **Note:** This information should be available in the NAPD documentation. Click **"Create"** button
8. ☐	**PMAC GUI:** *Verify that Create VM task successfully completes.*	Verify that the Virtual Machine successfully created.  The user should see a screen similar to above with a **Progress** value of **100%**.

Procedure 12: Create, IPM and Install Application on all Virtual Machines

Step	Procedure	Result
9. ☐	**PMAC GUI:** *Install the TPD operating system on the VM.*	Select the VM Guest Name from the VM Entities list, and click **Install OS** button 
10. ☐	**PMAC GUI:** *Select the TPD 7.0.x image and start installing TPD*	Select the desired TPD image (highlighted in green), and click **Start Software Install** button. 

Procedure 12: Create, IPM and Install Application on all Virtual Machines

Step	Procedure	Result
11. ☐	**PMAC GUI:** *Monitor the Install OS task and wait until it successfully completes.*	Navigate to this GUI page **Main Menu → Task Monitoring** to monitor the progress of the OS installation task. A separate task will appear for each VM guest affected When the installation is complete, the task will change to green and the Progress field will indicate "100%". 
12. ☐	**PMAC GUI:** *Record control IP address of each VM Guest*	Navigate to this GUI page **Main Menu → VM Management** Select the VM Guest Name from the VM Entities list, and click **"Network"** tab  Determine control IP address of each VM Guest and record it in step 13.

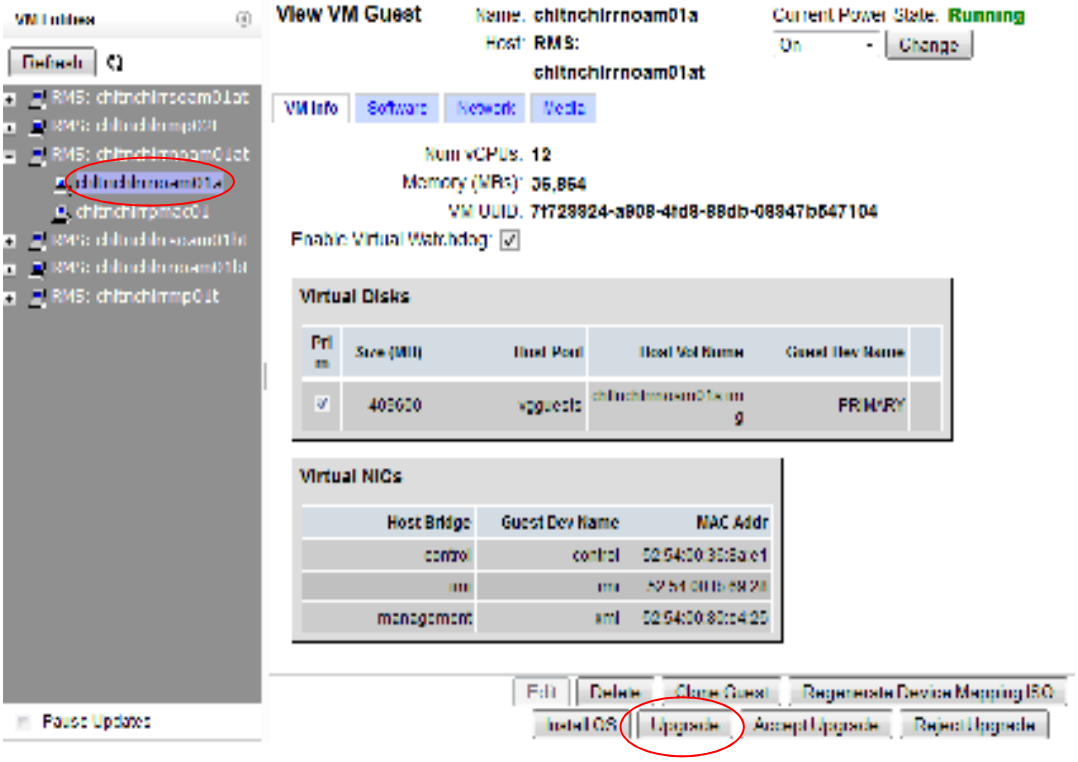
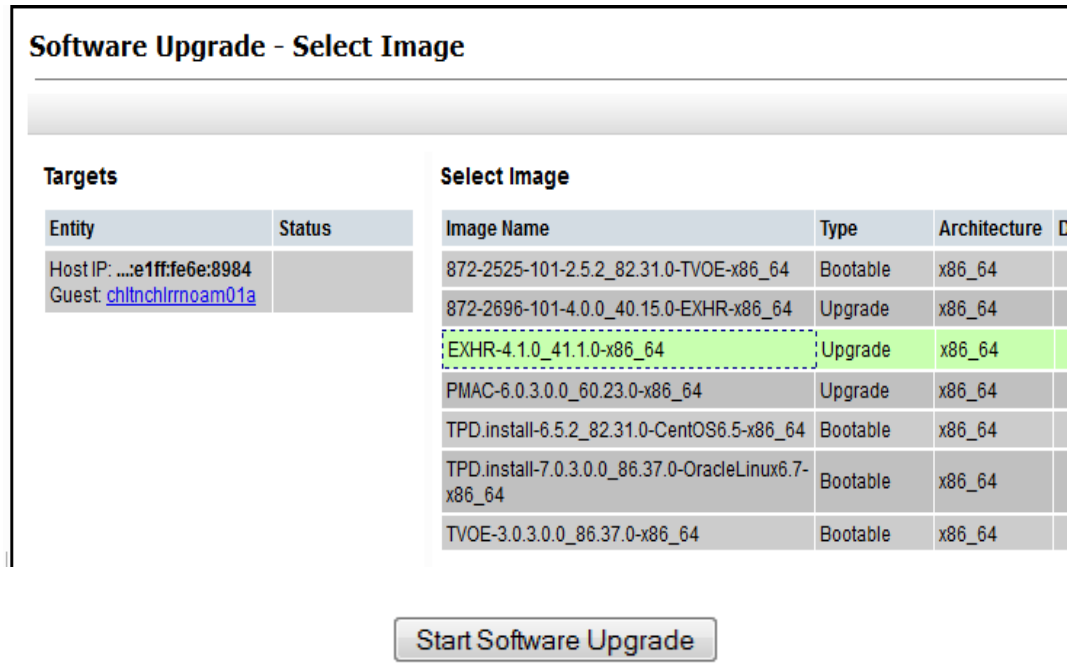
Procedure 12: Create, IPM and Install Application on all Virtual Machines

Step	Procedure	Result
13. ☐	**PMAC GUI:** *Record control IP address of each VM Guest*	Determine control IP address of each VM Guest and record it below. **Primary Site:** ☐ NOAM-A: _____ ☐ NOAM-B: _____ ☐ SOAM-A:_____ ☐ SOAM-B:_____ ☐ QS-1:_____ ☐ MP-1:_____ ☐ MP-2:_____ ☐ MP-3:_____ ☐ MP-4:_____ ☐ MP-5:_____ **Disaster Recovery Site: (Optional)** ☐ NOAM-A: _____ ☐ NOAM-B: _____ ☐ SOAM-A:_____ ☐ SOAM-B:_____ ☐ QS-1:_____ ☐ MP-1:_____ ☐ MP-2:_____ ☐ MP-3:_____ ☐ MP-4:_____ ☐ MP-5:_____

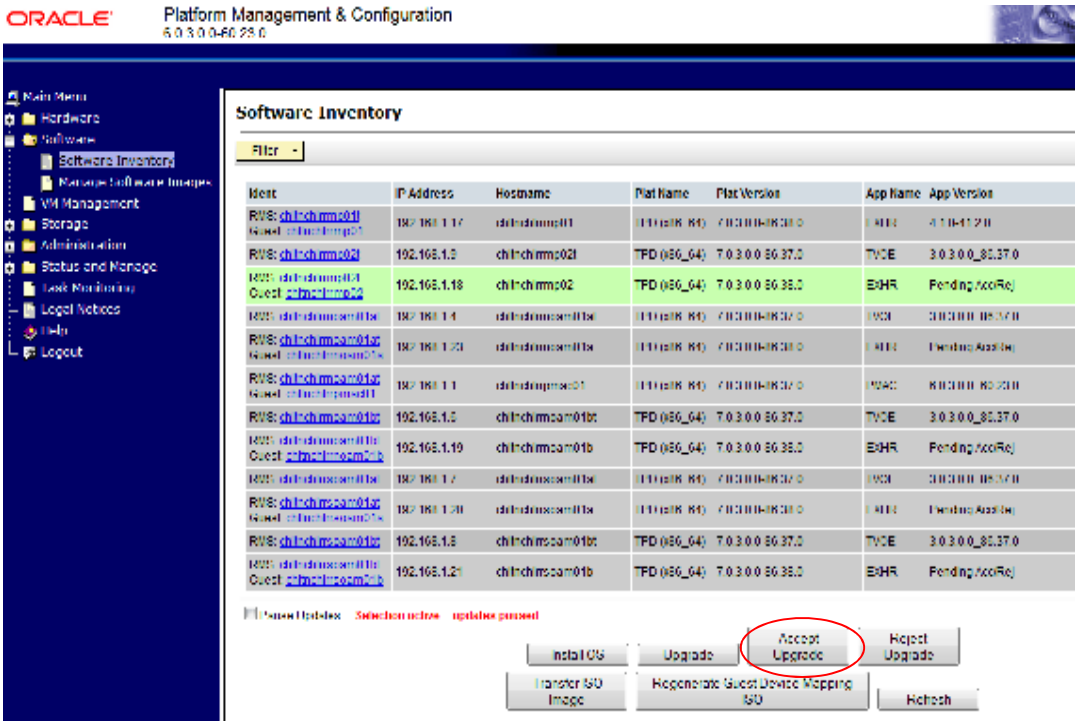
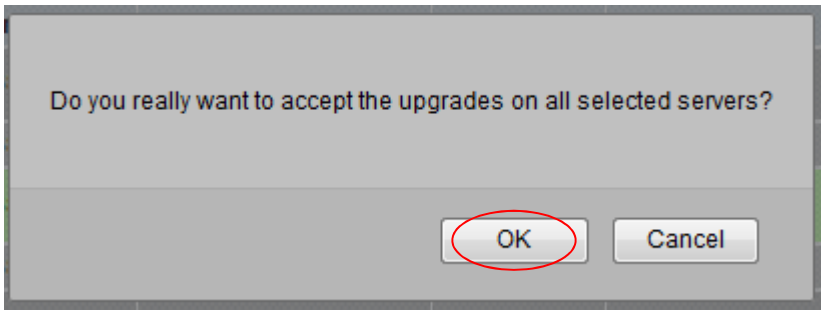
Procedure 12: Create, IPM and Install Application on all Virtual Machines

Step	Procedure	Result
14. ☐	**Virtual PMAC server SSH:** *SSH into the VM Guest* *Record initial hostname of each VM Guest*	From PMAC server console, open SSH session to the VM Guest using admusr credentials and the <VM Guest Control IP Address> obtained from Step 13 of this procedure. **$ ssh <VM Guest Control IP Address>** Determine initial hostname of each VM Guest and record it below. **Primary Site:** ☐ NOAM-A: _____ ☐ NOAM-B: _____ ☐ SOAM-A:_____ ☐ SOAM-B:_____ ☐ QS-1:_____ ☐ MP-1:_____ ☐ MP-2:_____ ☐ MP-3:_____ ☐ MP-4:_____ ☐ MP-5:_____ **Disaster Recovery Site: (Optional)** ☐ NOAM-A: _____ ☐ NOAM-B: _____ ☐ SOAM-A:_____ ☐ SOAM-B:_____ ☐ QS-1:_____ ☐ MP-1:_____ ☐ MP-2:_____ ☐ MP-3:_____ ☐ MP-4:_____ ☐ MP-5:_____
15. ☐	**PMAC GUI:** *Verify that the initial hostname of each VM Guest is unique*	Verify that initial hostname on each VM Guest is unique and correct. If any two or more VM Guests on a site have identical hostnames, then delete and re-create the duplicate VM Guest as shown in steps 3-11 of this procedure. Otherwise continue to the next step.

Procedure 12: Create, IPM and Install Application on all Virtual Machines

Step	Procedure	Result
16. ☐	**PMAC GUI:** *Install the HLRR 4.1 application on the VM.*	Select the VM Guest Name from the VM Entities list, and click **"Upgrade"** button 
17. ☐	**PMAC GUI:** *Select the Application image and start installing the HLRR 4.1 Application*	Select the HLR Router 4.1 Application image, and click **"Start Software Upgrade"** button. 

Procedure 12: Create, IPM and Install Application on all Virtual Machines

Step	Procedure	Result
18. ☐	**PMAC GUI:** *Monitor the Upgrade task.*	Navigate to this GUI page **Main Menu → Task Monitoring** to monitor the progress of the OS installation task. A separate task will appear for each VM Guest affected. When the upgrade is complete, the task will change to green and the Progress field will indicate "100%". 
19. ☐	**PMAC GUI:** *Accept the upgrade of this server* Select **Software => Software Inventory** **1)** Select the VM Guest that is to be accepted. It will be highlighted in green. **2)** Click **Accept Upgrade** button to accept the HLRR Application Upgrade. **3)** Click on the **OK** button on the pop up window to begin the acceptance process.	 
20. ☐	**Repeat Steps 2 - 19 for each Virtual Machine (VM) Guest listed in step 4 of this procedure.** **This procedure can be run on multiple VM Guests at the same time.**	

Procedure 12: Create, IPM and Install Application on all Virtual Machines

Step	Procedure	Result
21. ☐	**Optional: Repeat this procedure on the Disaster Recovery VM Guests.**	
THIS PROCEDURE HAS BEEN COMPLETED		

7. CONFIGURATION PROCEDURES

7.1 Configuring HLRR NOAM-A Server (1st NOAM site only)

This procedure configures the first NOAM server. This includes configuring a temporary interface to the NOAM-A GUI, creating Network Elements for all required networks (NOAMs, SOAMs and DR NOAMs), configuring Services and creating/configuring the first NOAM-A server.

Requirements: Procedure 12: Create, IPM and Install Application on all Virtual Machines has been completed for all servers.

Assumptions:

- This procedure assumes that the HLRR Network Element XML file for the NOAM and SOAM sites have been previously created, as described in Appendix D: Creating an XML file for Installing HLRR Network Elements.
- The HLRR Network Element XML files for the Disaster Recovery NOAM and SOAM sites (optional) should also be created as described in Appendix D: Creating an XML file for Installing HLRR Network Elements.
- This procedure assumes that the Network Element XML files are either on a USB flash drive or the laptop's hard drive. The steps are written as if the XML files are on a USB flash drive, but the files can exist on any accessible drive.

This procedure requires that the user connects to the HLRR GUI prior to configuring the first HLRR server. This can be done either by one of two procedures:

1. Configuring a temporary external IP address, as described in **Appendix C:** Creating Temporary External IP Address for Accessing HLRR GUI
2. Plugging a laptop into an unused, unconfigured port on the NOAM-A server using a direct-connect Ethernet cable.

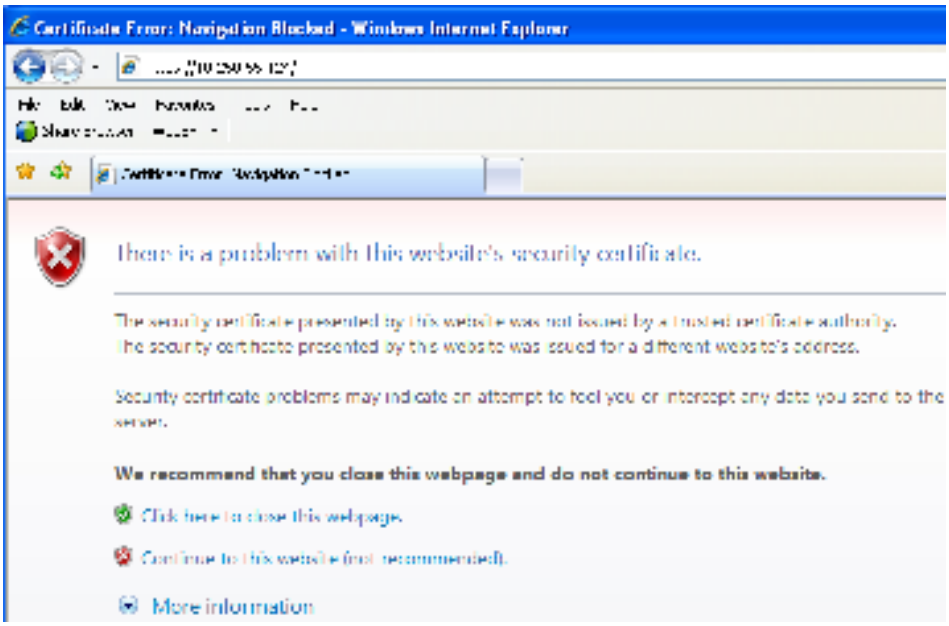
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

IF THIS PROCEDURE FAILS, CONTACT MY ORACLE SUPPORT AND ASK FOR ASSISTANCE.

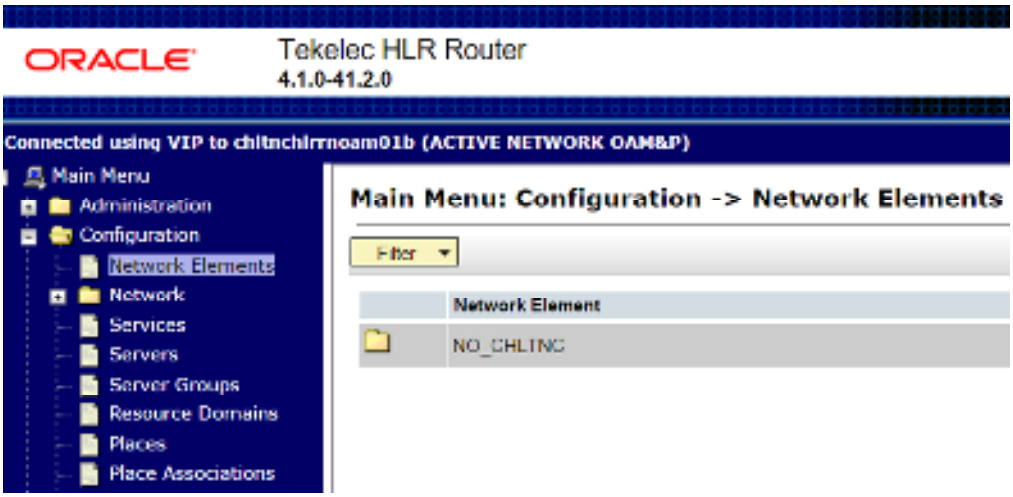
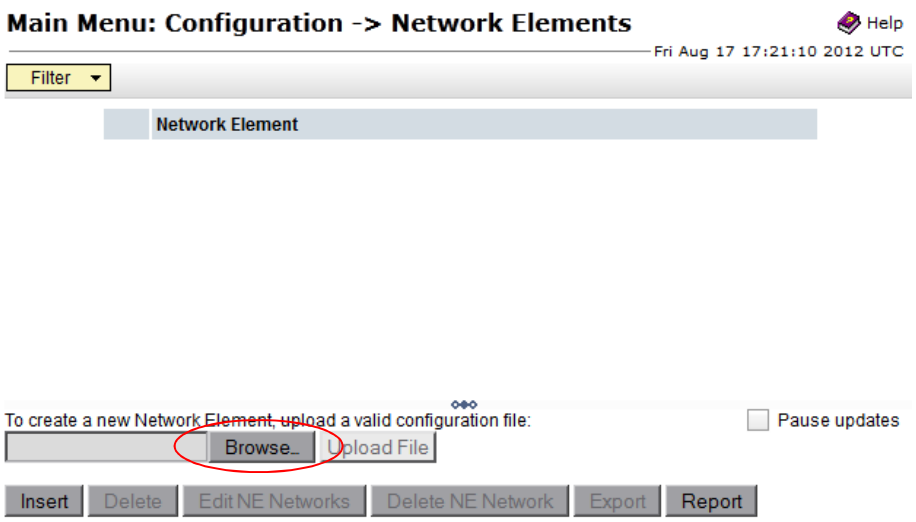
Procedure 13: Configuring HLRR NOAM-A Server (1st NOAM site only)

Step	Procedure	Result
1. ☐	**NOAM-A Server:** Connect to the HLRR GUI.	Execute **Appendix C**: Establishing a Local Connection for Accessing HLRR GUI.

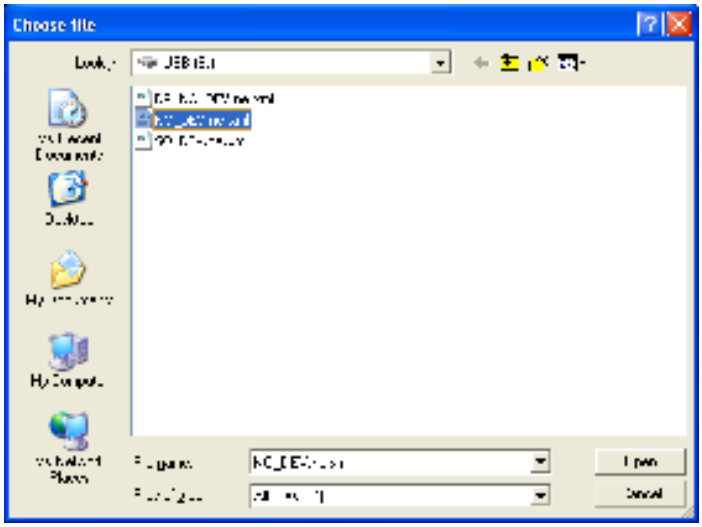
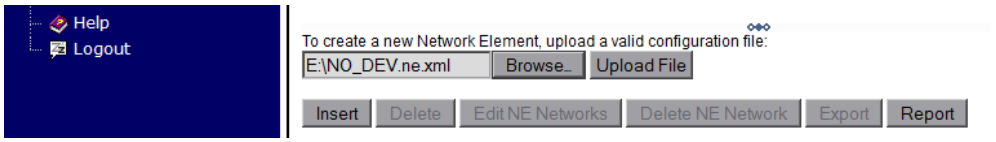
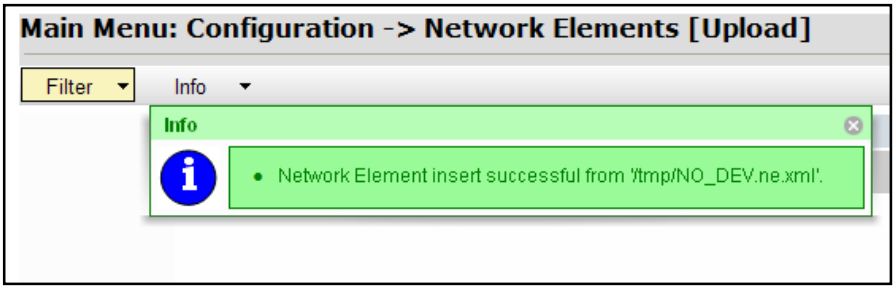
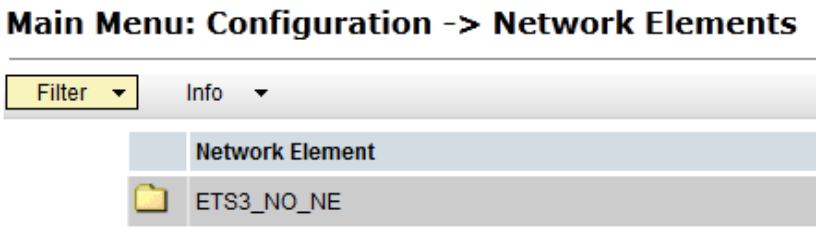
Procedure 13: Configuring HLRR NOAM-A Server (1st NOAM site only)

Step	Procedure	Result
2. ☐	**NOAM-A GUI:** Launch an approved web browser and connect to the NOAM-A Server's IP address **NOTE:** If presented with the "security certificate" warning screen shown to the right, choose the following option: **"Continue to this website (not recommended)".**	
3. ☐	**NOAM-A GUI:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	
4. ☐	**NOAM-A GUI:** The user should be presented the HLRR Main Menu as shown on the right.	

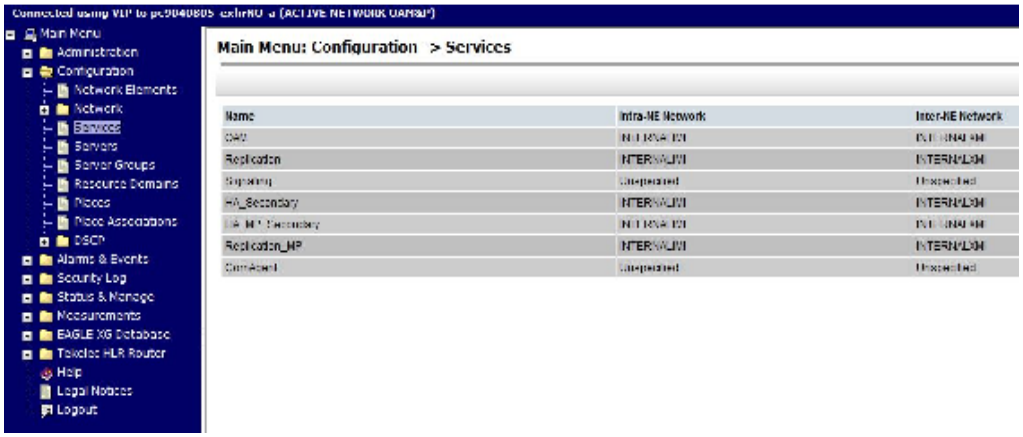
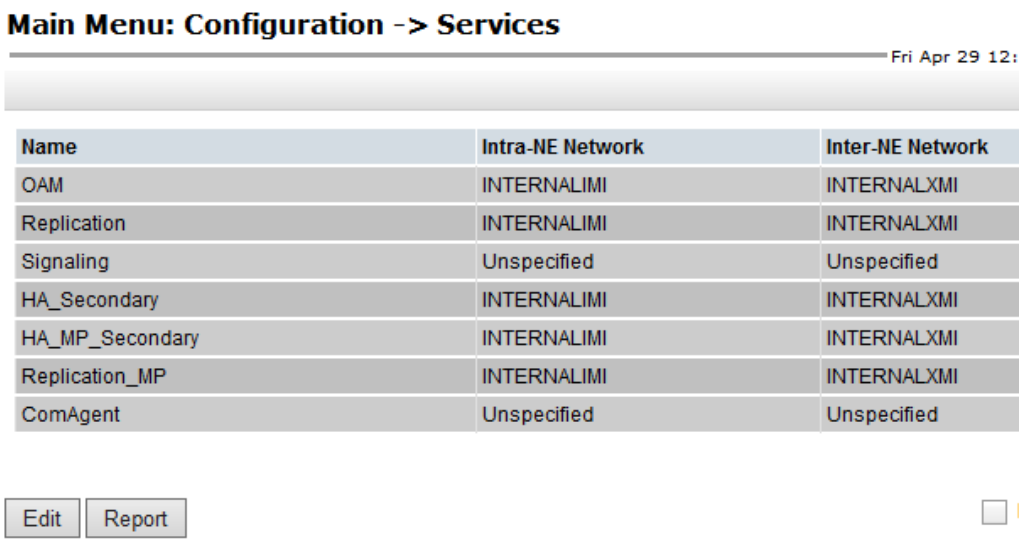
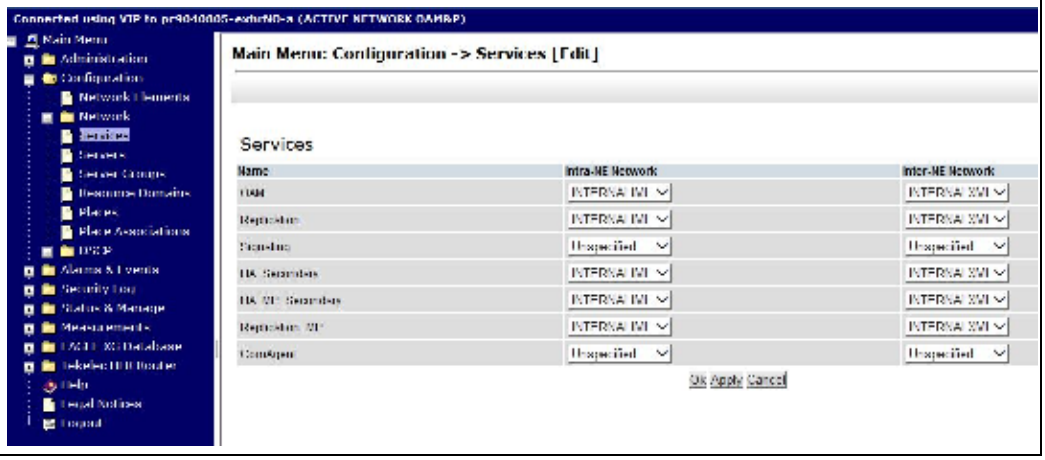
Procedure 13: Configuring HLRR NOAM-A Server (1st NOAM site only)

Step	Procedure	Result
5. ☐	**NOAM-A GUI:** *Configuring Network Element* Select… **Main Menu** → **Configuration** → ***Network Elements***	
6. ☐	**NOAM-A GUI:** From the **Configuration / Network Elements** screen… Select the **"Browse"** dialogue button (scroll to bottom left corner of screen).	

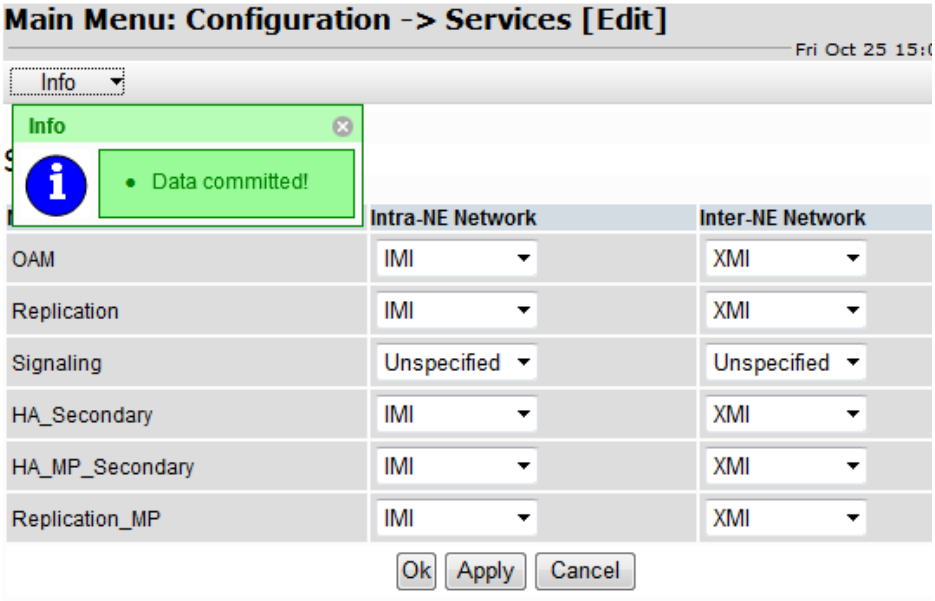
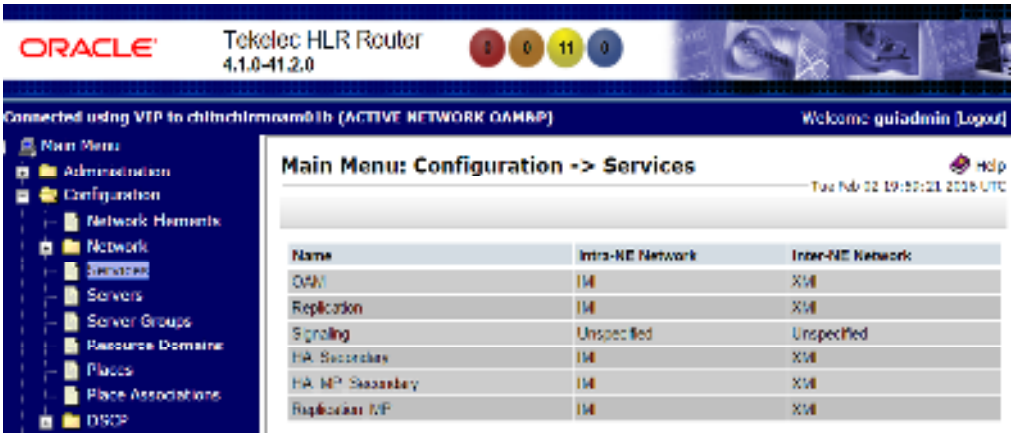
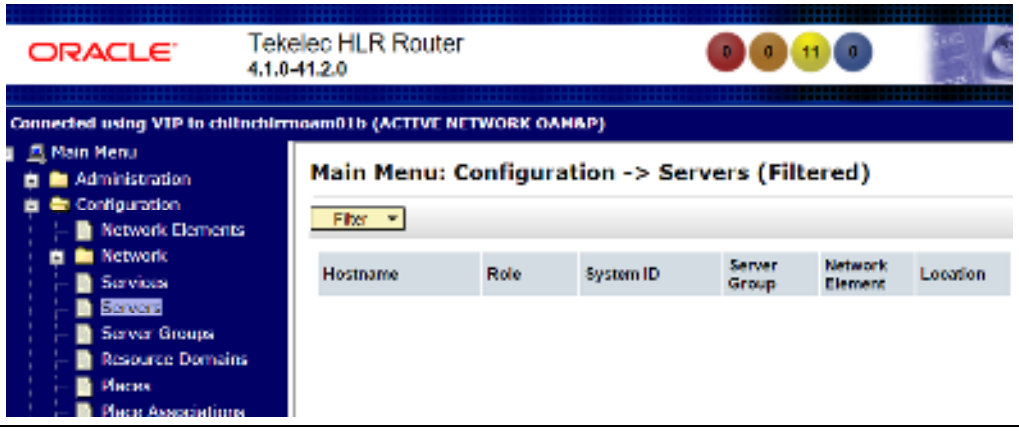
Procedure 13: Configuring HLRR NOAM-A Server (1st NOAM site only)

Step	Procedure	Result
7. ☐	**NOAM-A GUI:** **Note**: This step assumes that the **xml** files were previously prepared, as described in Appendix D. **1)** Select the location containing the site **.xml** file. **2)** Select the **.xml** file and click the **"Open"** dialogue button.	
8. ☐	**NOAM-A GUI:** Select the **"Upload File"** dialogue button (bottom left corner of screen).	
9. ☐	**NOAM-A GUI:** If the values in the **.xml** file pass validation rules, the user receives a banner information message showing that the data has been successfully committed to the DB. **Note:** *You may have to left mouse click the **"Info"** banner option in order to see the banner output.*	 
10. ☐	**Repeat steps 5 - 9 for the SOAM Network Element File.**	
11. ☐	**Optional**: **Repeat steps 5 - 9 for the DR NOAM and DR SOAM Network Element files.**	

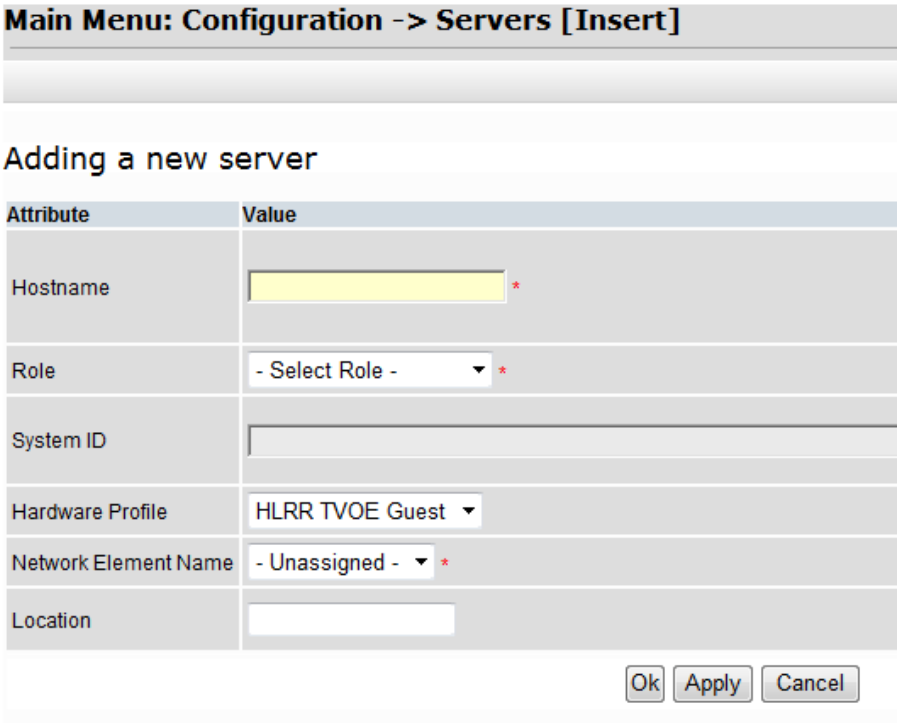
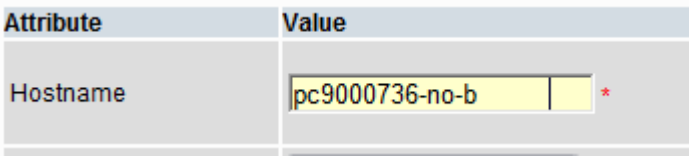
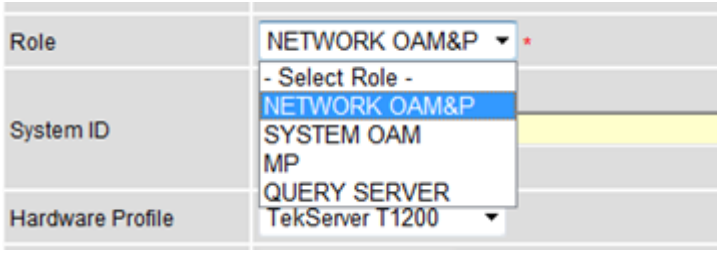
Procedure 13: Configuring HLRR NOAM-A Server (1st NOAM site only)

Step	Procedure	Result
12. ☐	**NOAM-A GUI:** *Configuring Services* Select… **Main Menu** → **Configuration** → ***Services***	
13. ☐	**NOAM-A GUI:** **1)** The user will be presented with the "**Services**" configuration screen as shown on the right. **2)** Select the **"Edit"** dialogue button.	
14. ☐	**NOAM-A GUI:** **1)** Set the services values as shown on the right. **2)** Select the **"Apply"** dialogue button.	

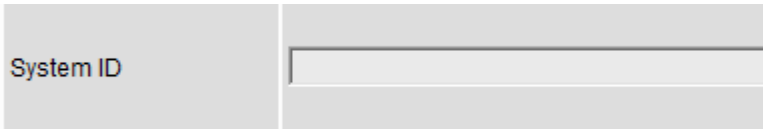
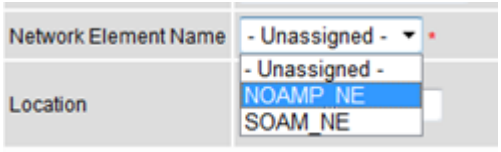
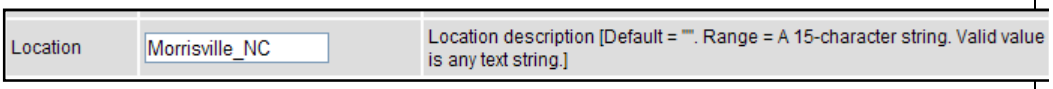
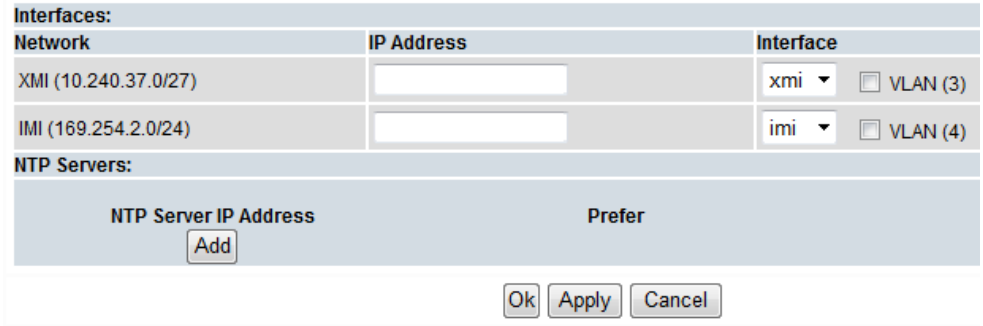
Procedure 13: Configuring HLRR NOAM-A Server (1st NOAM site only)

Step	Procedure	Result
15. ☐	**NOAM-A GUI:** **1)** The user should be presented with a banner information message stating **"Data committed"** **2)** Select the **"Ok"** dialogue button.	
16. ☐	**NOAM-A GUI:** The user will be presented with the "**Services**" configuration screen as shown on the right	
17. ☐	**NOAM-A GUI:** *Configuring HLRR Server* Select… **Main Menu** → **Configuration** → ***Servers***	

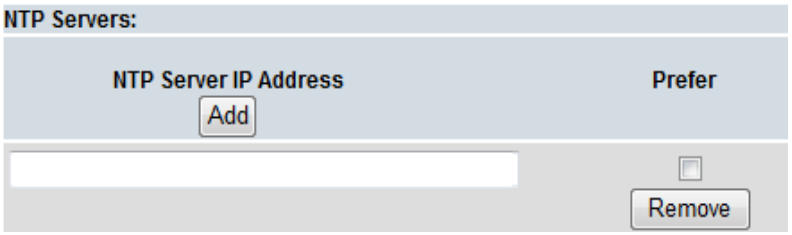
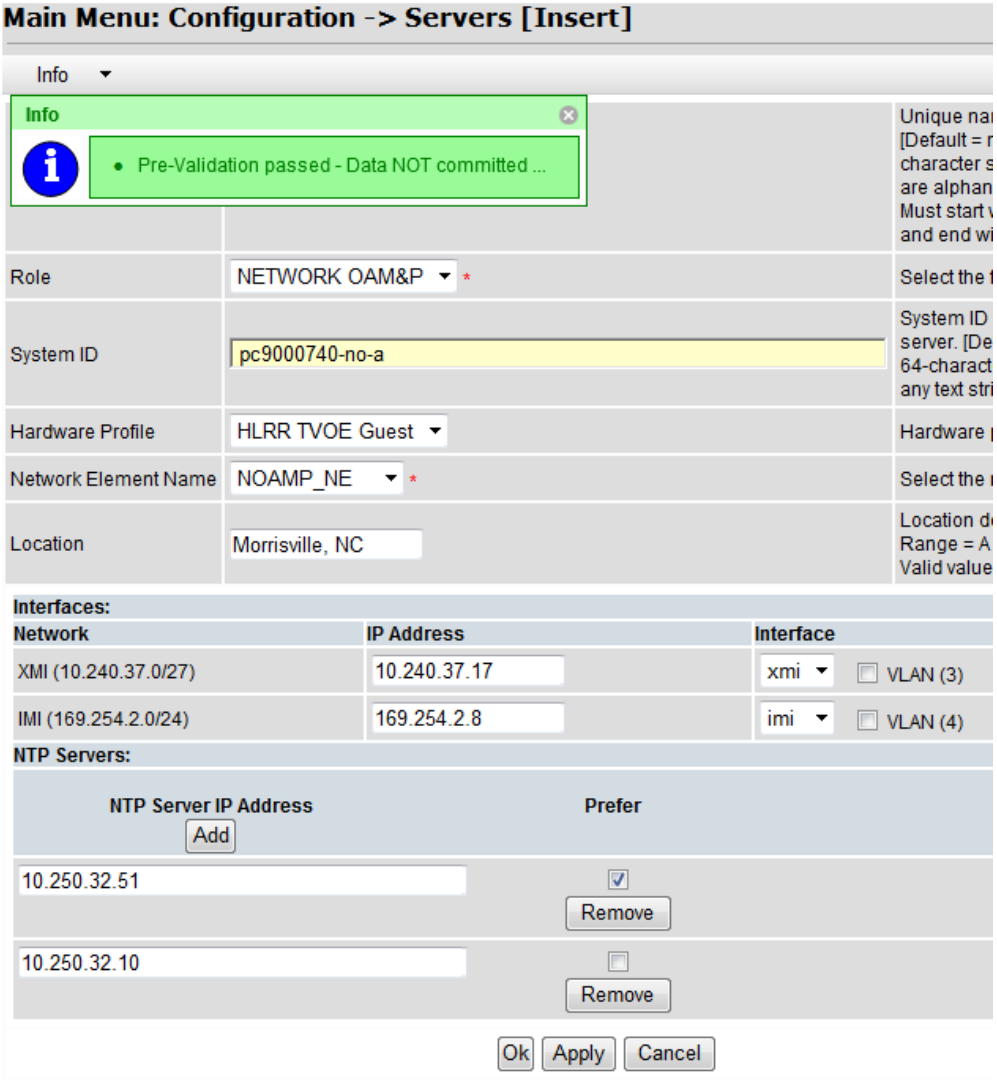
Procedure 13: Configuring HLRR NOAM-A Server (1st NOAM site only)

Step	Procedure	Result
18. ☐	**NOAM-A GUI:** Select the **"Insert"** dialogue button.	
19. ☐	**NOAM-A GUI:** The user is now presented with the **"Server [Insert]"** configuration screen.	
20. ☐	**NOAM-A GUI:** Input the assigned "**hostname**" for the NOAM-A Server. See NAPD document for this information.	
21. ☐	**NOAM-A GUI:** Select **"NETWORK OAM&P"** for the server **"Role"** from the pull-down menu.	

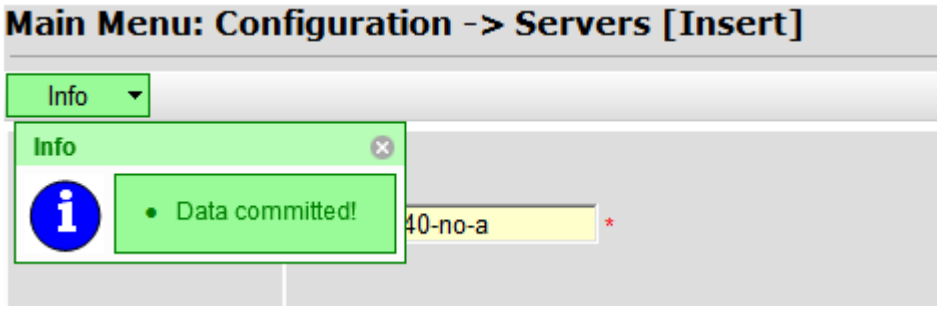
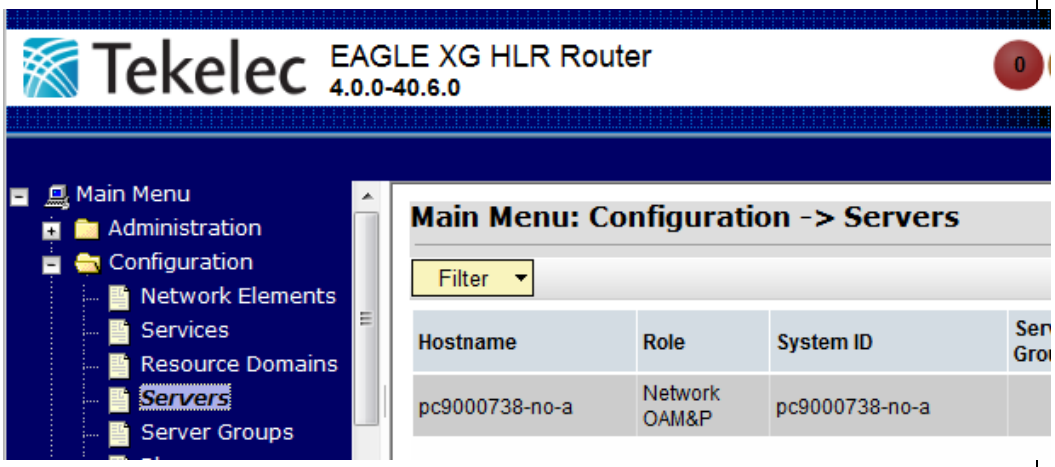
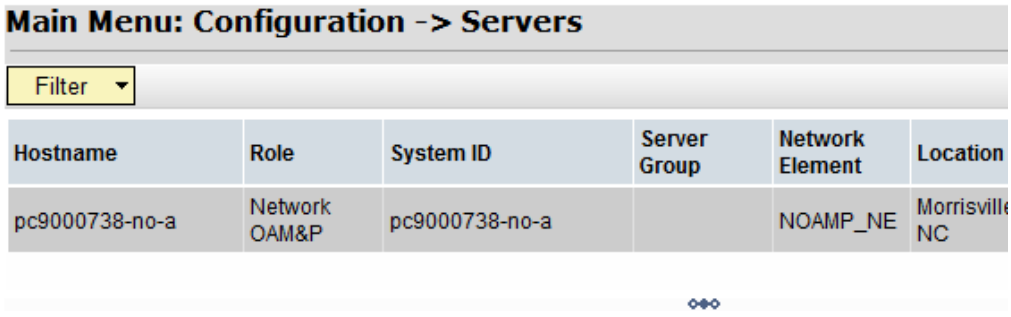
Procedure 13: Configuring HLRR NOAM-A Server (1st NOAM site only)

Step	Procedure	Result
22. ☐	**NOAM-A GUI:** **Optional:** Input the assigned "**System ID**"	
23. ☐	**NOAM-A GUI:** Select "**HLRR TVOE Guest**" for the **Hardware Profile** from the pull-down menu.	
24. ☐	**NOAM-A GUI:** Select the **Network Element Name** from the pull-down menu.	 **NOTE:** *After the Network Element Name is selected, the Interfaces fields will be displayed, as seen in* **Step 26**
25. ☐	**NOAM-A GUI:** Enter the site location. **NOTE:** *Location is an optional field.*	
26. ☐	**NOAM-A GUI:** **1)** Enter the **XMI** and **IMI** IP addresses for the **HLRR NOAM-A Server**. Refer to the NAPD documentation for this information. **2)** Set the **XMI** and **IMI Interfaces** to "**xmi**" and "**imi**", respectively. **3) DO NOT** check any **VLAN** box.	

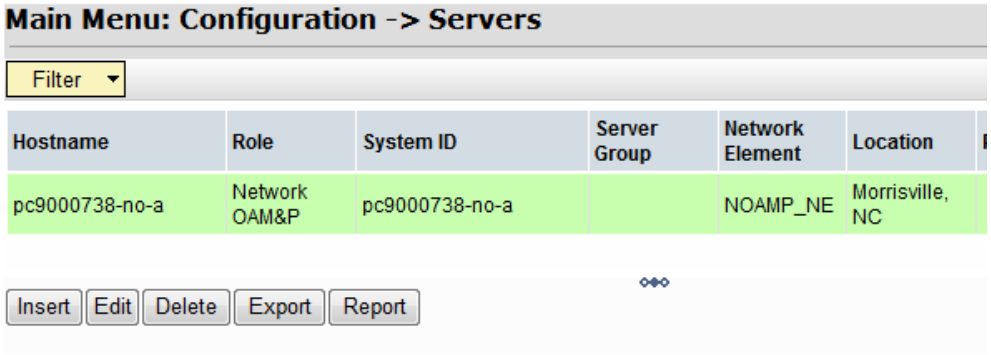
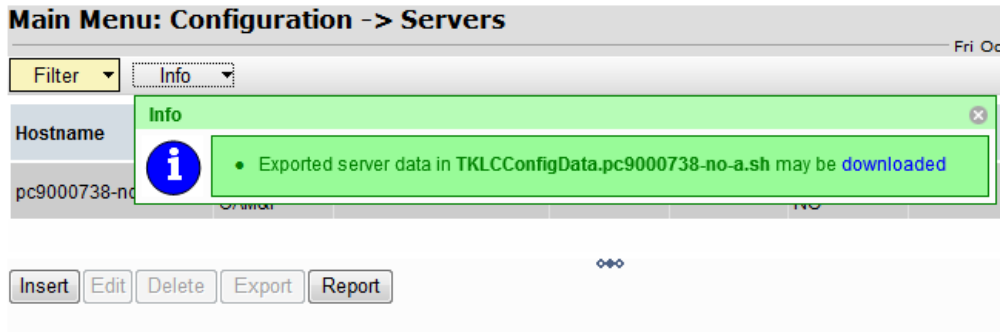
Procedure 13: Configuring HLRR NOAM-A Server (1st NOAM site only)

Step	Procedure	Result
27. ☐	**NOAM-A GUI:** **1)** Click **Add** button and assign the IP address for the **NTP Server.** **2)** Click on check box to select preferred NTP Server.	 **This should be the XMI address of the TVOE server hosting this VM Guest.** **Only one NTP server should be entered per guest.** **See paragraph 4.4 NTP Strategy for more information on NTP deployment.**
28. ☐	**NOAM-A GUI:** **1)** The user should be presented with a banner information message stating **"Pre-Validation passed"**. **2)** Click the **"OK"** button.	

Procedure 13: Configuring HLRR NOAM-A Server (1st NOAM site only)

Step	Procedure	Result
29. ☐	**NOAM-A GUI:** *If the values provided match the network ranges assigned to the HLRR NE, the user will receive a banner information message showing that the data has been validated and committed to the DB.*	
30. ☐	**NOAM-A GUI:** *Applying the HLRR Server Configuration File* Select… **Main Menu** → **Configuration** → ***Servers***	
31. ☐	**NOAM-A GUI:** The **"Configuration →Servers" screen** should now show the newly added **HLRR Server** in the list.	

Procedure 13: Configuring HLRR NOAM-A Server (1st NOAM site only)

Step	Procedure	Result
32. ☐	**NOAM-A GUI:** **1)** Use the cursor to select the **HLRR Server** entry The row containing the desired **HLRR Server** should now be highlighted in **GREEN**. **2)** Select the **"Export"** dialogue button.	
33. ☐	**NOAM-A GUI:** The user will receive a banner information message showing a download link for the **HLRR Server** configuration data.	 The configurationt file was created and stored in the /var/TKLC/db/filemgmt directory. The configuration file will have a file name like TKLCConfigData.<***hostname***>.sh.
34. ☐	**PMAC Server:** Connect to the PMAC Server Console.	Connect to the PMAC server's console using one of the access methods described in **Section 2.3.** Use the PMAC_Management_ip_address.
35. ☐	**PMAC Server:** **1)** Access the command prompt. **2)** Log into the PMAC server as the "**admusr**" user.	login as: admusr admusr@10.250.xx.yy's password: **<admusr_password>** Last login: Mon Jul 30 10:33:19 2012 from 10.25.80.199 [admusr@pmac-pc9000738 ~]$

Procedure 13: Configuring HLRR NOAM-A Server (1st NOAM site only)

Step	Procedure	Result
36. ☐	**PMAC Server:** SSH into the NOAM-A server using the Control IP Address	Using an SSH client such as putty, ssh to the NOAM-A server using admusr credentials and the <NOAM-A Control IP Address> from list in, Procedure 12: Create, IPM and Install Application on all Virtual Machines, step 13. [admusr@pmac-pc9000738 ~]$ ssh 192.168.1.xx admusr@192.168.1.6's password: **<admusr_password>**
37. ☐	**NOAM-A Server:** Output similar to that shown on the right will appear as the server access the command prompt.	***** TRUNCATED OUTPUT ***** VPATH=/var/TKLC/rundb:/usr/TKLC/appworks:/usr/TKLC/awpcommon:/usr/TKLC/awptransportmgr:/usr/TKLC/awpss7 PRODPATH=/opt/comcol/prod VPATH=/opt/TKLCcomcol/runcm6.2:/opt/TKLCcomcol/cm6.2 PRODPATH= RELEASE=6.2 VPATH=/var/TKLC/rundb:/usr/TKLC/appworks:/usr/TKLC/awpcommon:/usr/TKLC/awptransportmgr:/usr/TKLC/awpss7:/usr/TKLC/exhr PRODPATH=/opt/comcol/prod RUNID=00 [admusr@hostname1382738107 ~]$
38. ☐	**NOAM-A Server:** Copy the **server** configuration file to the **"/var/tmp"** directory on the server, making sure to rename the file by omitting the server hostname from the file name. **NOTE:** *The server will poll the **/var/tmp** directory for the presence of the configuration file and automatically execute it when found.*	***Example:*** TKLCConfigData<.**server_hostname**>.sh ➔ will translate to ➔TKLCConfigData.sh $ **sudo cp –p /var/TKLC/db/filemgmt/TKLCConfigData.pc9000738-no-a.sh /var/tmp/TKLCConfigData.sh**

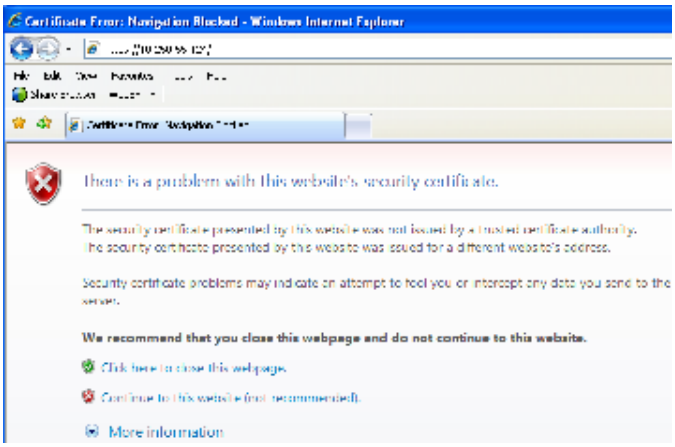
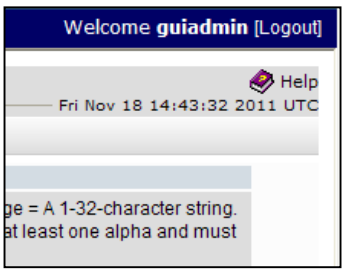
Procedure 13: Configuring HLRR NOAM-A Server (1st NOAM site only)

Step	Procedure	Result
39. ☐	**NOAM-A Server:** After the configuration script completes, a broadcast message will be sent to the terminal window.	***** NO OUTPUT FOR ≈ 3-10 MINUTES ***** Broadcast message from admusr@pc9000738-no-a (Fri Oct 25 19:16:09 2013): **Server configuration completed successfully!** See /var/TKLC/appw/logs/Process/install.log for details. Please remove the USB flash drive if connected and reboot the server. Ignore the output shown and press the **<ENTER>** key to return to the command prompt. **NOTE:** *The user should be aware that the time to complete this step varies by each server and may take from 3-10 minutes to complete.*
40. ☐	**NOAM-A Server:** Configure the time zone	**Note:** The following command example uses the GMT time zone. Replace, as appropriate, with the time zone you have selected for this installation. See **Appendix E** for a list of valid time zones. **$ sudo set_ini_tz.pl "Etc/UTC"**
41. ☐	**NOAM-A Server:** Initiate a reboot of the **HLRR NOAM-A Server**.	**$ sudo init 6**
42. ☐	**PMAC Server:** The SSH session for the NOAM-A server is terminated by previous step.	The previous step should cause the ssh session to the NOAM-A Server to close and user should return to the PMAC server console prompt. The user should see output similar to the below output: Connection to 192.168.1.x closed by remote host. Connection to 192.168.1.x closed.
43. ☐	**PMAC Server:** Wait until server reboot is done. Then, SSH into the NOAM-A server using the XMI IP Address.	Wait about 5 minutes until the server reboot is done. Using an SSH client such as putty, ssh to the NOAM-A server using admusr credentials and the <NOAM-A_XMI IP Address> **$ ssh 10.240.241.xx** admusr@10.240.241.xx's password: **<admusr_password>** Note: If the server isn't up, wait a few minutes and re-enter the ssh command. You can also try running the "ping 10.240.241.xx" command to see if the server is up.

Procedure 13: Configuring HLRR NOAM-A Server (1st NOAM site only)

Step	Procedure	Result
44. ☐	**NOAM-A Server:** Use the **"ntpq"** command to verify that the server has connectivity to the assigned NTP server.	$ **ntpq -np** remote refid st t when poll reach delay offset jitter ========== *10.240.241.105 192.5.41.209 2 u 651 1024 377 0.339 0.583 0.048 **Note:** It may take a few minutes for the NTP server to connect and sync with the VM.
45. ☐	**NOAM-A Server:** Verify the health of the server.	Execute the following command on the server and make sure that no errors are returned: **$ sudo 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
	**IF CONNECTIVITY TO THE NTP SERVER(S) CANNOT BE ESTABLISHED, STOP AND EXECUTE THE FOLLOWING STEPS:** • Have the customer's IT group provide a network path from the OAM server IP to the assigned NTP IP addresses. **ONCE NETWORK CONNECTIVITY IS ESTABLISHED TO THE NTP IP ADDRESSES, REPEAT STEP 44**	
46. ☐	**NOAM Server A:** Execute **"alarmMgr"** to verify the current health of the server	$ **alarmMgr --alarmStatus** NOTE: This command should return no output on a healthy system. If any alarms are reported as SNMP traps, please contact Oracle's Customer Care Center for assistance.
47. ☐	**NOAM Server A:** Exit the SSH session for the NOAM-A server	$ **exit**

Procedure 13: Configuring HLRR NOAM-A Server (1st NOAM site only)

Step	Procedure	Result
48. ☐	**NOAM-A GUI:** Verify that you can log back into the GUI. **NOTE:** *If presented with the "security certificate" warning screen shown to the right,* ***choose the following option:*** ***"Continue to this website (not recommended)".***	Launch an approved web browser and connect to the NOAM-A Server's IP address. 
49. ☐	**NOAM-A GUI:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	
50. ☐	**NOAM-A GUI:** Click the **"Logout"** link on the HLRR server GUI.	
THIS PROCEDURE HAS BEEN COMPLETED		

7.2 Configure Remaining HLRR Servers (All Sites)

This procedure is used to create and configure all HLRR Servers except the first NOAM-A server.

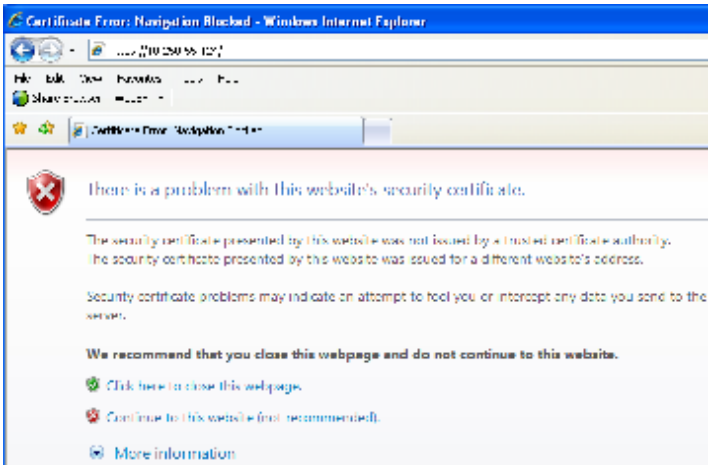
Requirements:

- **Procedure 12: Create, IPM and Install Application on all Virtual Machines** has been completed on all servers.
- **Procedure 13: Configuring HLRR NOAM-A Server (1st NOAM site only)** 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 MY ORACLE SUPPORT AND ASK FOR ASSISTANCE.

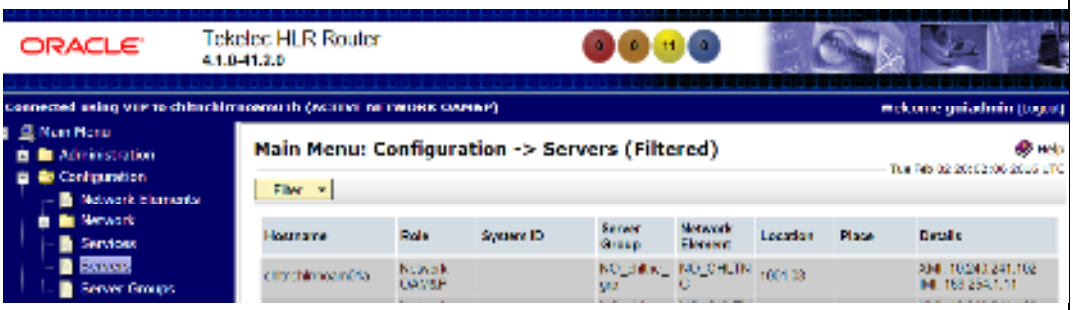
Procedure 14: Configuring Remaining HLRR Servers

Step	Procedure	Result
1. ☐	**NOAM-A GUI:** Launch an approved web browser and connect to NOAM-A's IP address	
2. ☐	**NOAM-A GUI:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	

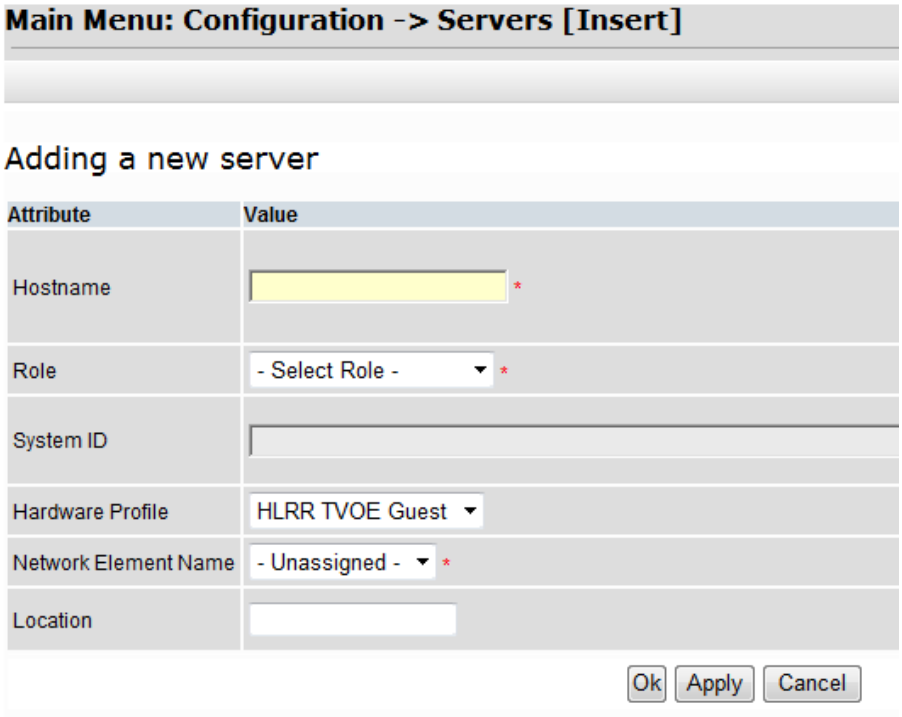
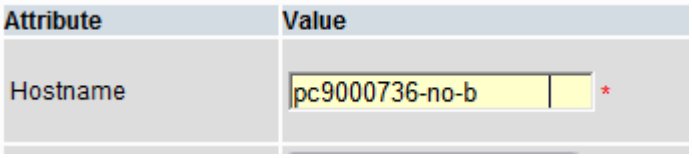
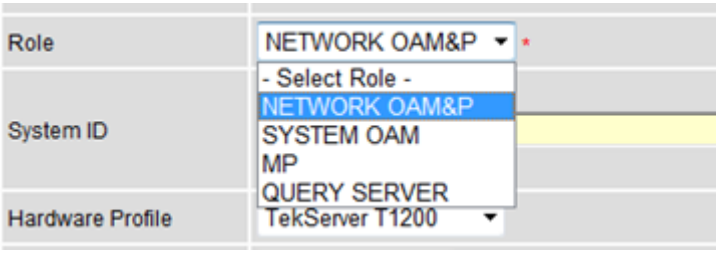
Procedure 14: Configuring Remaining HLRR Servers

Step	Procedure	Result
3. ☐	**NOAM-A GUI:** The user should be presented the HLRR Main Menu as shown on the right.	
Note: The following steps need to run on all servers EXCEPT the first NOAM-A server.		

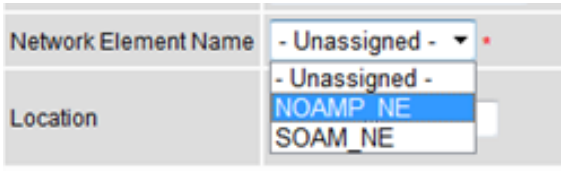
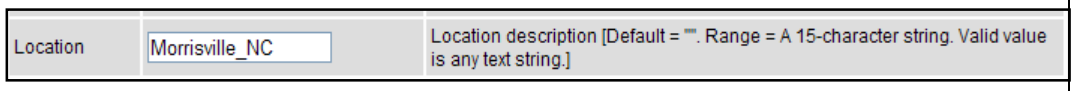
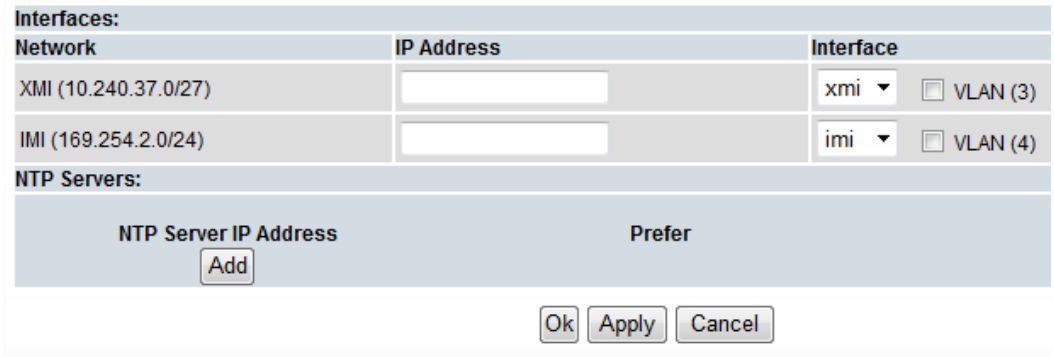
Procedure 14: Configuring Remaining HLRR Servers

Step	Procedure	Result
4. ☐	**NOAM-A GUI:** Select… **Main Menu** → **Configuration** → ***Servers***	 • **"Check off"** the associated **Check Box** as each server is completed. **Primary Site:** ☐ NOAM-B ☐ SOAM-A ☐ SOAM-B ☐ QS-1 ☐ MP-1 ☐ MP-2 ☐ MP-3 ☐ MP-4 ☐ MP-5 **Disaster Recovery Site (Optional):** ☐ DR-NOAM-A ☐ DR-NOAM-B ☐ SOAM-A ☐ SOAM-B ☐ QS-1 ☐ MP-1 ☐ MP-2 ☐ MP-3 ☐ MP-4 ☐ MP-5
5. ☐	**NOAM-A GUI:** Select the **"Insert"** dialogue button.	

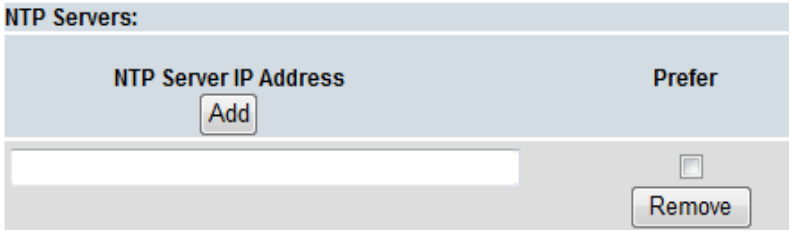
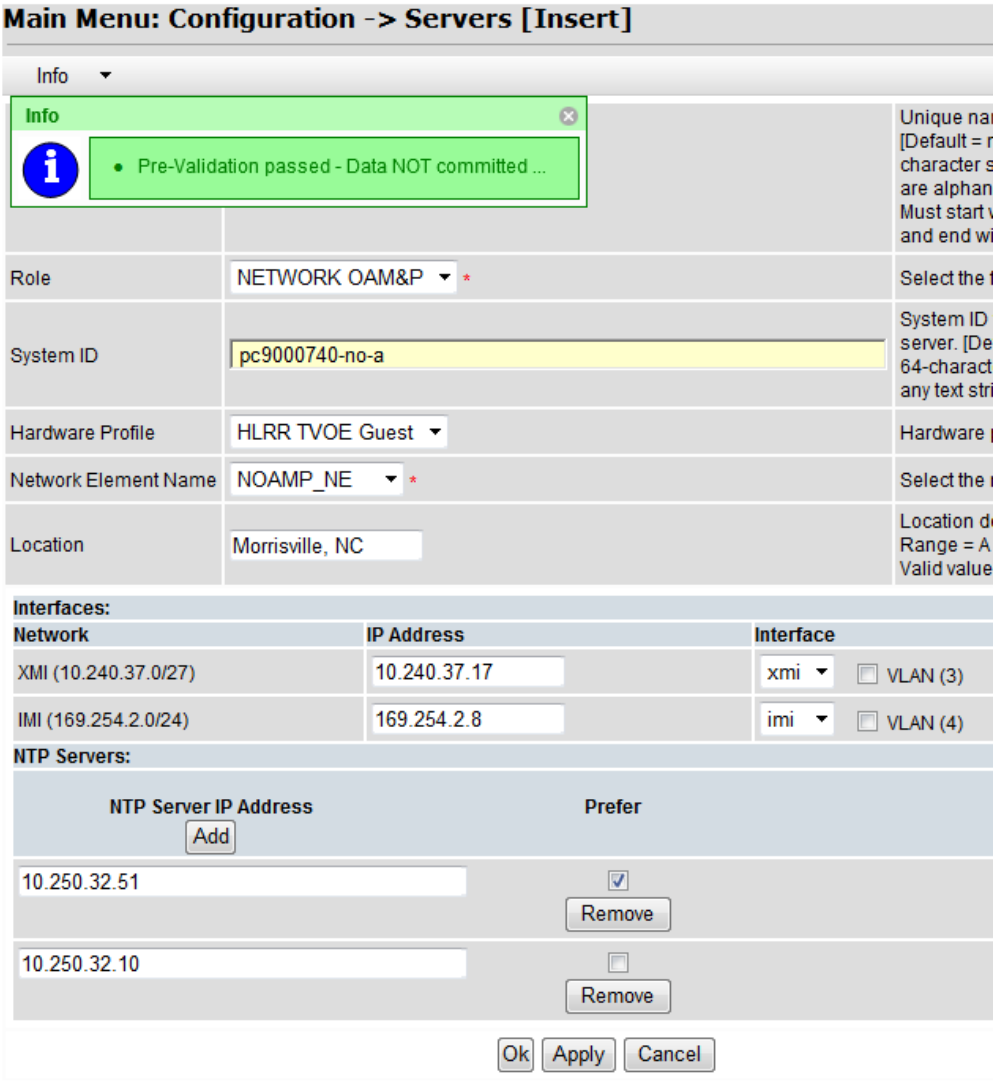
Procedure 14: Configuring Remaining HLRR Servers

Step	Procedure	Result
6. ☐	**NOAM-A GUI:** The user is now presented with the **"Server [Insert]"** configuration screen.	
7. ☐	**NOAM-A GUI:** Input the assigned "**hostname"** for the server. Refer to the NAPD documentation for this information.	
8. ☐	**NOAM-A GUI:** Select the appropriate server **"Role"** from the pull-down menu for the type of server you are adding.	
9. ☐	**NOAM-A GUI:** Optional: Input the assigned "**System ID**"	

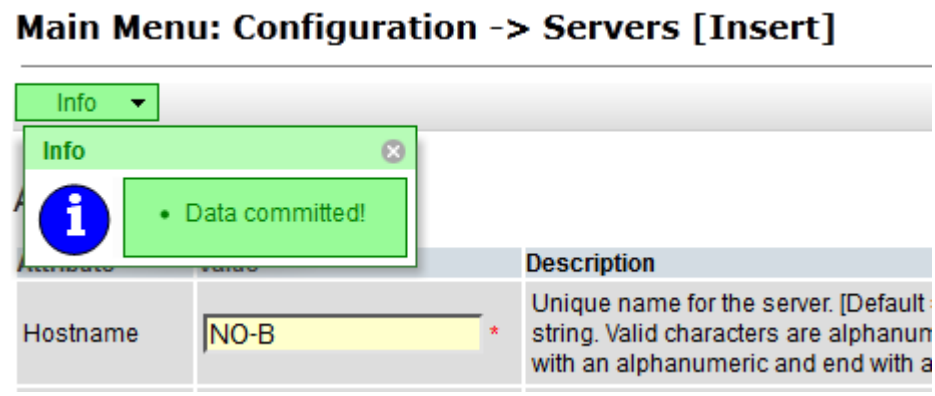
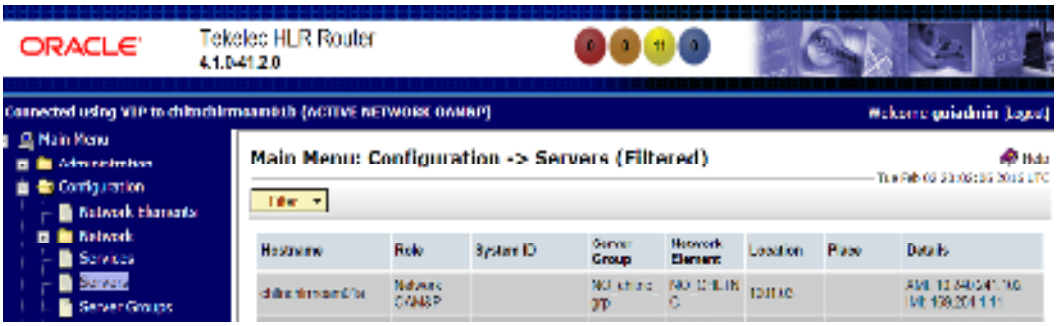
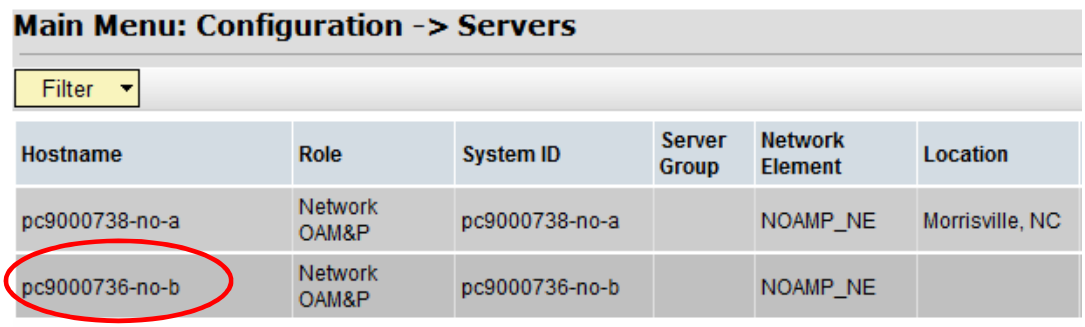
Procedure 14: Configuring Remaining HLRR Servers

Step	Procedure	Result
10. ☐	**NOAM-A GUI:** Select "**HLRR TVOE Guest**" for the **Hardware Profile** from the pull-down menu.	
11. ☐	**NOAM-A GUI:** Select the correct **Network Element Name** from the pull-down menu.	 **NOTE**: *The above picture shows the "NOAM" NE and SOAM NE. Select the appropriate Network Element Name for the server being created. All of the SOAM and MP servers at a site should use the SOAM NE.* *Disaster Recovery Site servers should use their own unique "NOAM" NE and SOAM NEs.* *After the Network Element Name is selected, the Interfaces fields will be displayed, as seen in* **Step 13**
12. ☐	**NOAM-A GUI:** Enter the site location. **NOTE:** *Location is an optional field.*	
13. ☐	**NOAM-A GUI:** **1)** Enter the **XMI** and **IMI** IP addresses for the **HLRR Server**. Refer to the NAPD documentation for this information. **2)** Set the **XMI** and **IMI Interfaces** to "**xmi**" and "**imi**", respectively. **3) DO NOT** check any **VLAN** box.	

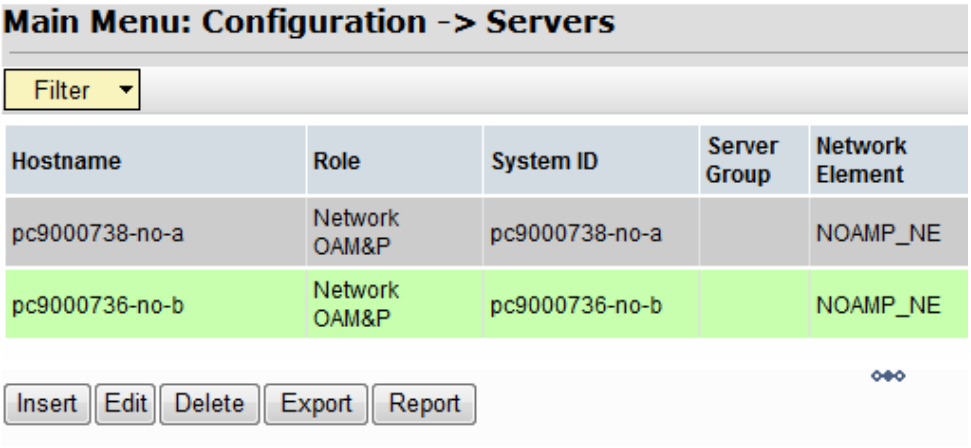
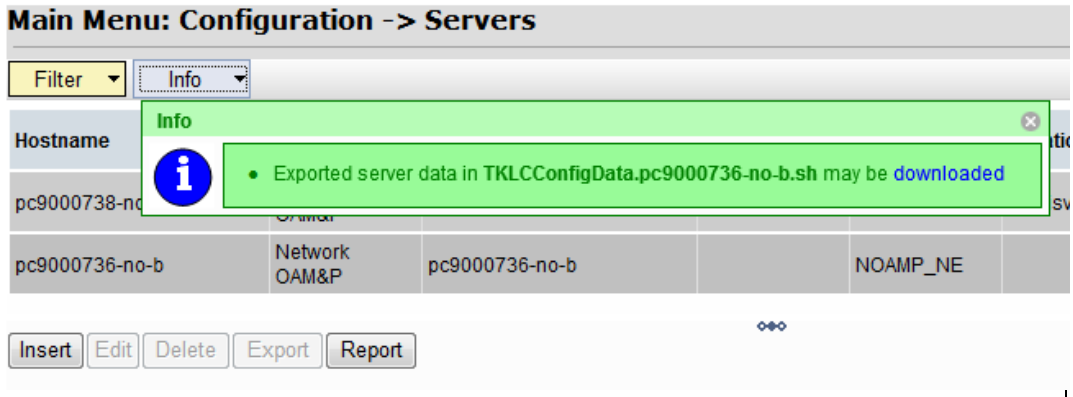
Procedure 14: Configuring Remaining HLRR Servers

Step	Procedure	Result
14. ☐	**NOAM-A GUI:** **1)** Click **Add** button and assign the IP address for the **NTP Server.** **2)** Click on check box to select preferred NTP Server.	 **This should be the XMI address of the TVOE host of the server.** **Only one NTP server should be entered per server.** **See paragraph 4.4 NTP Strategy for more information on NTP deployment.**
15. ☐	**NOAM-A GUI:** **1)** The user should be presented with a banner information message stating **"Pre-Validation passed"**. **2)** Click the **"OK"** dialogue button.	

Procedure 14: Configuring Remaining HLRR Servers

Step	Procedure	Result
16. ☐	**NOAM-A GUI:** If the values provided match the network ranges assigned to the HLRR NE, the user will receive a banner information message showing that the data has been validated and committed to the DB.	
17. ☐	**NOAM-A GUI:** *Applying the HLRR Server Configuration File* **Main Menu** → **Configuration** → ***Servers***	
18. ☐	**NOAM-A GUI:** The **"Configuration →Servers" screen** should now show the newly added **HLRR Server** in the list.	

Procedure 14: Configuring Remaining HLRR Servers

Step	Procedure	Result
19. ☐	**NOAM-A GUI:** **1)** Use the cursor to select the **HLRR Server** entry added in **Steps** 6 through 16 The row containing the desired **HLRR Server** should now be highlighted in **GREEN**. **2)** Select the **"Export"** dialogue button.	
20. ☐	**NOAM-A GUI:** The user will receive a banner information message showing a download link for the configuration data.	 The configuration file is created and stored in the /var/TKLC/db/filemgmt directory on the primary NOAM-A server. The configuration file will have a file name like TKLCConfigData.<***hostname***>.sh
21. ☐	**NOAM-A Server:** Connect to the NOAM-A Server Console at the Primary NOAM site	Connect to the NOAM-A server's console using one of the access methods described in **Section 2.3.** Use the Primary NOAM-A XMI IP address that was entered in **Procedure 12:** Create, IPM and **Install Application on all Virtual Machines**, Step 26

Procedure 14: Configuring Remaining HLRR Servers

Step	Procedure	Result
22. ☐	**NOAM-A Server:** **1)** Access the command prompt. **2)** Log into the Primary NOAM-A server as "**admusr**".	login as: admusr admusr@10.250.xx.yy's password: **<admusr_password>** Last login: Mon Jul 30 10:33:19 2012 from 10.25.80.199
23. ☐	**NOAM-A Server:** Output similar to that shown on the right will appear as the server access the command prompt.	***** TRUNCATED OUTPUT ***** VPATH=/var/TKLC/rundb:/usr/TKLC/appworks:/usr/TKLC/awpcommon:/usr/TKLC/awptransportmgr:/usr/TKLC/awpss7 PRODPATH=/opt/comcol/prod VPATH=/opt/TKLCcomcol/runcm6.2:/opt/TKLCcomcol/cm6.2 PRODPATH= RELEASE=6.2 VPATH=/var/TKLC/rundb:/usr/TKLC/appworks:/usr/TKLC/awpcommon:/usr/TKLC/awptransportmgr:/usr/TKLC/awpss7:/usr/TKLC/exhr PRODPATH=/opt/comcol/prod RUNID=00 [admusr@pc9000738-no-a ~]$

24. ☐	**NOAM-A Server:**
	Change directory to the filemgmt directory and verify that the configuration file is in the filemgmt directory.
		[admusr@pc9000738-no-a ~]$ **cd /var/TKLC/db/filemgmt**
		[admusr@pc9000738-no-a filemgmt]$ **ls –ltr TKLCConfigData*.sh**
		`-rw-rw-rw- 1 root root 3570 Aug 17 14:01 TKLCConfigData.pc9000738-so-a.sh`
		`-rw-rw-rw- 1 root root 3570 Aug 17 14:30 TKLCConfigData.pc9000736-so-b.sh`
		
		Verify that the configuration file was created and stored in the /var/TKLC/db/filemgmt directory on the primary NOAM-A server. The configuration file will have a file name like TKLCConfigData.<***hostname***>.sh.

25. ☐	**NOAM-A Server:** Copy the configuration files found in the previous step to the "tmp" directory on the PM&C. server that manages the desired server.	**Note:** The below example shows copying 2 files. Any number of configuration files can be copied in one step. [admusr@pc9040833-no-a filemgmt]$ **sudo scp -p <configuration_file-a> <configuration_file-b> admusr@<Desired_PMAC_IP>:/tmp** admusr@10.240.39.4's password:**<admusr_password>** TKLCConfigData.pc9000738-so-a.sh 100% 1741 1.7KB/s 00:00 TKLCConfigData.pc9000736-so-b.sh 100% 1741 1.7KB/s 00:00 [admusr@pc9040833-no-a filemgmt]$

Procedure 14: Configuring Remaining HLRR Servers

Step	Procedure	Result
26. ☐	**PMAC Console:** Connect to the PMAC Server Console that manages the desired server using admusr.	Open a ssh terminal session using putty to the PMAC that manages the desired server. Use the PMAC_Management Server's IP Address that was entered in *Procedure 4: PMAC Deployment, Step 3*.
27. ☐	**PMAC Console:** Copy the server configuration file to the Control IP for the desired server	**Note:** The Control IPs are listed in, *Procedure 12: Create, IPM and Install Application on all Virtual Machines, Step 13*. The name of the configuration file varies for each server. The output is just an example. admusr@pmac ~]$ **sudo scp -p /tmp/<Desired Server_configuration_file> admusr@<Desired_Server_Control_IP>:/tmp/** admusr@192.168.1.10's password:**<admusr_password>** TKLCConfigData.pc9000738-so-a.sh 100% 1741 1.7KB/s 00:00 [admusr@pmac ~]$
28. ☐	**PMAC Console:** Connect to the desired server console from the PM&C Server Console.	SSH to the desired server console from the PMAC console using the Control IP. **Note:** The Control IPs are listed in, *Procedure 12: Create, IPM and Install Application on all Virtual Machines, Step 13*. admusr@pmac ~]$ **ssh <desired_server_control_ip>** admusr@192.168.1.10's **<admusr_password>**
29. ☐	**Desired Server:** Copy the server configuration file to the "/var/tmp" directory on the desired server, making sure to rename the file by omitting the server hostname from the file name.	Copy the server configuration file to the "/var/tmp" directory on the server, making sure to rename the file by omitting the server hostname from the file name. Example: TKLCConfigData<.server_hostname>.sh > will translate to > TKLCConfigData.sh [admusr@192.168.1.10 ~]$ **sudo cp -p /tmp/TKLCConfigData.pc9000738-so-a.sh /var/tmp/TKLCConfigData.sh** **Note:** The server will poll the /var/tmp directory for the presence of the configuration file and automatically execute it when found.

Procedure 14: Configuring Remaining HLRR Servers

Step	Procedure	Result
30. ☐	**Desired Server:** After the script completes, a broadcast message will be sent to the terminal. **Note:** The user should be aware that the time to complete this step varies by server and may take from 3-10 minutes to complete.	***** NO OUTPUT FOR ≈ 3-10 MINUTES ***** *Broadcast message from admusr (Thu Dec 1 09:41:24 2011):* *Server configuration completed successfully!* *See /var/TKLC/appw/logs/Process/install.log for details.* *Please remove the USB flash drive if connected and reboot the server.* Ignore the output shown and press the **<ENTER>** key to return to the command prompt. [admusr@ pc9000738-so-a~]$
31. ☐	**Desired Server:** Verify config script was successful and Reboot the Server	Verify the config script was successful by checking the following file: **$ sudo cat /var/TKLC/appw/logs/Process/install.log** Verify the following message is displayed: `[SUCCESS] script completed successfully!` Now Reboot the Server: **$ sudo reboot** Wait for the server to reboot, this normally takes 3-5 minutes.
32. ☐	**Desired Server:** Login	Open a terminal window connection to the newly created server's console by establishing a ssh session from the NOAM-A's terminal console to the newly created server's XMI address. $ **ssh admusr@< desired_server _XMI_IP>** [admusr@pc9000738-so-a~]$ **<admusr_password>**
33. ☐	**Desired Server:** Use the **"ntpq"** command to verify that the server has connectivity to the assigned NTP server.	[admusr@ pc9000738-so-a~]$ **ntpq -np** remote refid st t when poll reach delay offset jitter == *10.250.32.10 192.5.41.209 2 u 651 1024 377 0.339 0.583 0.048 **Note:** It may take a few minutes for the NTP server to connect and sync with the server.

Procedure 14: Configuring Remaining HLRR Servers

Step	Procedure	Result
34. ☐	**Desired Server:** Verify Server Health	Execute the following command on the server and make sure that no errors are returned: **$ sudo 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
35. ☐	**Desired Server:** Execute a **"alarmMgr"** to verify the current health of the server	$ **sudo alarmMgr --alarmStatus** NOTE: This command should return no output on a healthy system. If any alarms are reported as SNMP traps, please contact Oracle's Customer Care Center for assistance.
36. ☐	**Desired Server:** Exit the SSH session	**$ exit** logout Connection to 10.240.241.2 closed.
37. ☐	**Repeat steps 4 through 36 of this procedure for each of the remaining NOAM, SOAM, Query Server, and MP servers.**	
38. ☐	**Optional: Repeat steps 4 through 36 of this procedure for each of the Disaster Recovery NOAM, SOAM, Query Server, and MP servers.**	
THIS PROCEDURE HAS BEEN COMPLETED		

7.3 Configure XSI Networks (All SOAM Sites)

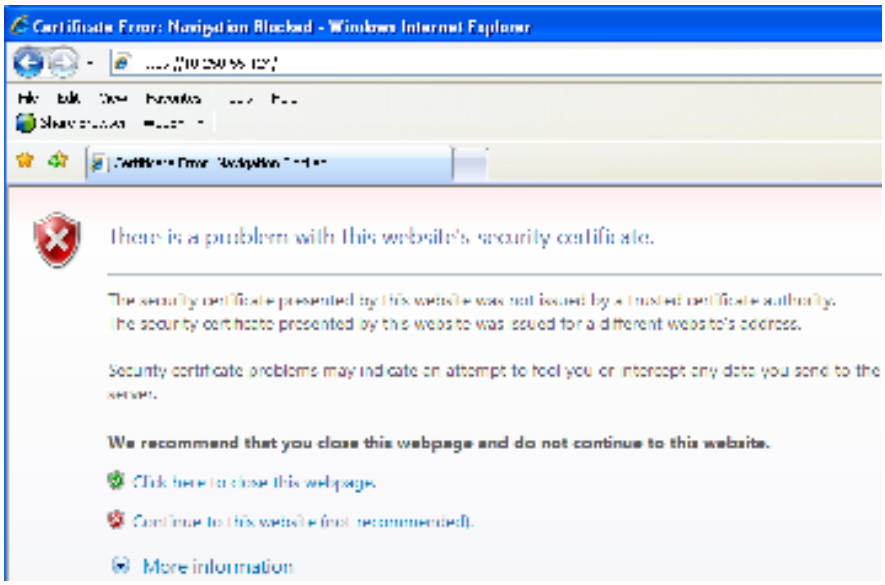
This procedure configures the XSI networks by adding the xsi1 and xsi2 networks.

Requirements: Procedure 14: Configuring Remaining HLRR Servers has been completed.

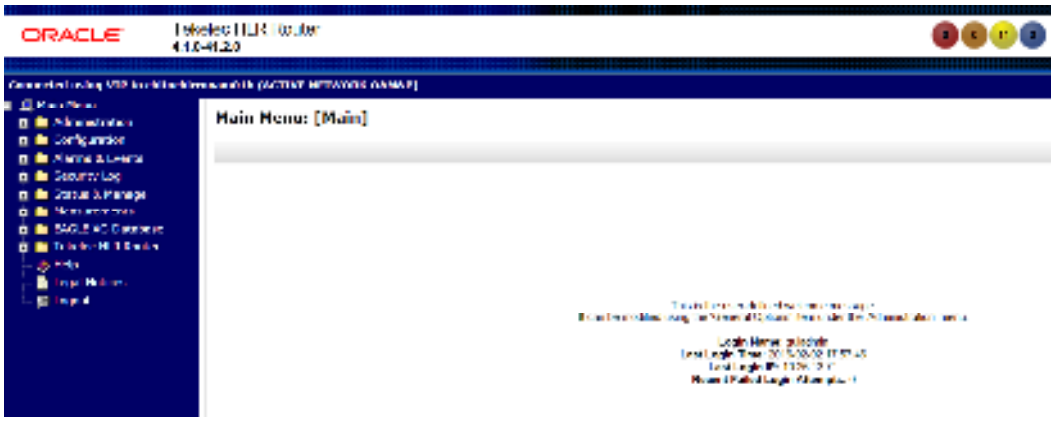
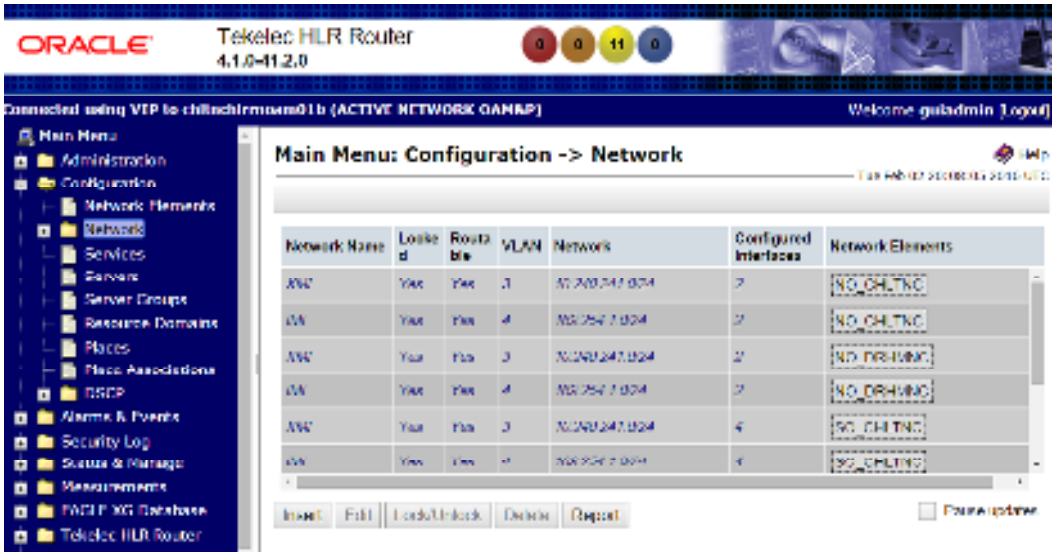
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

IF THIS PROCEDURE FAILS, CONTACT MY ORACLE SUPPORT AND ASK FOR ASSISTANCE.

Procedure 15: Configure XSI Networks

Step	Procedure	Result
1. ☐	**NOAM-A GUI:** Launch an approved web browser and connect to the XMI IP address assigned to **NOAM-A Server** using "https://"	
2. ☐	**NOAM-A GUI:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	

Procedure 15: Configure XSI Networks

Step	Procedure	Result
3. ☐	**NOAM-A GUI:** The user should be presented the HLRR Main Menu as shown on the right.	
4. ☐	**NOAM-A GUI:** Select… **Main Menu** → **Configuration** → ***Network***	

Procedure 15: Configure XSI Networks

Step	Procedure	Result
5. ☐	**NOAM-A GUI:** Add the XSI 1 and XSI 2 networks. Use the NAPD documentation for this networking information.	Click the **Insert** button. Output similar to that shown below may be observed. **Main Menu: Configuration -> Network [Insert]** Info **Insert Network** Field / Value / Description Network Name: XSI1 * — The name of this network. [Default = N/A. Range = Alphanu Network Element: - Unassigned - — The network element this network is a part of. If not specifie VLAN ID: 5 * — The VLAN ID to use for this network. [Default = N/A. Range Network Address: 10.240.237.216 * — The network address of this network. [Default = N/A. Range (IPv6) format.] Netmask: 255.255.255.248 * — Subnetting to apply to servers within this network. [Default = dotted decimal (IPv4) format.] Router IP: 10.240.237.217 — The IP address of a router on this network. If this is a defau servers with interfaces on this network. If customer router r Default Network: Yes / No — A selection indicating whether this is the network with a def Routable: Yes / No — Whether or not this network is routable outside its network present in all network elements. Ok Apply Cancel Enter all of the above fields for the **XSI 1** network and press the **Apply** button. Enter Network Name: **XSI1 or XSI2** Network Element: **Leave Unassigned** VLAN ID: **(NAPD document)** Network Address: **(NAPD document)** Netmask: **(NAPD document)** Router IP: Gateway Address **(NAPD document)** Default Network: NO Routeable: Yes Enter all of the above fields for the **XSI 1** network and press the **Apply** button. Enter all of the above fields for the **XSI 2** network and press the **Ok** button.
		THIS PROCEDURE HAS BEEN COMPLETED

7.4 OAM Pairing for the Primary NOAM Servers (1st NOAM site only)

The user should be aware that during the OAM Pairing procedure, various errors may be seen at different stages of the procedure. During the execution of a step, the user is directed to ignore errors related to values other than the ones referenced by that step.

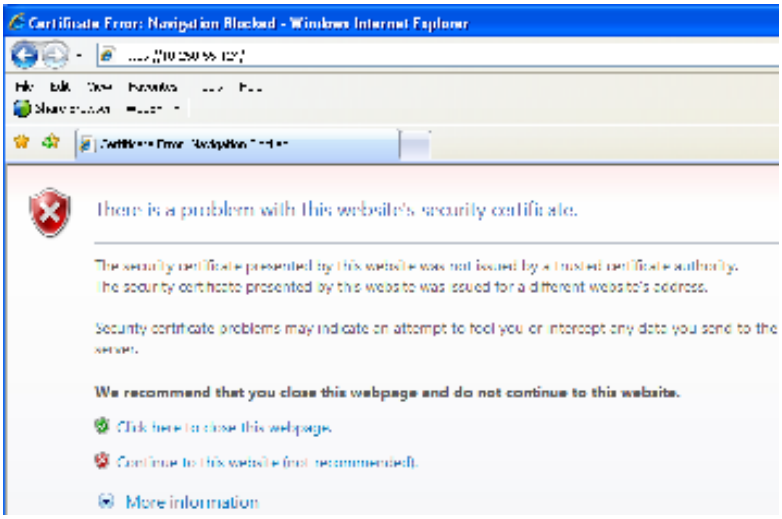
This procedure creates active/standby pair for the NOAM servers at the Primary Provisioning Site.

Requirements: Procedure 14: Configuring Remaining HLRR Servers has been completed.

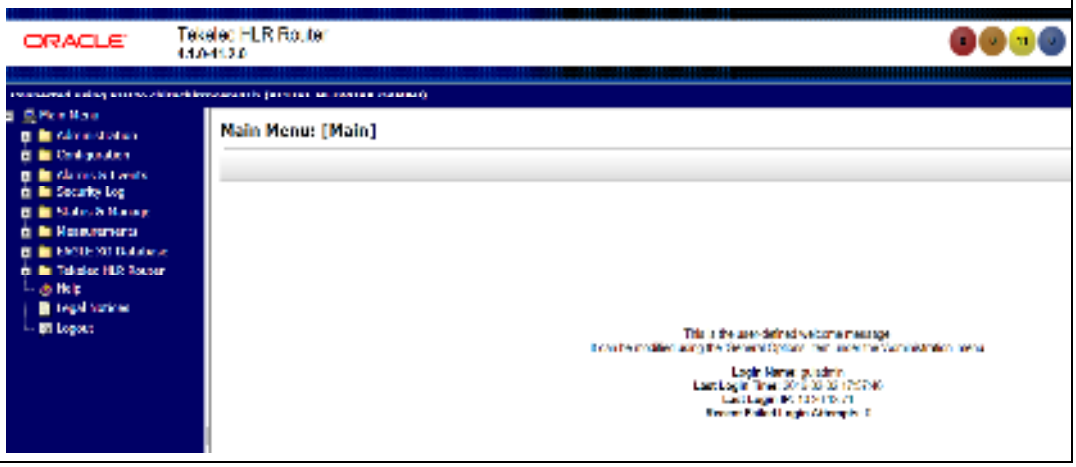
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

IF THIS PROCEDURE FAILS, CONTACT MY ORACLE SUPPORT AND ASK FOR ASSISTANCE.

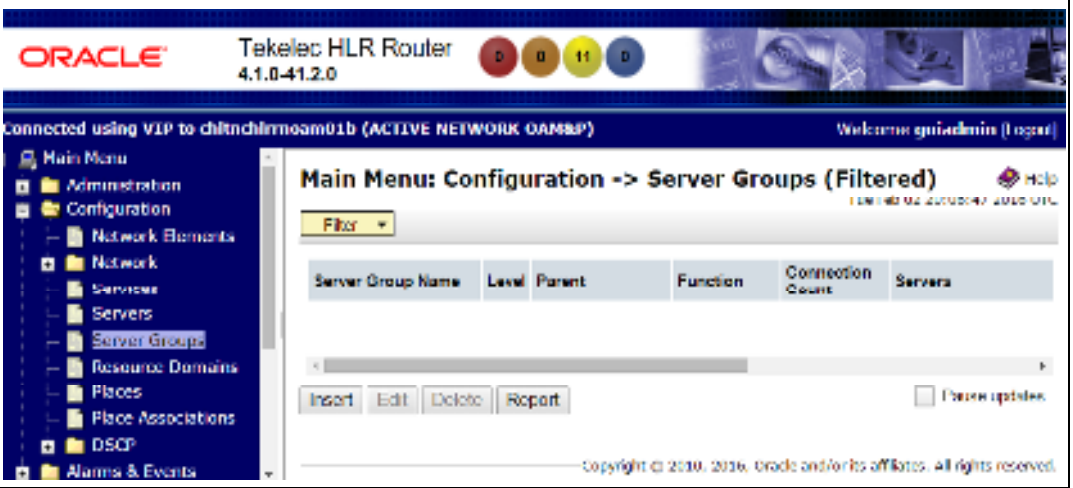
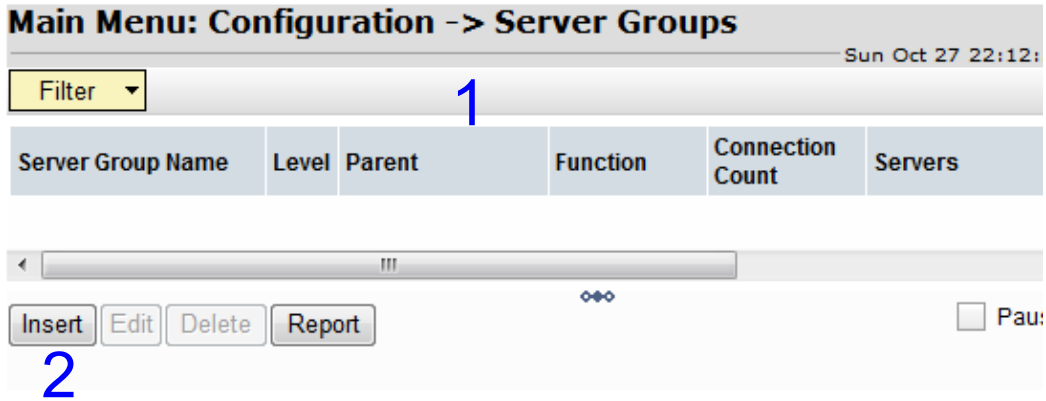
Procedure 16: OAM Pairing for the Primary NOAM Servers

Step	Procedure	Result
1. ☐	**NOAM-A GUI:** Launch an approved web browser and connect to the XMI IP address assigned to **NOAM-A Server** using "https://"	

Procedure 16: OAM Pairing for the Primary NOAM Servers

Step	Procedure	Result
2. ☐	**NOAM-A GUI:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	
3. ☐	**NOAM-A GUI:** The user should be presented the HLRR Main Menu as shown on the right.	

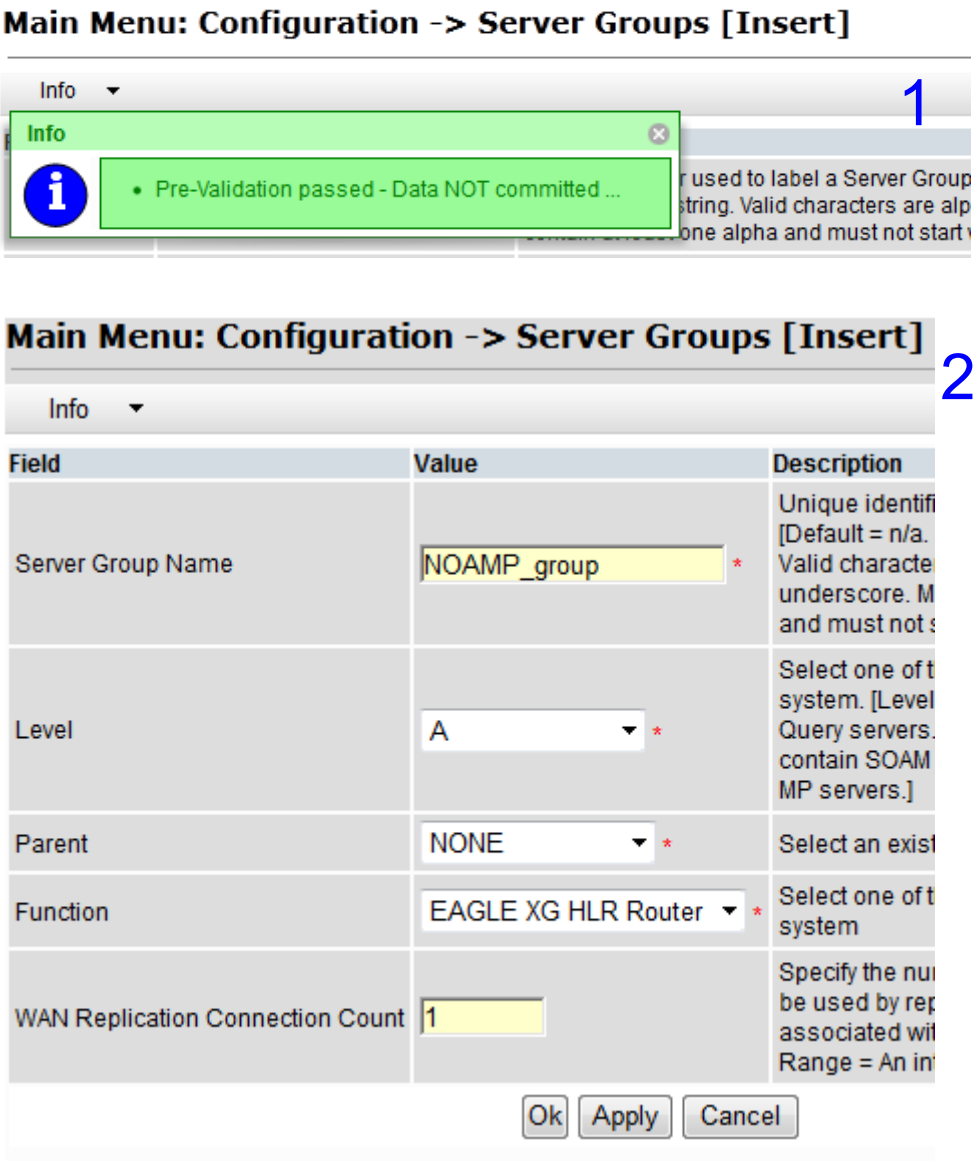
Procedure 16: OAM Pairing for the Primary NOAM Servers

Step	Procedure	Result
4. ☐	**NOAM-A GUI:** *Configuring HLRR Server Group* Select… **Main Menu** → **Configuration** → ***Server Groups***	
5. ☐	**NOAM-A GUI:** **1)** The user will be presented with the **"Server Groups"** configuration screen as shown on the right. **2)** Select the **"Insert"** dialogue button from the bottom left corner of the screen.	 **NOTE:** *The user may need to use the vertical scroll-bar in order to make the **"Insert"** dialogue button visible.*

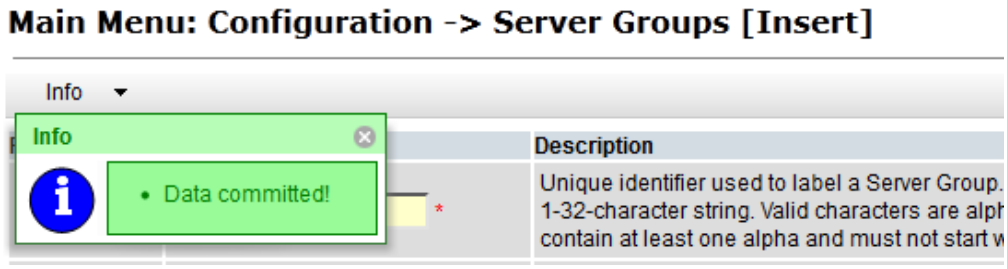
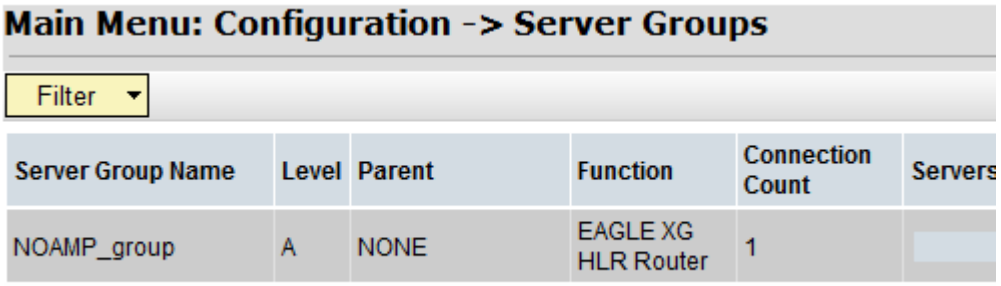
Procedure 16: OAM Pairing for the Primary NOAM Servers

Step	Procedure	Result
6. ☐	**NOAM-A GUI:** The user will be presented with the **"Server Groups [Insert]"** screen as shown on the right.	**Main Menu: Configuration -> Server Groups [Insert]** Field / Value / Description Server Group Name — Unique identifier used to label a Server = A 1-32-character string. Valid charact underscore. Must contain at least one a a digit.] Level — - Select Level - * — Select one of the Levels supported by t contain NOAMP and Query servers. Lev contain SOAM servers. Level C groups Parent — - Select Parent - * — Select an existing Server Group or NON Function — - Select Function - * — Select one of the Functions supported WAN Replication Connection Count — Specify the number of TCP connections replication over any WAN connection as Group. [Default = 1. Range = An integer Ok Apply Cancel
7. ☐	**NOAM-A GUI:** Input the **Server Group Name**.	Field / Value / Description Server Group Name — NOAMP_group * — Unique identifier use = A 1-32-character st underscore. Must cor a digit.]
8. ☐	**NOAM-A GUI:** Select **"A"** on the **"Level"** pull-down menu.	Level — A * — Select one of the Levels sup contain NOAMP and Query s contain SOAM servers. Level
9. ☐	**NOAM-A GUI:** Select **"None"** on the **"Parent"** pull-down menu.	Parent — NONE * — Select an existing Server Gr
10. ☐	**NOAM-A GUI:** Select "**EAGLE XG HLR Router**" on the "**Function**" pull-down menu.	Function — EAGLE XG HLR Router * — Select one of the

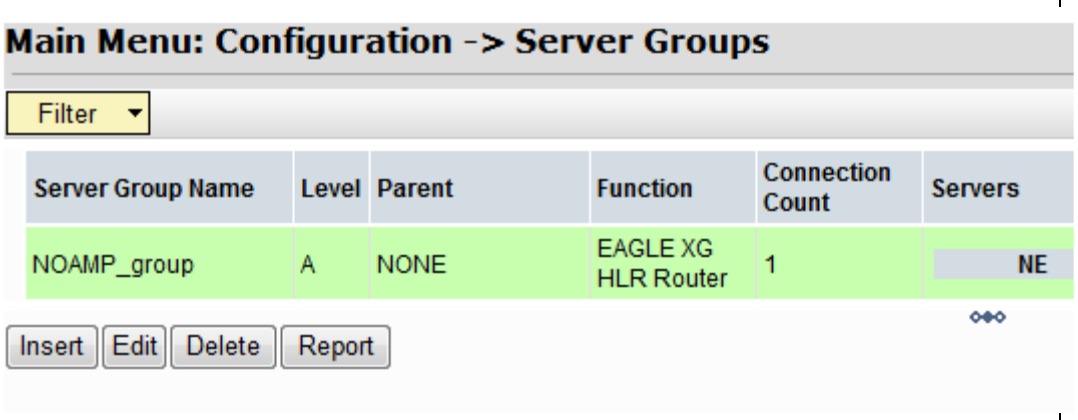
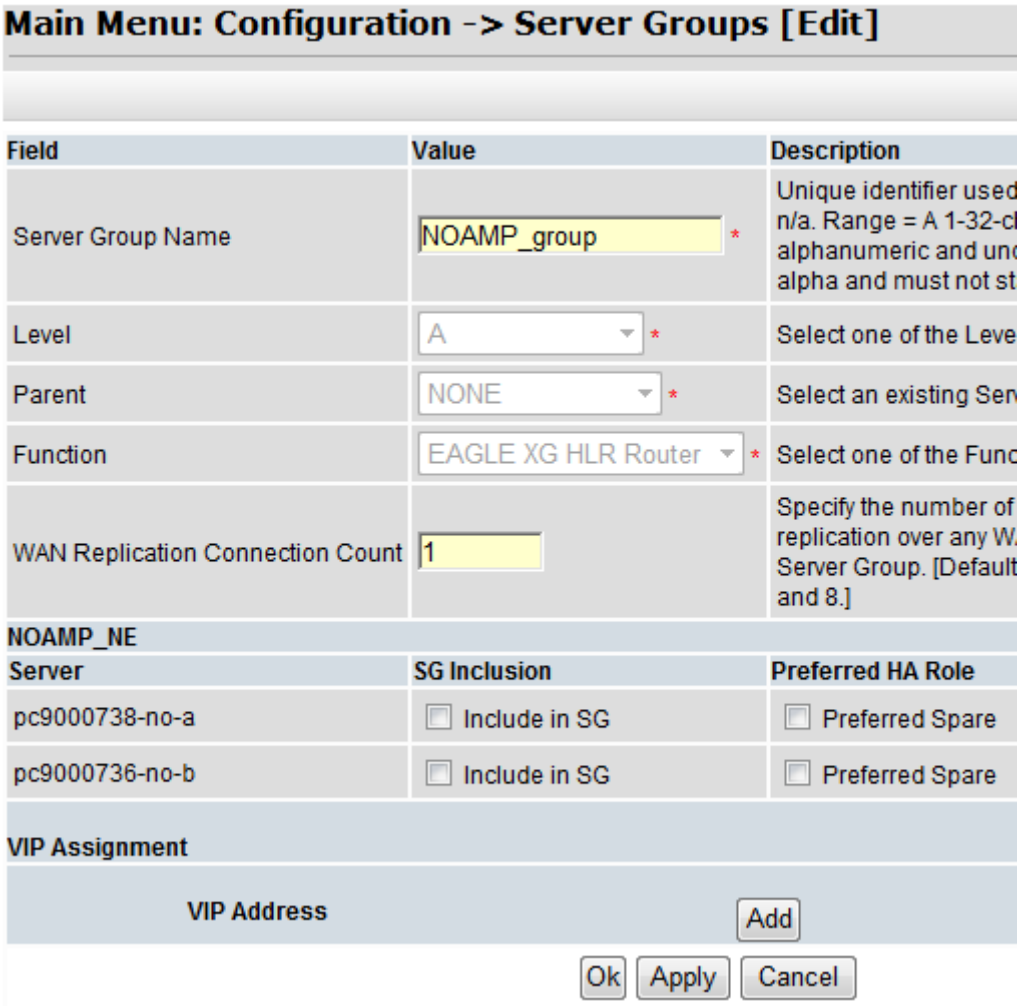
Procedure 16: OAM Pairing for the Primary NOAM Servers

Step	Procedure	Result
11. ☐	**NOAM-A GUI:** Enter value of "**1**" for "**WAN Replication Connection Count**" field.	
12. ☐	**NOAM-A GUI:** **1)** The user should be presented with a banner information message stating **"Pre-Validation passed"**. **2)** Select the **"OK"** dialogue button.	

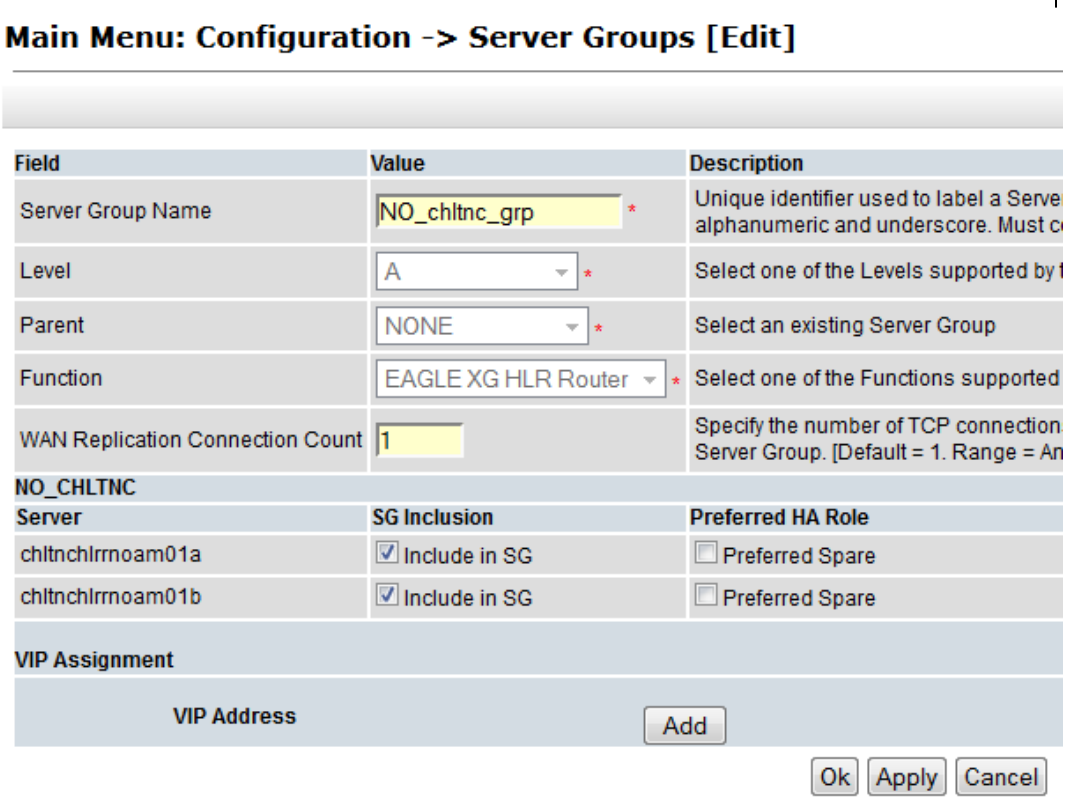
Procedure 16: OAM Pairing for the Primary NOAM Servers

Step	Procedure	Result
13. ☐	**NOAM-A GUI:** The user should be presented with a banner information message stating **"Data committed"**.	
14. ☐	**NOAM-A GUI:** Select… **Main Menu** → **Configuration** → ***Server Groups***	
15. ☐	**NOAM-A GUI:** The **Server Group** entry added in **Steps 4** through **13** should now appear on the **"Server Groups"** configuration screen as shown on the right.	

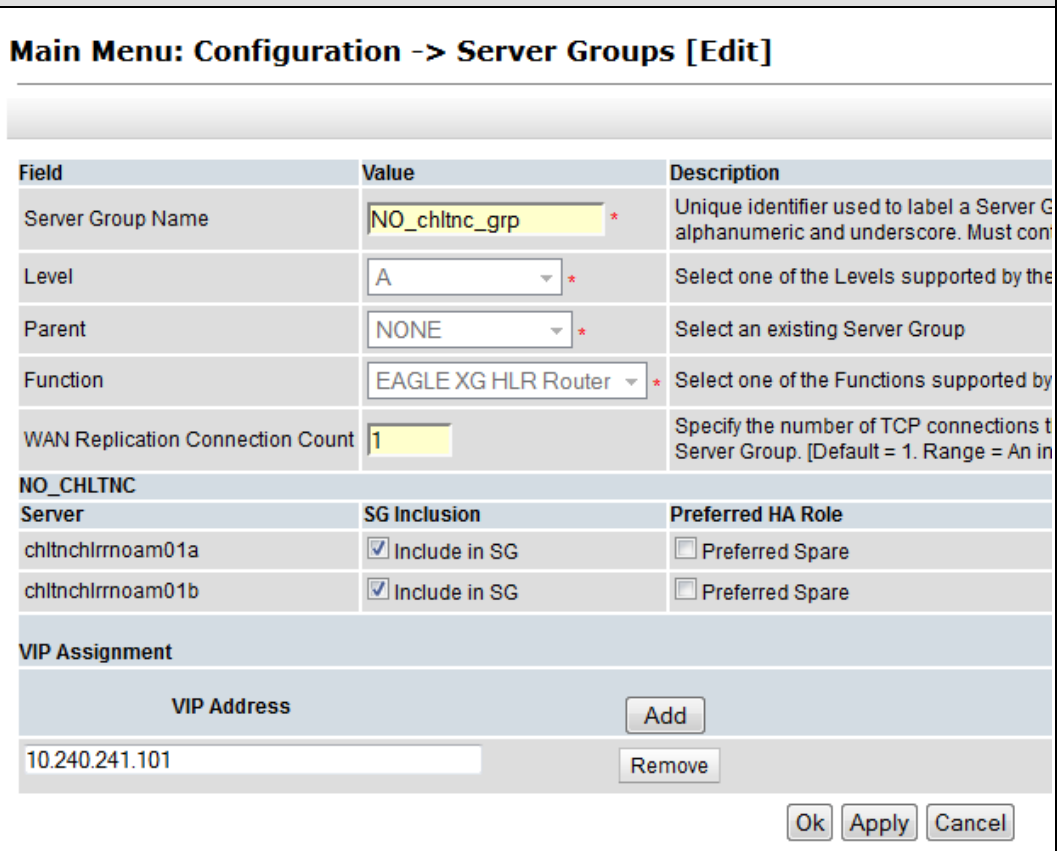
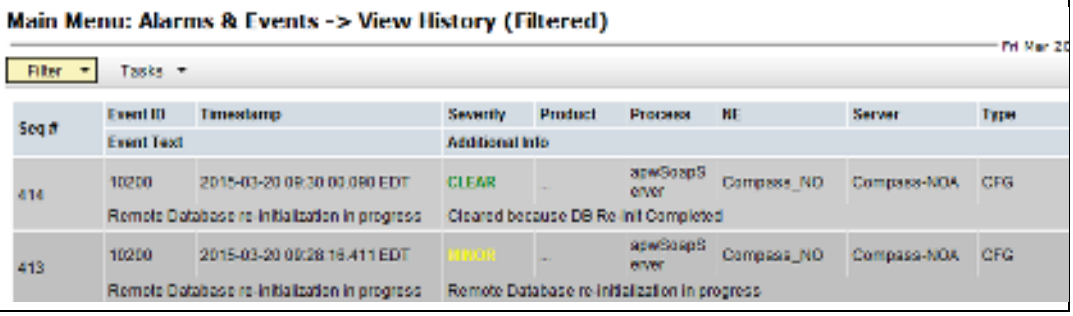
Procedure 16: OAM Pairing for the Primary NOAM Servers

Step	Procedure	Result
16. ☐	**NOAM-A GUI:** **1)** Select the newly created **Server Group**. The line entry should now be highlighted in **GREEN**. **2)** Select the **"Edit"** dialogue button from the bottom left corner of the screen.	
17. ☐	**NOAM-A GUI:** The user will be presented with the **"Server Groups [Edit]"** screen as shown on the right.	

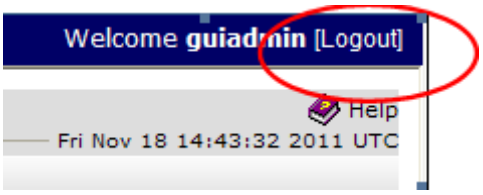
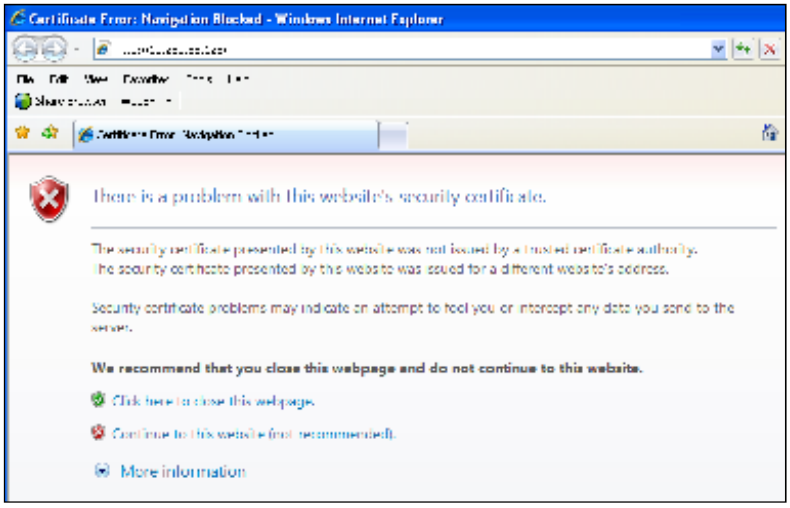
Procedure 16: OAM Pairing for the Primary NOAM Servers

Step	Procedure	Result
18. ☐	**NOAM-A GUI:** **1)** To add a server to the server group, select the checkbox for **SG Inclusion**. When checked, the server will be included in the server group. **2)** Select **NOAM-A** and **NOAM-B** checkboxes from the SG Inclusion Field. **3)** If a **Query Server** is part of the system configuration it should also be checked so it will be included in the NO Grouping. **4)** Click "**Apply"** to submit the information.	
19. ☐	**NOAM-A GUI:** To add the virtual IP address, select **Add** in the **VIP Assignment** section.	

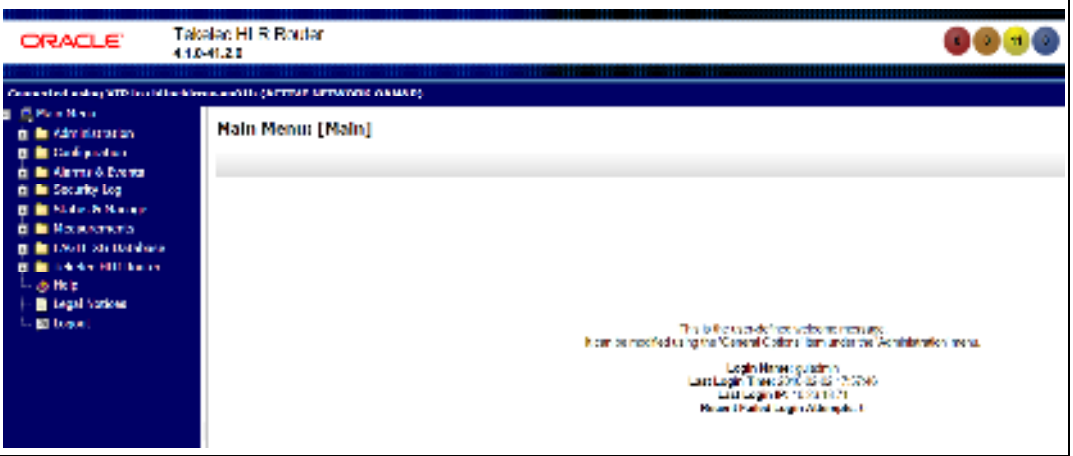
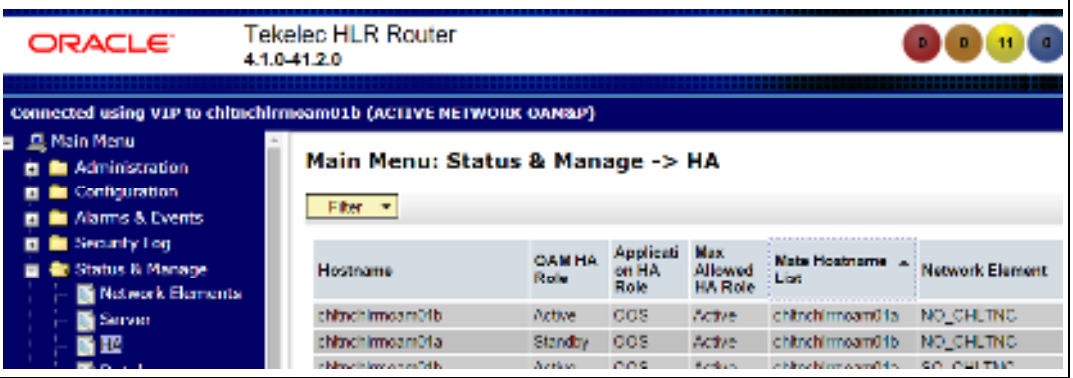
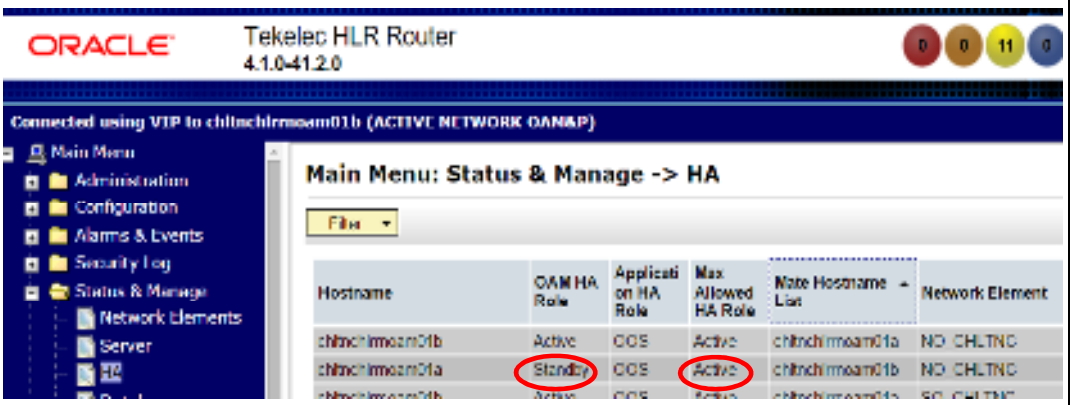
Procedure 16: OAM Pairing for the Primary NOAM Servers

Step	Procedure	Result
20. ☐	**NOAM-A GUI:** **1)** Enter the XMI virtual IP address in **VIP Address** field. **Note:** Use the NAPD documentation for this networking information. **2)** Select the **"OK"** dialogue button to commit the information.	
21. ☐	**IMPORTANT:** Wait a few minutes before proceeding on to the next Step.	Now that the NOAM servers 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.
22. ☐	**NOAM VIP:** Wait for Remote Database Alarm to Clear for the NOAMs and optional Query Server.	Wait for alarm **10200 Remote Database re-initialization in progress** to clear for both NOAM-A, NOAM-B and Query Server (Optional) before proceeding. Navigate to **Main menu->Alarms & Events->View Active** 

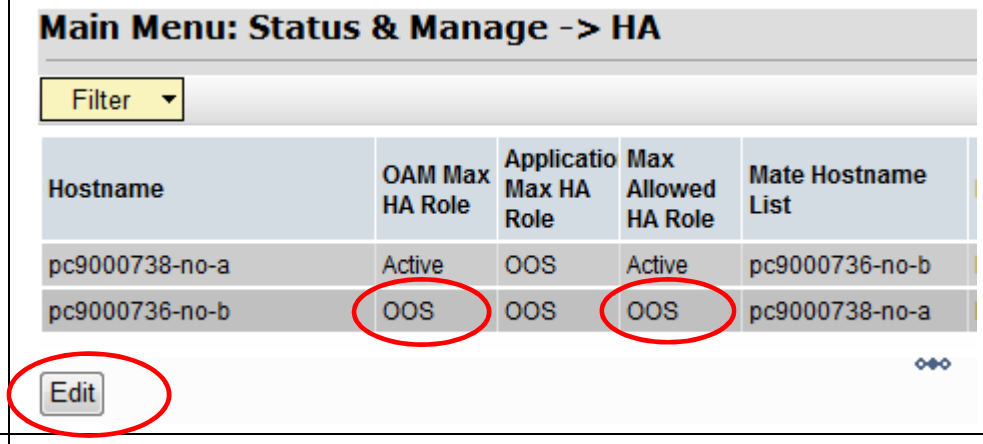
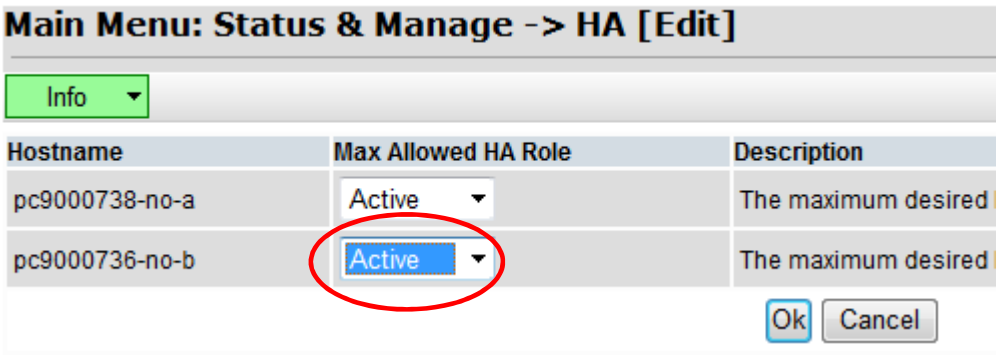
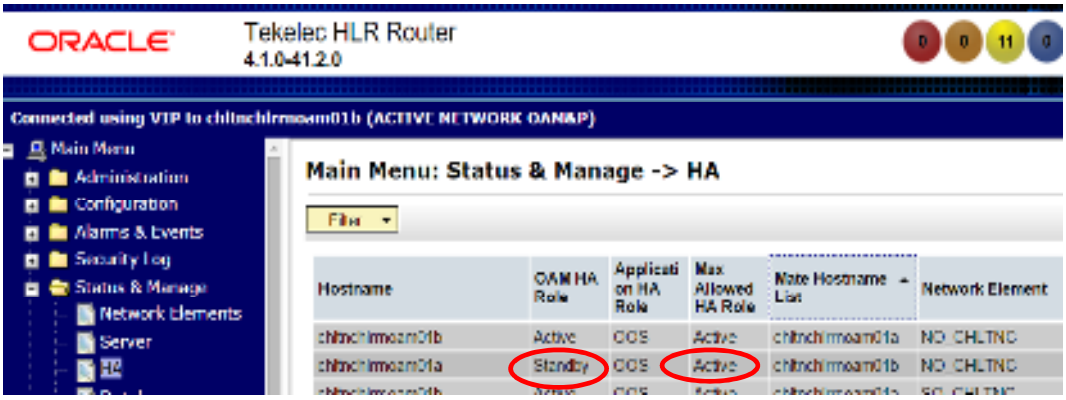
Procedure 16: OAM Pairing for the Primary NOAM Servers

Step	Procedure	Result
23. ☐	**NOAM-A GUI:** Click the **"Logout"** link on the NOAM-A server GUI.	
24. ☐	**NOAM VIP:** Launch an approved web browser and connect to the **XMI Virtual IP Address (VIP)** assigned in **STEP 20** to the **HLRR Server Group** using **"https://".**	
25. ☐	**NOAM VIP:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	

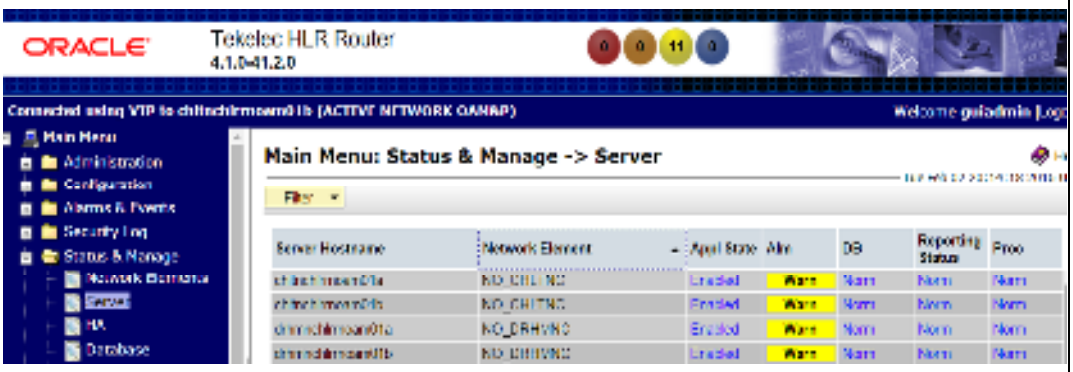
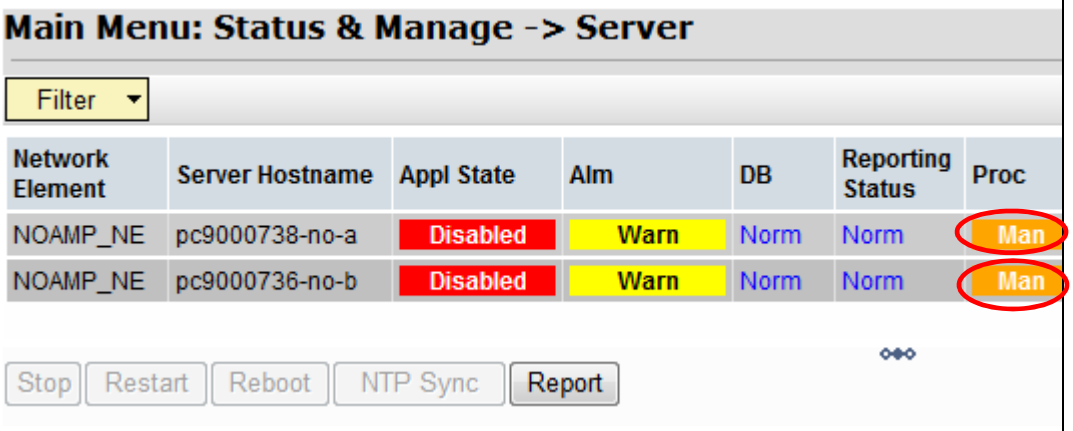
Procedure 16: OAM Pairing for the Primary NOAM Servers

Step	Procedure	Result
26. ☐	**NOAM VIP:** The user should be presented the HLRR Main Menu as shown on the right.	
27. ☐	**NOAM VIP:** Select… **Main Menu** → **Status & Manage** → ***HA***	
28. ☐	**NOAM VIP:** Verify that the **OAM HA Role** shows **"Standby"** and **Max Allowed HA Role** shows **"Active"** for **NOAM Server B** If it shows **"OOS"** then continue with the next step. Otherwise skip forward to **Step 34** of this procedure.	

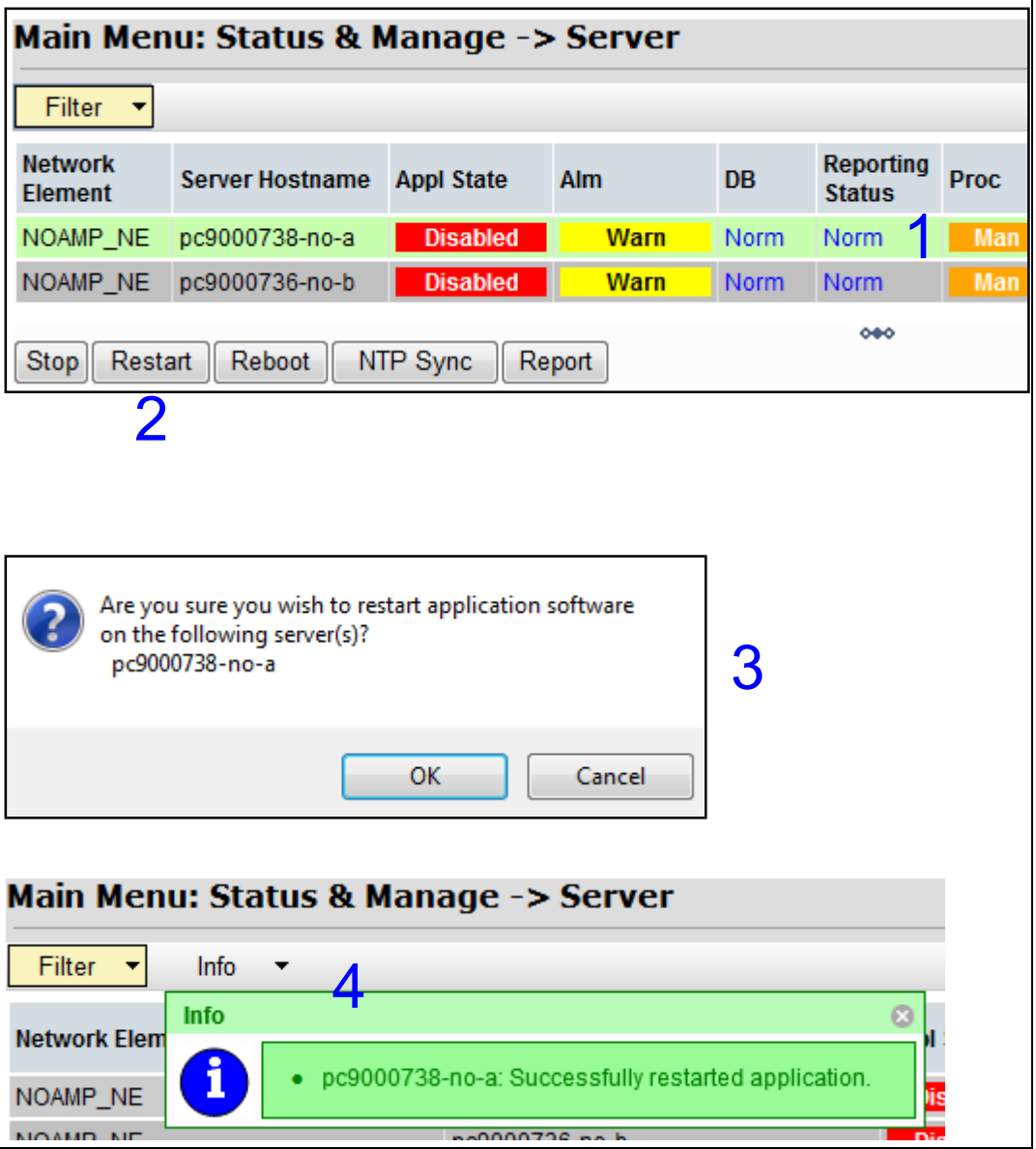
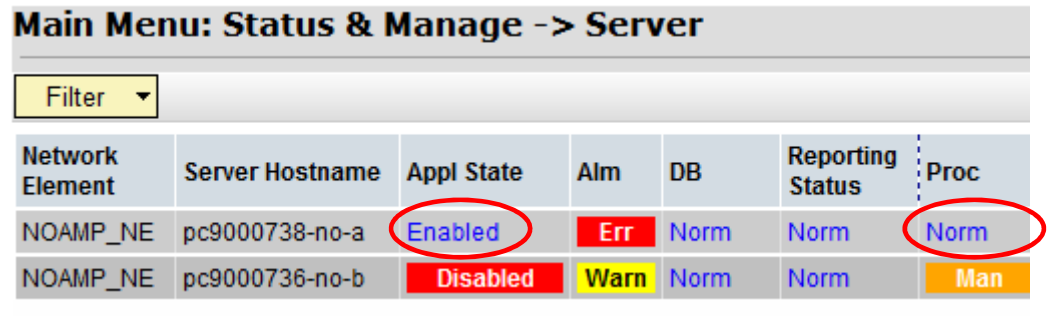
Procedure 16: OAM Pairing for the Primary NOAM Servers

Step	Procedure	Result
29. ☐	**NOAM VIP:** Click **Edit** button	
30. ☐	**NOAM VIP:** Change the **Max Allowed HA Role** for **NOAM Server B** to **Active** and click OK button. **Optional:** Change the **Max Allowed HA Role** for **Query Server** to **Observer** and click **OK** button.	
31. ☐	**NOAM VIP:** Verify that the **OAM HA Role** shows **"Standby"** and **Max Allowed HA Role** shows **"Active"** for **NOAM Server B** **Optional:** Verify that the **OAM Max HA Role** shows **"Active"** and **Max Allowed HA Role** shows **"Observer"** for **Query Server.**	

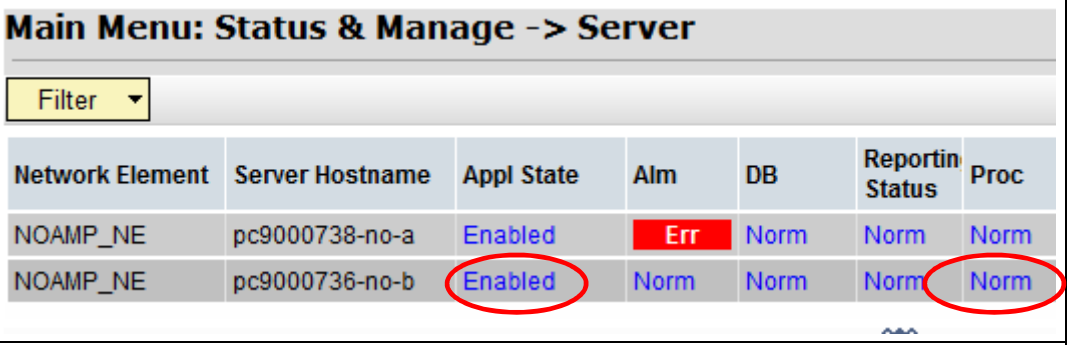
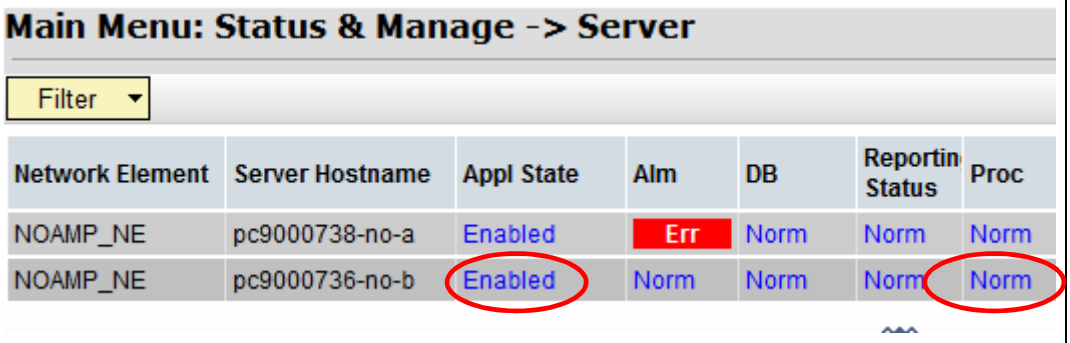
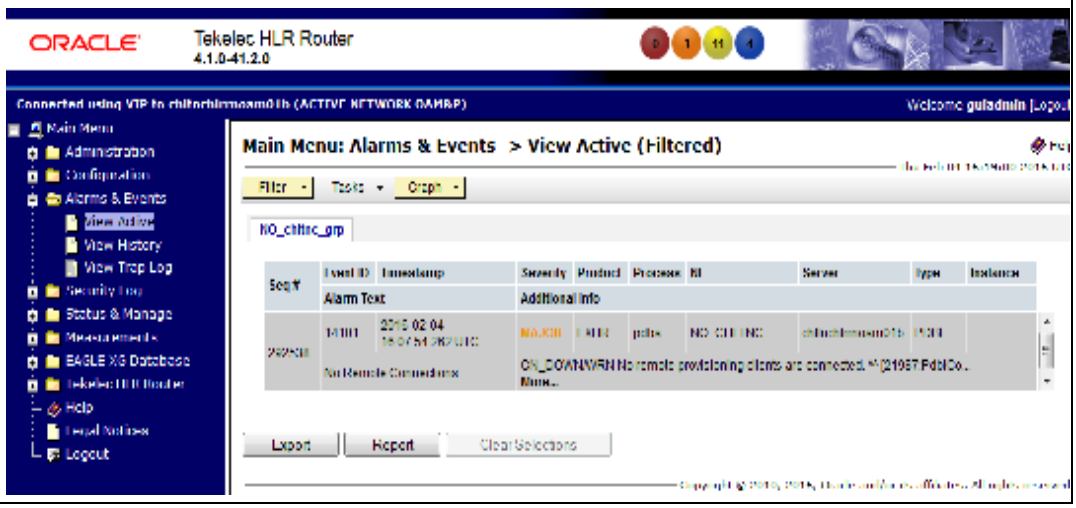
Procedure 16: OAM Pairing for the Primary NOAM Servers

Step	Procedure	Result
32. ☐	**NOAM VIP:** *Restarting the NOAM Server Application* Select… **Main Menu** → **Status & Manage** → ***Server***	
33. ☐	**NOAM VIP:** **1)** The **"A"** and **"B"** NOAM servers should now appear in the right panel. **2)** Verify that the "**Appl State**" now shows "**Disabled**" **"DB"** status shows **"Norm"** and the **"Proc"** status shows **"Man"** for both servers before proceeding to the next Step.	

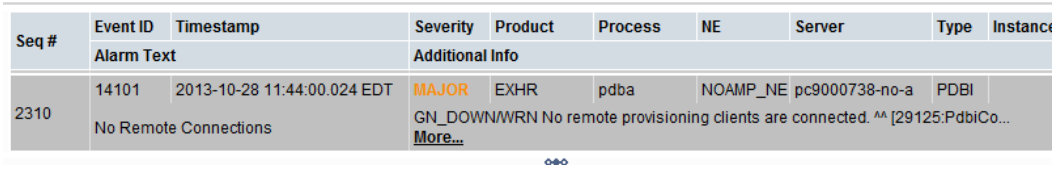
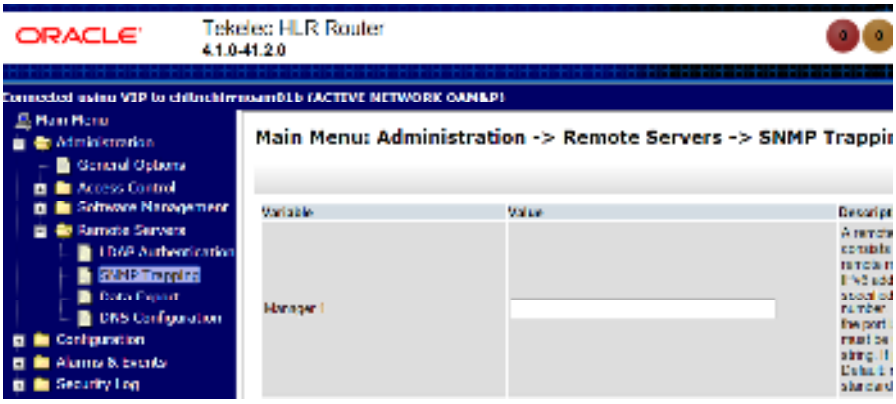
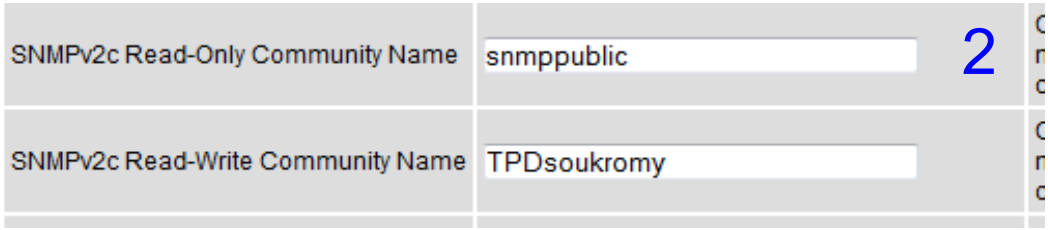
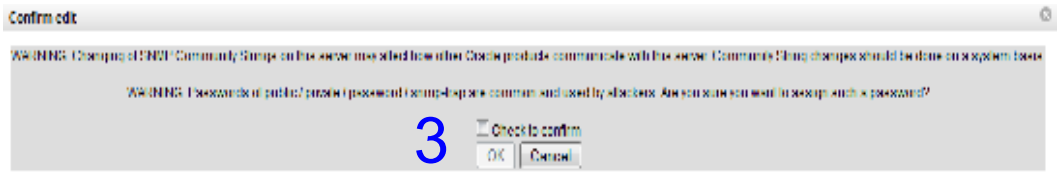
Procedure 16: OAM Pairing for the Primary NOAM Servers

Step	Procedure	Result
34. ☐	**NOAM VIP:** **1)** Select **NOAM Server A**. The line entry should now be highlighted in **GREEN**. **2)** Select the **"Restart"** dialogue button from the bottom left corner of the screen. **3)** Click the **"OK"** button on the confirmation dialogue box. **4)** The user should be presented with a confirmation message (in the banner area) for **NOAM-A Server** stating: **Successfully restarted application"**. **NOTE:** *The user may need to use the vertical scroll-bar in order to make the **"Restart"** dialogue button visible.*	
35. ☐	**NOAM VIP:** Verify that the **"Appl State"** now shows **"Enabled"** and the **"Proc"** status column shows **"Norm"** for **NOAM-A Server** before proceeding to the next Step.	

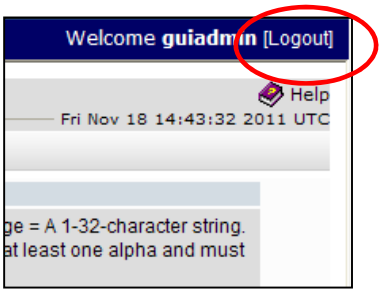
Procedure 16: OAM Pairing for the Primary NOAM Servers

Step	Procedure	Result
36. ☐	**NOAM VIP:** Repeat **Step 34** of this Procedure for **NOAM Server B.**	Repeat **Step 34** of this Procedure to restart application on **NOAM Server B.**
37. ☐	**NOAM VIP:** Verify that the **"Appl State"** now shows **"Enabled"** and the **"Proc"** status column shows **"Norm"** for **NOAM Server B** before proceeding to the next step.	
38. ☐	**NOAM VIP:** **Optional:** Repeat **Step 34** of this Procedure for **Query Server.**	**Optional:** Repeat **Step 34** of this Procedure to restart application on **Query Server.**
39. ☐	**NOAM VIP:** **Optional:** Verify that the **"Appl State"** now shows **"Enabled"** and the **"Proc"** status column shows **"Norm"** for the **Query Server** before proceeding to the next step.	
40. ☐	**NOAM VIP:** *Verifying the NOAM Server Alarm status* Select… **Main Menu** → **Alarms & Events** → ***View Active***	

Procedure 16: OAM Pairing for the Primary NOAM Servers

Step	Procedure	Result
41. ☐	**NOAM VIP:** Verify that **Event ID 14101** (“*No remote provisioning clients are connected”)* is the only alarm present on system at this time.	
42. ☐	**NOAM VIP:** Configuring SNMP for Traps from Individual Servers Select… **Main Menu** → **Administration** → **Remote Servers** → ***SNMP Trapping***	
43. ☐	**NOAM VIP:** **1)** Using the cursor, place a “check” in the check box for **“Traps from Individual Servers”**. **2)** Enter the values for the **SNMPv2c Read-Only** and **Read-Write** Community Strings. Click the **“OK”** dialogue button located at the bottom of the screen. **3)** Check the “Check to confirm” box on the popup window, and then click on the “**OK**” button to commit the changes.	  

Procedure 16: OAM Pairing for the Primary NOAM Servers

Step	Procedure	Result
44. ☐	**NOAM VIP:** Click the **"Logout"** link on the server GUI.	
THIS PROCEDURE HAS BEEN COMPLETED		

7.5 OAM Pairing for SOAM and DR sites (All SOAM and DR sites)

The user should be aware that during the OAM Pairing procedure, various errors may be seen at different stages of the procedure. During the execution of a step, the user is directed to ignore errors related to values other than the ones referenced by that step. The steps in this procedure are for all SOAM servers and the optional DR NOAM servers. This procedure creates active/standby pair for the SOAM servers at any site or the optional DR NOAM Servers.

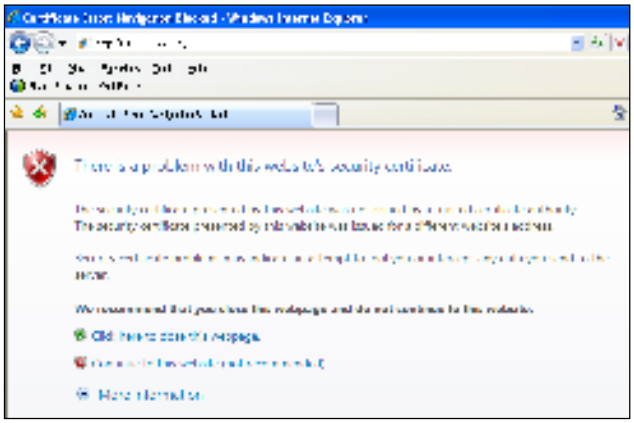
Requirements:

- **Procedure 14: Configuring Remaining HLRR Servers**has been completed.
- **Procedure 16: OAM Pairing for the Primary NOAM Servers** has been completed.

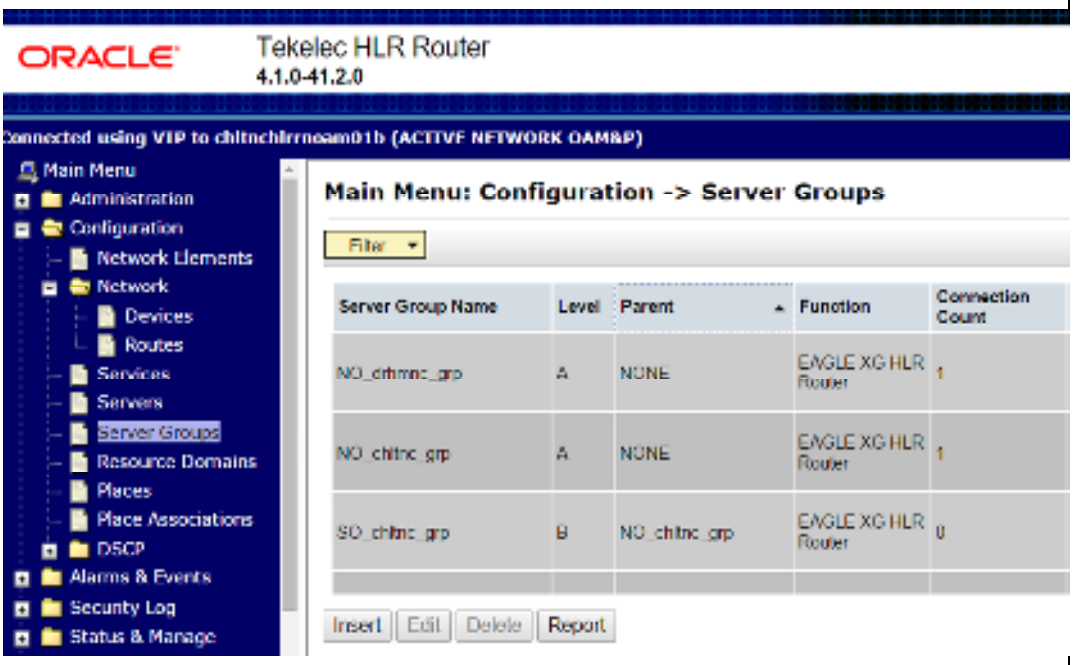
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

IF THIS PROCEDURE FAILS, CONTACT MY ORACLE SUPPORT AND ASK FOR ASSISTANCE..

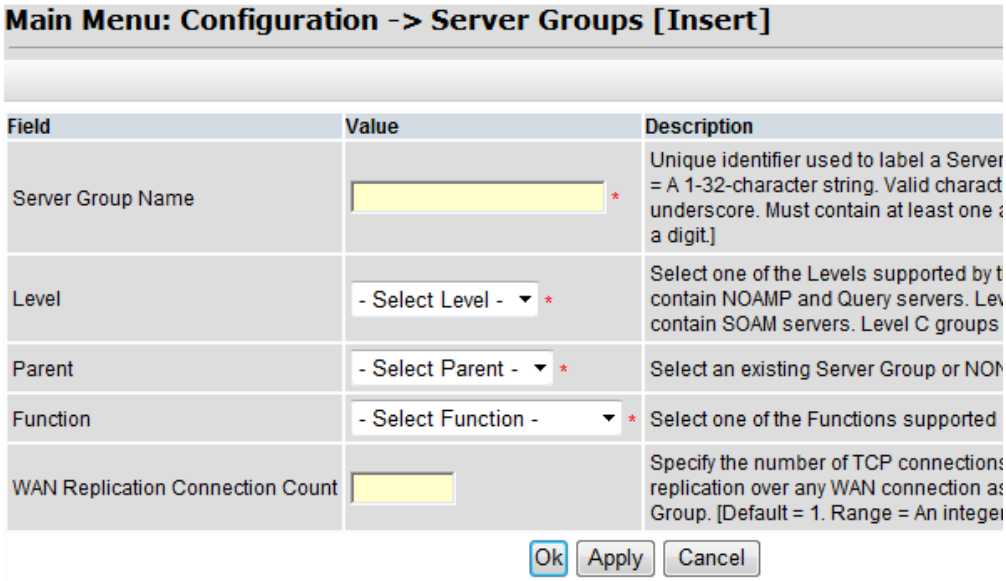
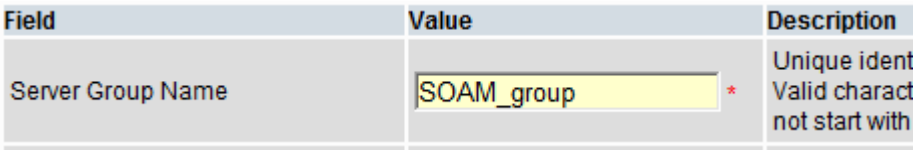
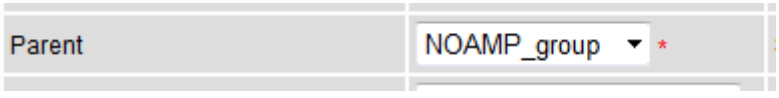
Procedure 17: OAM Pairing for SOAM or DR NOAM sites

Step	Procedure	Result
1. ☐	**Active NOAM VIP:** Launch an approved web browser and connect to the **XMI Virtual IP Address (VIP)** of the **Active NOAM site** using "https://"	
2. ☐	**Active NOAM VIP:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	

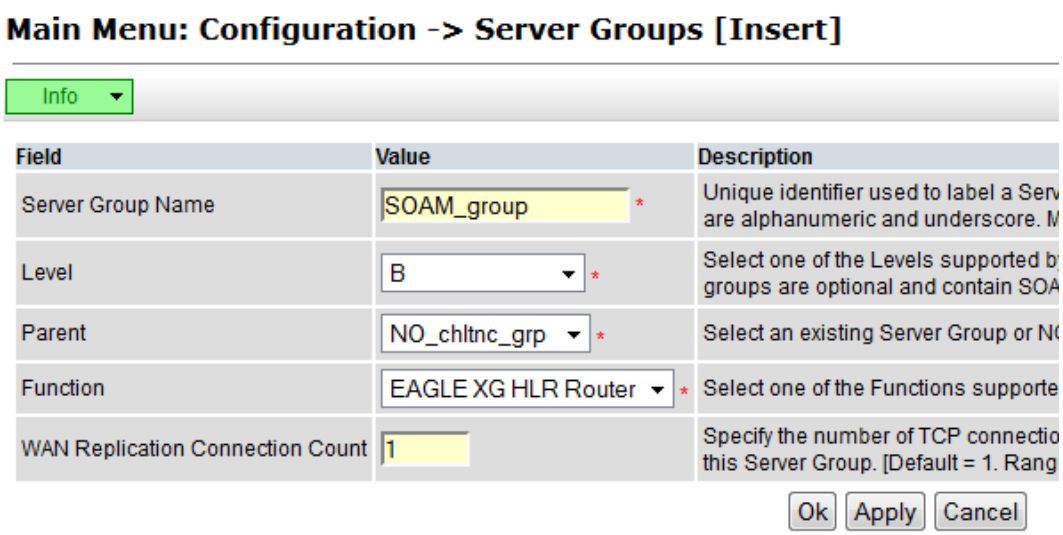
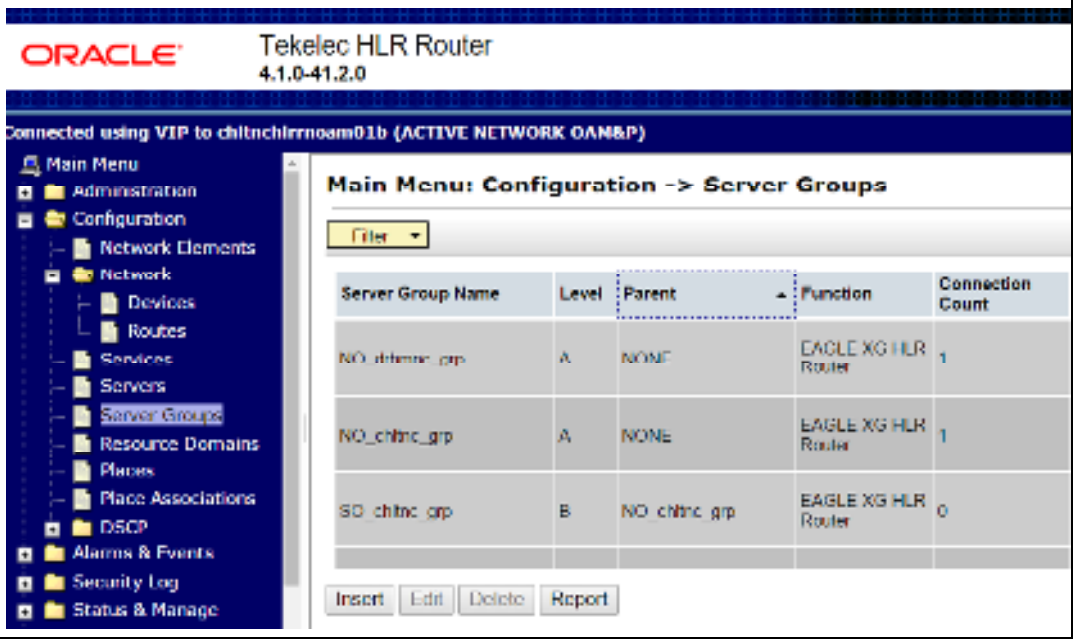
Procedure 17: OAM Pairing for SOAM or DR NOAM sites

Step	Procedure	Result
3. ☐	**Active NOAM VIP:** The user should be presented the HLRR Main Menu as shown on the right.	
4. ☐	**Active NOAM VIP:** Select… **<u>Main Menu</u>** **→ Configuration** ***→ Server Groups*** **1)** The user will be presented with the **"Server Groups"** configuration screen as shown on the right. **2)** Select the **"Insert"** dialogue button from the bottom left corner of the screen.	

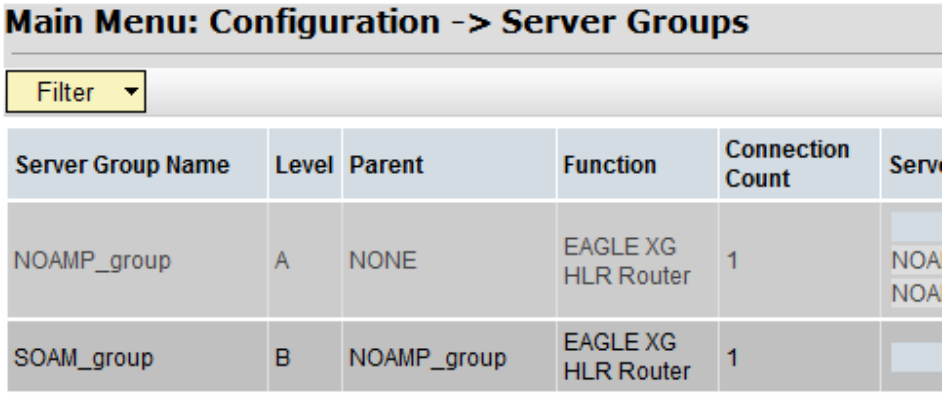
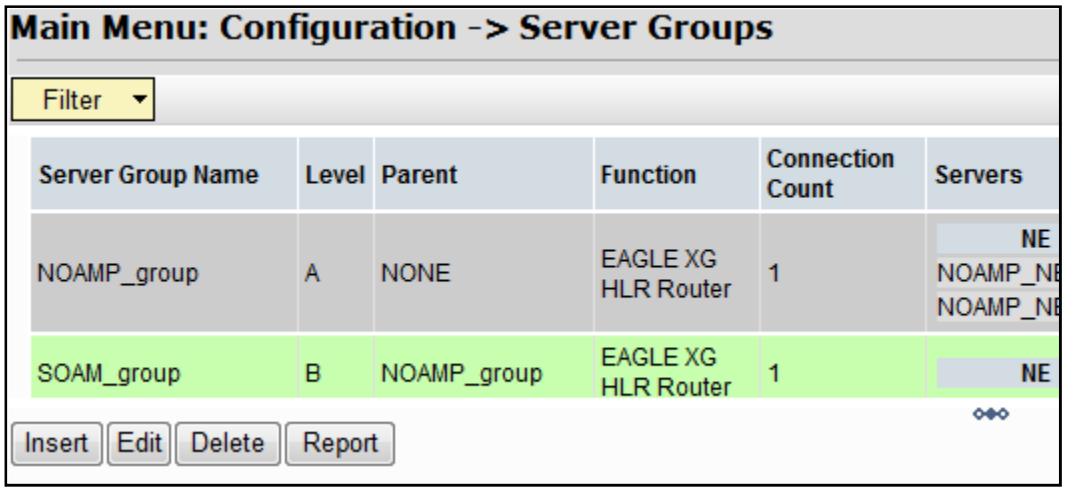
Procedure 17: OAM Pairing for SOAM or DR NOAM sites

Step	Procedure	Result
5. ☐	**Active NOAM VIP:** The user will be presented with the **"Server Groups [Insert]"** screen as shown on the right.	
6. ☐	**Active NOAM VIP:** Input the **Server Group Name**.	
7. ☐	**Active NOAM VIP:** For SOAM server group, select **"B"** on the **"Level"** pull-down menu.. **Optional:** For DR NOAM server group, select **"A"** on the **"Level"** pull-down menu.	
8. ☐	**Active NOAM VIP:** Select a **Parent** from the pull-down menu. **Optional:** For DR NOAM server group, select **"None"** on the **"Parent"** pull-down menu.	

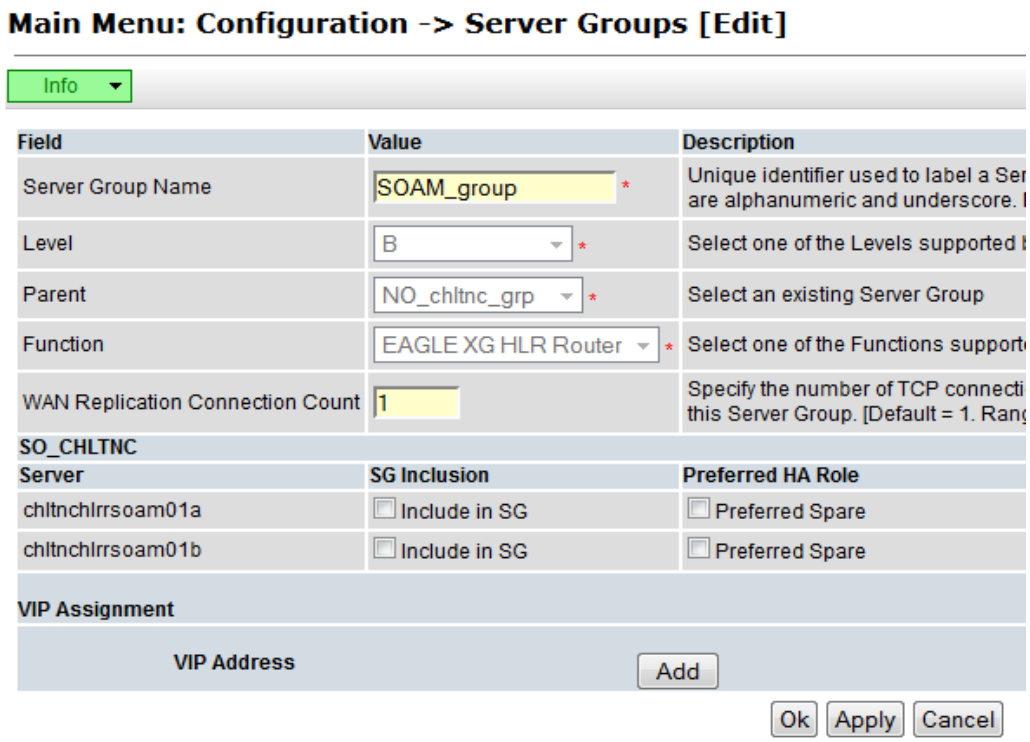
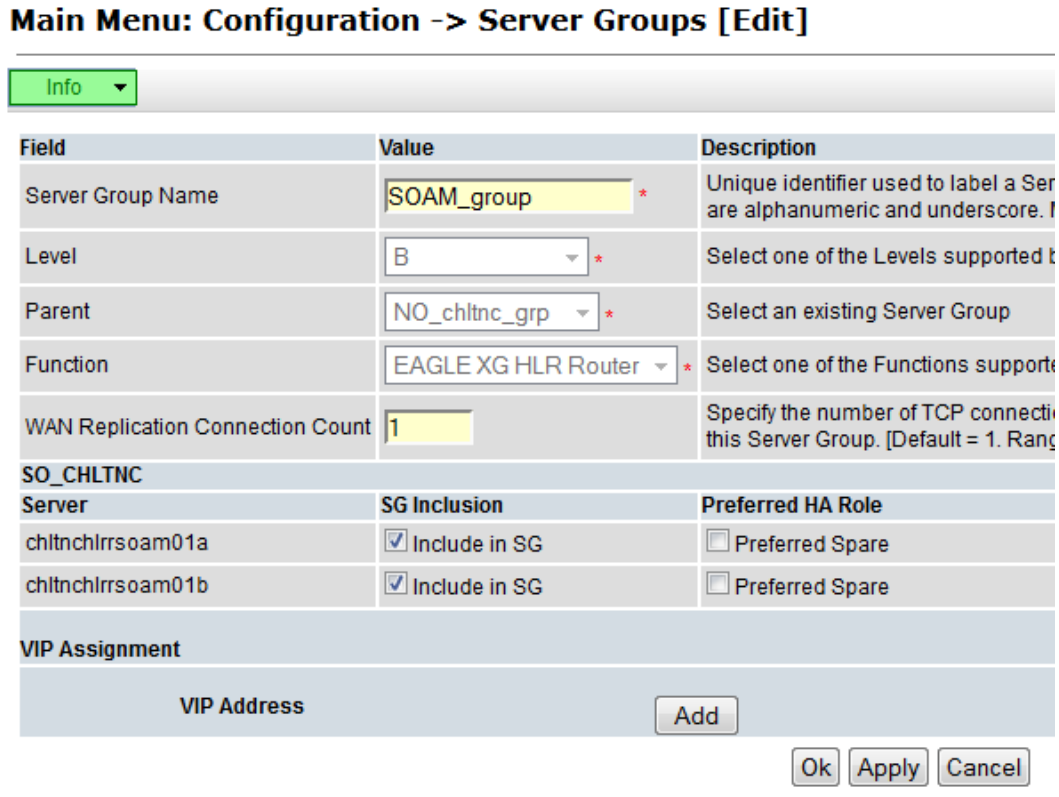
Procedure 17: OAM Pairing for SOAM or DR NOAM sites

Step	Procedure	Result
9. ☐	**Active NOAM VIP:** Select a **Function** from the pull-down menu.	
10. ☐	**Active NOAM VIP:** Enter a **WAN Replication Connection Count**	
11. ☐	**Active NOAM VIP:** Click **OK** button to commit the information.	
12. ☐	**Active NOAM VIP:** Select… **<u>Main Menu</u>** → **Configuration** → ***Server Groups***	

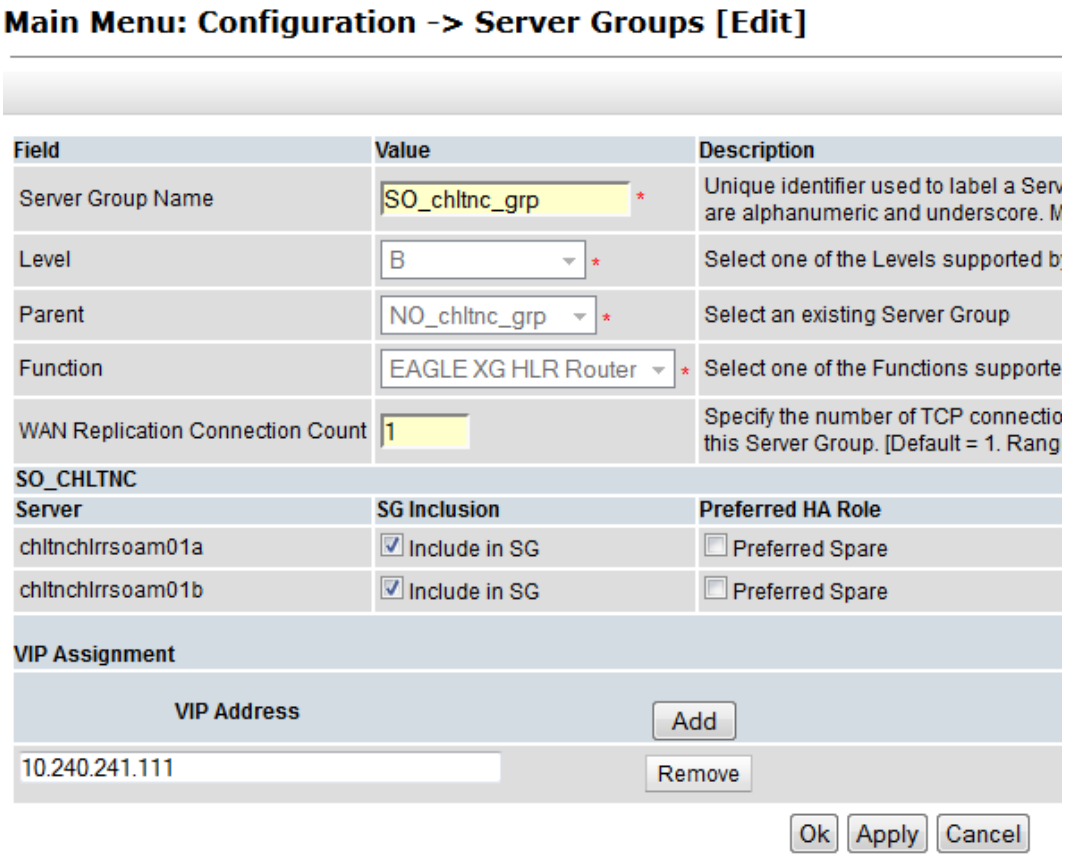
Procedure 17: OAM Pairing for SOAM or DR NOAM sites

Step	Procedure	Result
13. ☐	**Active NOAM VIP:** The **Server Group** entry should be shown on the **"Server Groups"** configuration screen as shown on the right.	
14. ☐	**NOAM Server A:** **1)** Select the **Server Group** entry created in **STEP 5 through STEP 11**. The line entry should now be highlighted in **GREEN**. **2)** Select the **"Edit"** button from the bottom left corner of the screen.	

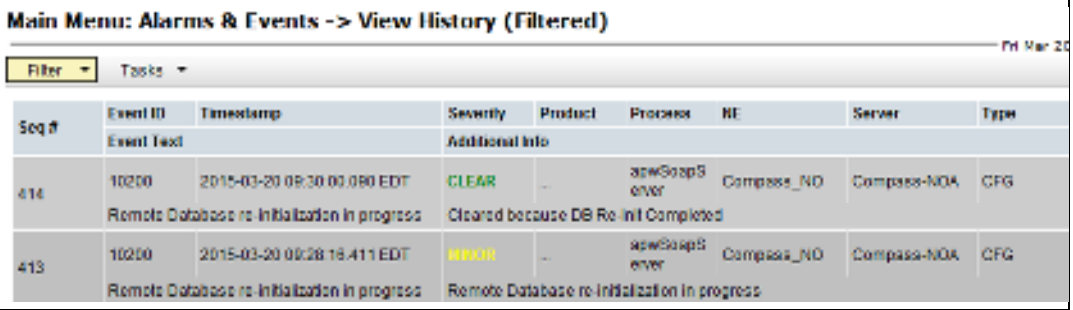
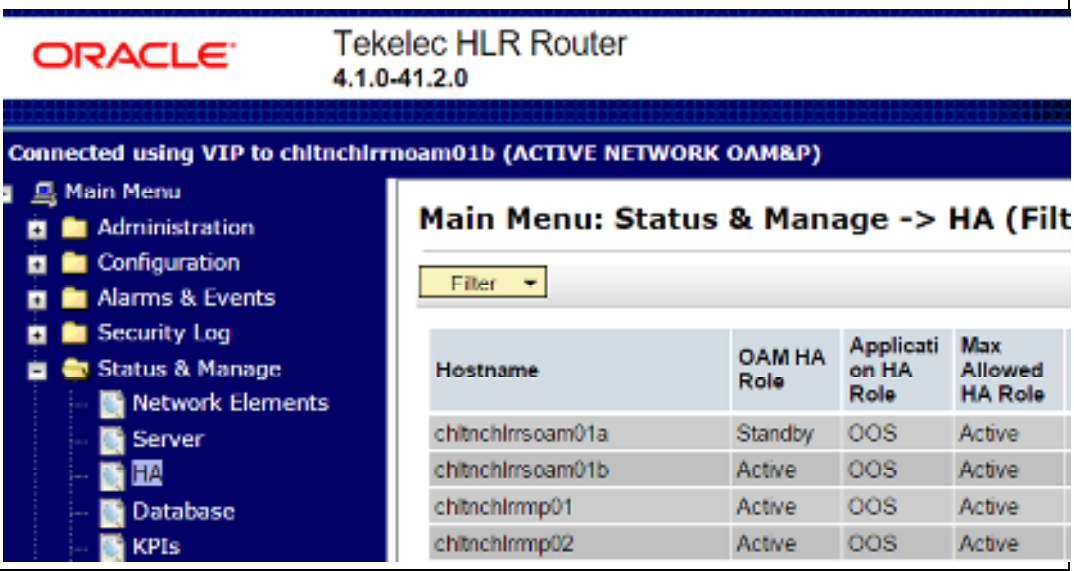
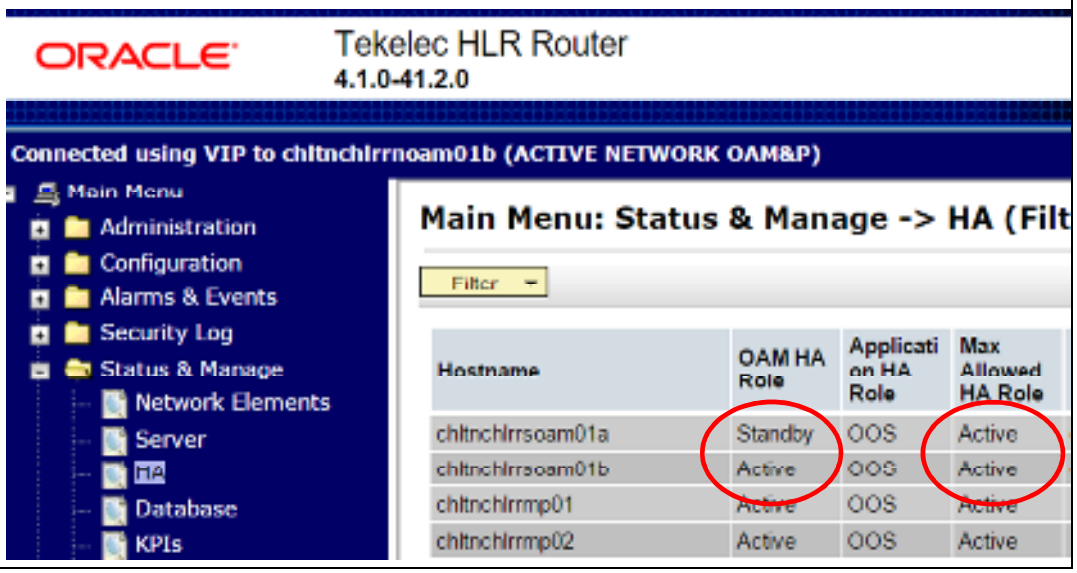
Procedure 17: OAM Pairing for SOAM or DR NOAM sites

Step	Procedure	Result
15. ☐	**Active NOAM VIP:** Adding a Server to the OAM Server Group (SOAM or DR NOAM) The user will be presented with the **"Server Groups [Edit]"** screen as shown on the right.	
16. ☐	**NOAM-A GUI:** **1)** Select **SOAM-A** and **SOAM-B or DR NOAM-A** and **DR NOAM-B** checkboxes from the **SG Inclusion** Field. **2)** Click "**Apply**" to submit the information.	

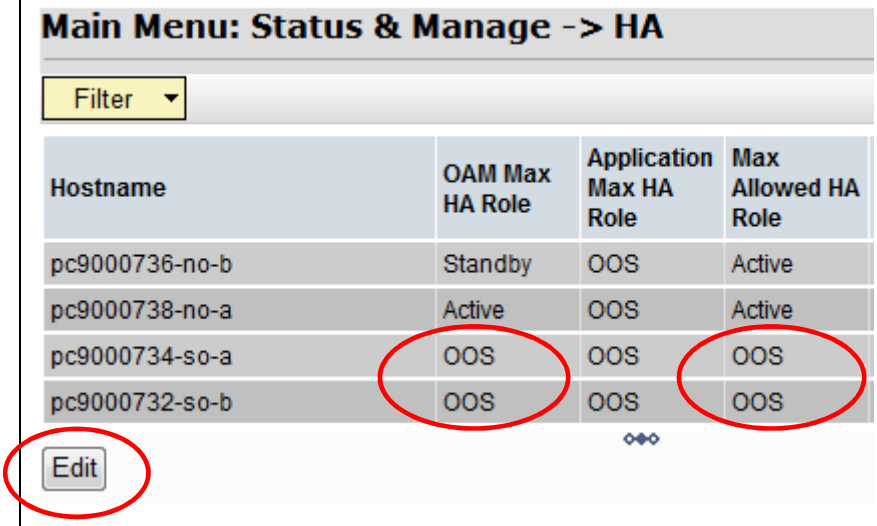
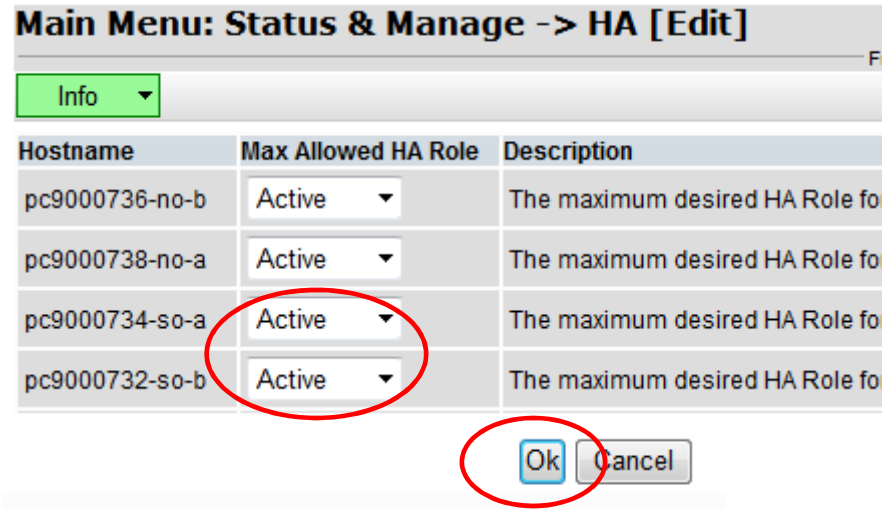
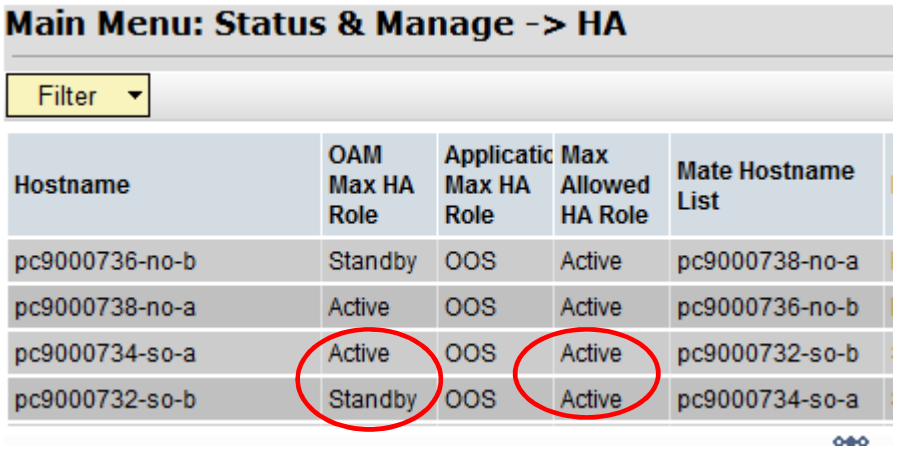
Procedure 17: OAM Pairing for SOAM or DR NOAM sites

Step	Procedure	Result
17. ☐	**NOAM-A GUI:** To add the virtual IP address, select **Add** in the **VIP Assignment** section.	
18. ☐	**NOAM-A GUI:** **1)** Enter the XMI virtual IP address in **VIP Address** field. **Note:** Use the NAPD documentation for this networking information. **2)** Select the **"OK"** dialogue button to commit the information.	
19. ☐	**IMPORTANT:** Wait a few minutes before proceeding on to the next step.	Now that the SOAM or DR NOAM servers 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.

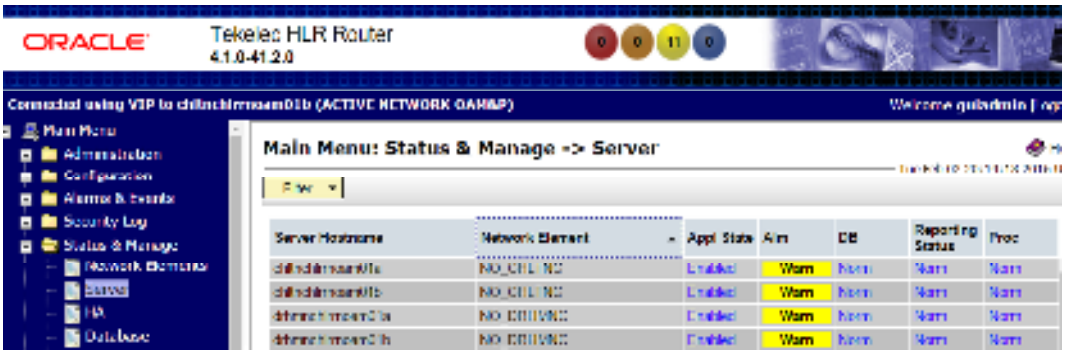
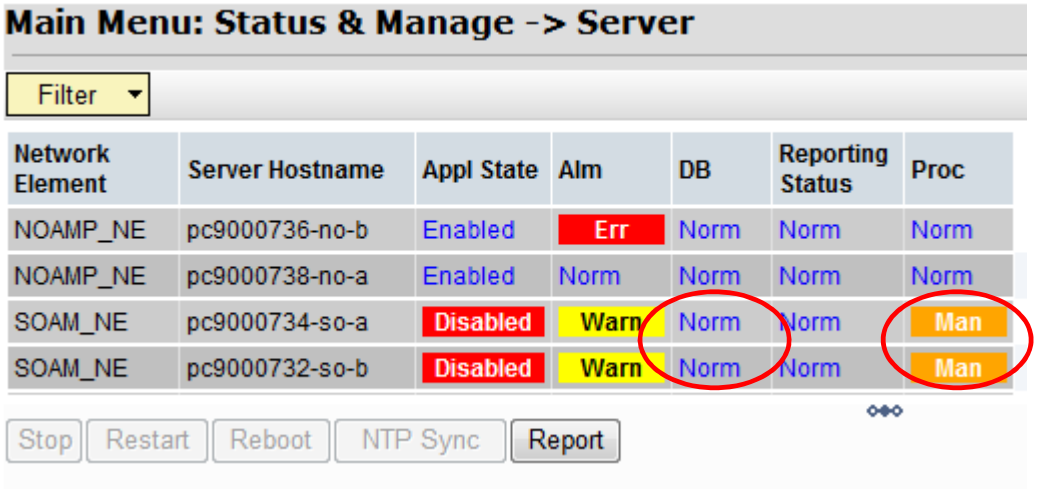
Procedure 17: OAM Pairing for SOAM or DR NOAM sites

Step	Procedure	Result
20. ☐	**NOAM VIP:** Wait for Remote Database Alarm to Clear.	Wait for alarm **10200 Remote Database re-initialization in progress** to clear for both the SOAM-A and SOAM-B or DR NOAM-A and DR NOAM-B before proceeding. Navigate to **Main menu->Alarms & Events->View Active** 
21. ☐	**Active NOAM VIP:** Select… **Main Menu** → **Status & Manage** → ***HA***	
22. ☐	**Active NOAM VIP:** Verify that the **OAM HA Role** shows **"Standby"** and **"Active"** and **Max Allowed HA Role** shows **"Active"** for SOAM or DR NOAM servers "A" and "B" If it shows **"OOS"** then continue with the next step. Otherwise skip forward to **Step 26** of this procedure.	

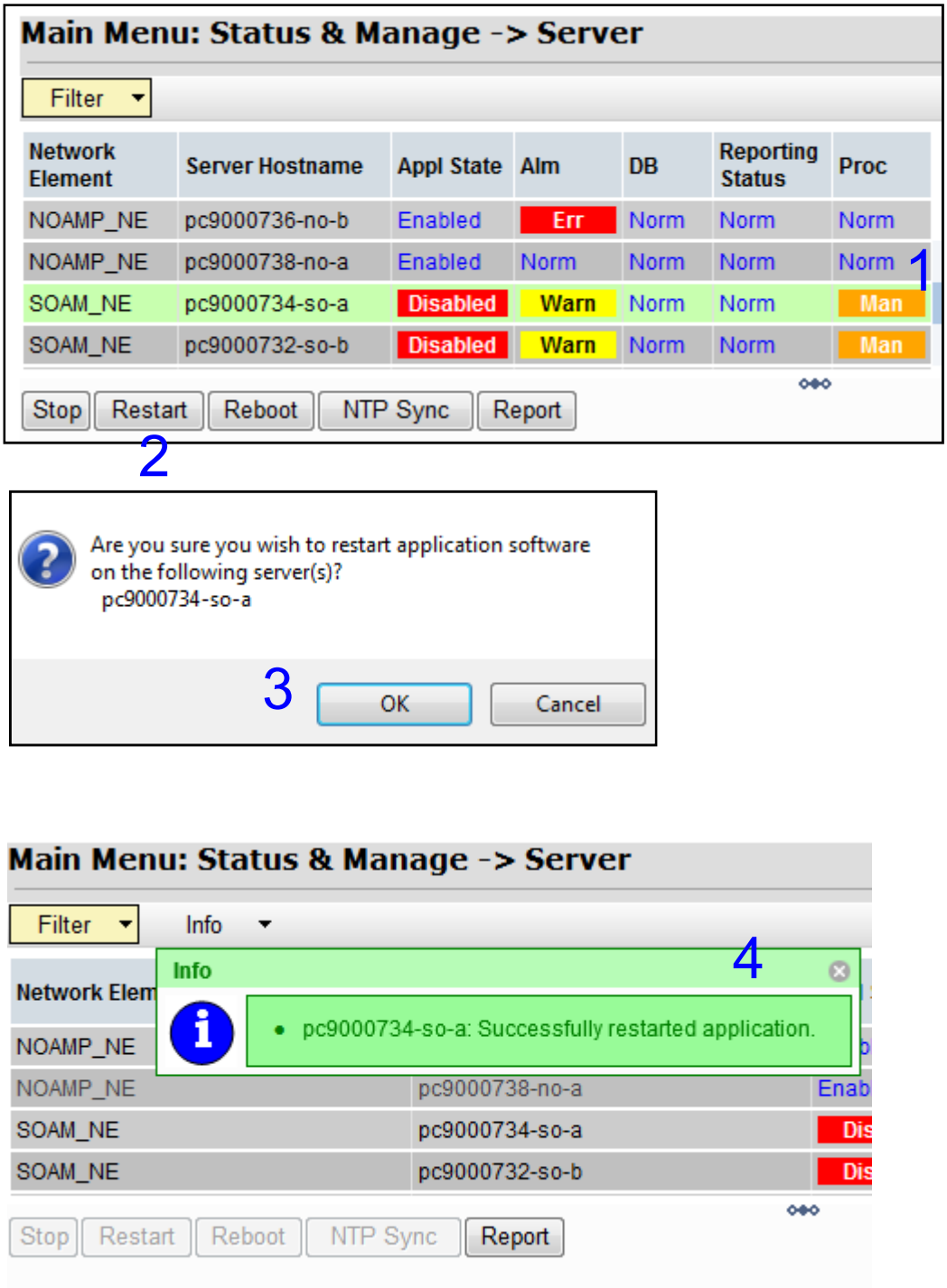
Procedure 17: OAM Pairing for SOAM or DR NOAM sites

Step	Procedure	Result
23. ☐	**Active NOAM VIP:** Click **Edit** button	
24. ☐	**Active NOAM VIP:** Change the **Max Allowed HA Role** for the SOAM or DR NOAM server(s) to **Active** and click the **OK** button.	
25. ☐	**Active NOAM VIP:** Verify that the **OAM HA Role** shows **"Standby"** and **"Active"** and **Max Allowed HA Role** shows **"Active"** for SOAM or DR NOAM servers "A" and "B"**.**	

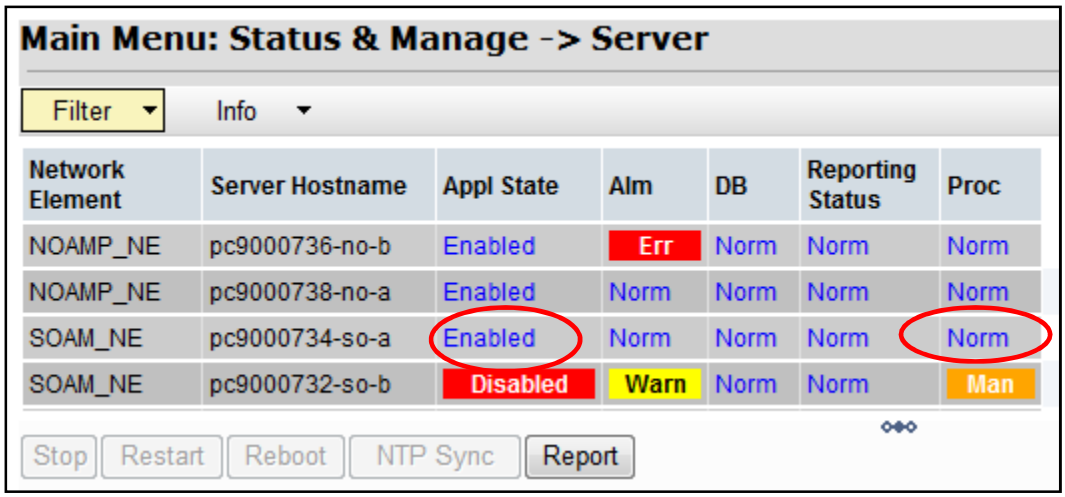
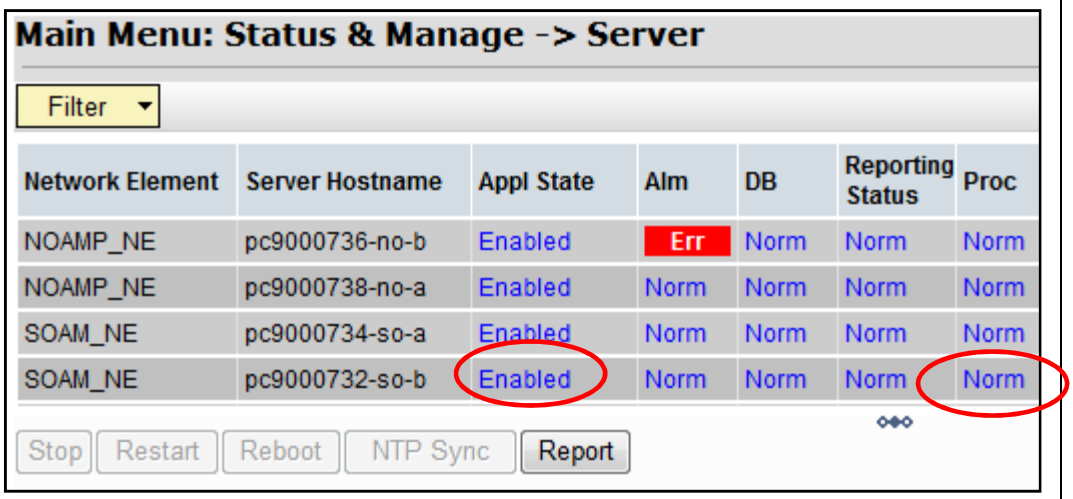
Procedure 17: OAM Pairing for SOAM or DR NOAM sites

Step	Procedure	Result
26. ☐	**Active NOAM VIP:** Restarting the OAM Server Application (SOAM) or DR NOAM Application. Select… **Main Menu** → **Status & Manage** → ***Server***	
27. ☐	**Active NOAM VIP:** **1)** SOAM or DR NOAM servers **"A"** and **"B"** should now appear in the right panel. **2)** Verify that the "**Appl State**" show "**Disabled**" and the **"DB"** status shows **"Norm"** and the **"Proc"** status shows **"Man"** for both servers before proceeding to the next step.	

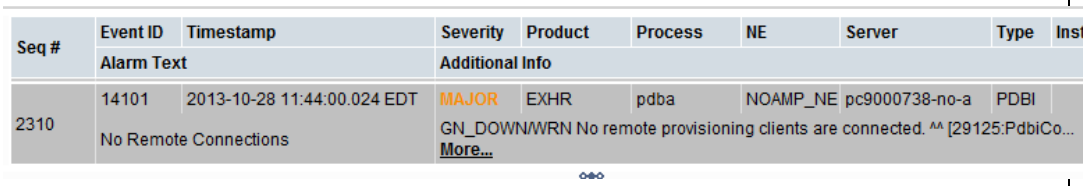
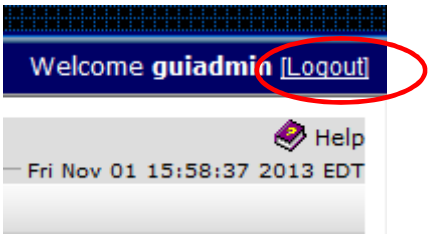
Procedure 17: OAM Pairing for SOAM or DR NOAM sites

Step	Procedure	Result
28. ☐	**Active NOAM VIP:** **1)** Select **SOAM-A or DR NOAM-A**. The line entry should now be highlighted in **GREEN**. **2)** Select the **"Restart"** dialogue button from the bottom left corner of the screen. **3)** Click the **"OK"** button on the confirmation dialogue box. **4)** The user should be presented with a confirmation message (in the banner area) for **SOAM or DR NOAM** stating: **"Successfully restarted application"**. **NOTE:** *The user may need to use the vertical scroll-bar in order to make the **"Restart"** dialogue button visible.*	

Procedure 17: OAM Pairing for SOAM or DR NOAM sites

Step	Procedure	Result
29. ☐	**Active NOAM VIP:** For **SOAM-A or DR NOAM-A** verify that the **"Appl State"** now shows **"Enabled"** and the **"Proc"** status column show **"Norm"** before proceeding to the next step.	
30. ☐	**Active NOAM VIP:** Repeat **Step 28** of this procedure for **SOAM-B or DR NOAM-B.**	Repeat **Step 28** of this Procedure for **SOAM Server B or DR NOAM-B.**
31. ☐	**Active NOAM VIP:** For **SOAM-B or DR NOAM-B** verify that the **"Appl State"** now shows **"Enabled"** and the **"Proc"** status column show **"Norm"** before proceeding to the next step.	

Procedure 17: OAM Pairing for SOAM or DR NOAM sites

Step	Procedure	Result
32. ☐	**NOAM VIP:** *Verifying the NOAM Server Alarm status* Select… **Main Menu** → **Alarms & Events** → ***View Active***	
33. ☐	**NOAM VIP:** Verify that **Event ID 14101** (“*No remote provisioning clients are connected”)* is the only alarm present on HLRR system at this time.	
34. ☐	**Active NOAM VIP:** Click the **“Logout”** link on the HLRR server GUI.	
Repeat this procedure for the DR SOAMs		
THIS PROCEDURE HAS BEEN COMPLETED		

7.6 Configuring MP Server Groups (All SOAM sites)

The user should be aware that during the Message Processor (MP) installation procedure, various errors may be seen at different stages of the procedure. During the execution of a step, the user is directed to ignore errors related to values other than the ones referenced by that step.

This procedure creates server groups for each MP.

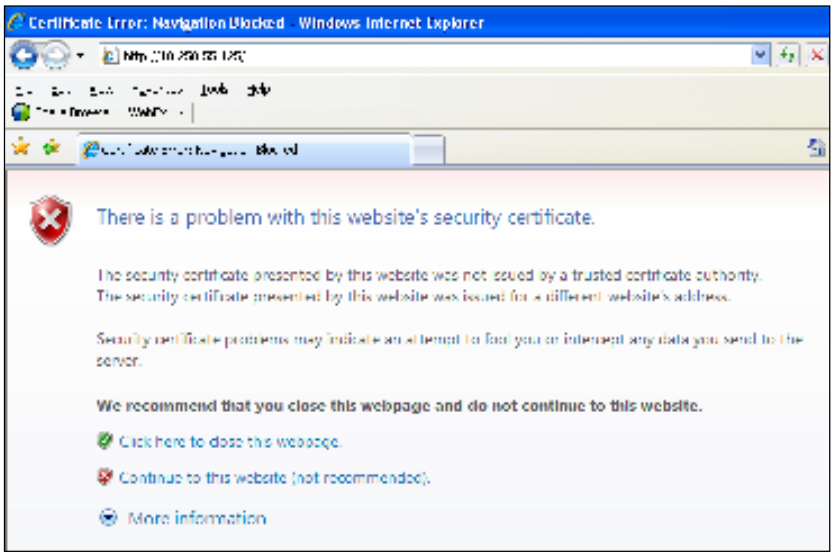
Requirements:

- **Procedure 14: Configuring Remaining HLRR Servers** has been completed.
- **Procedure 16: OAM Pairing for the Primary NOAM Servers** has been completed.
- **Procedure 17: OAM Pairing for SOAM or DR NOAM sites** has been completed.

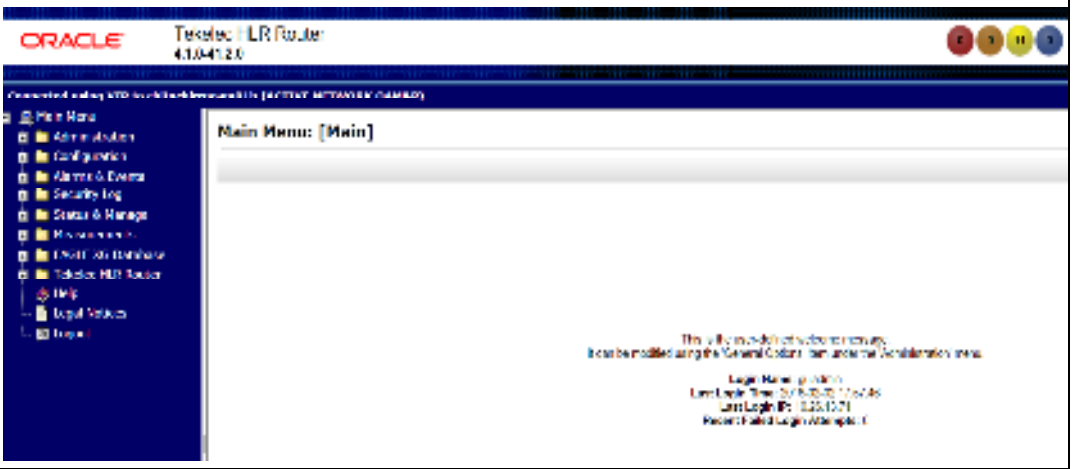
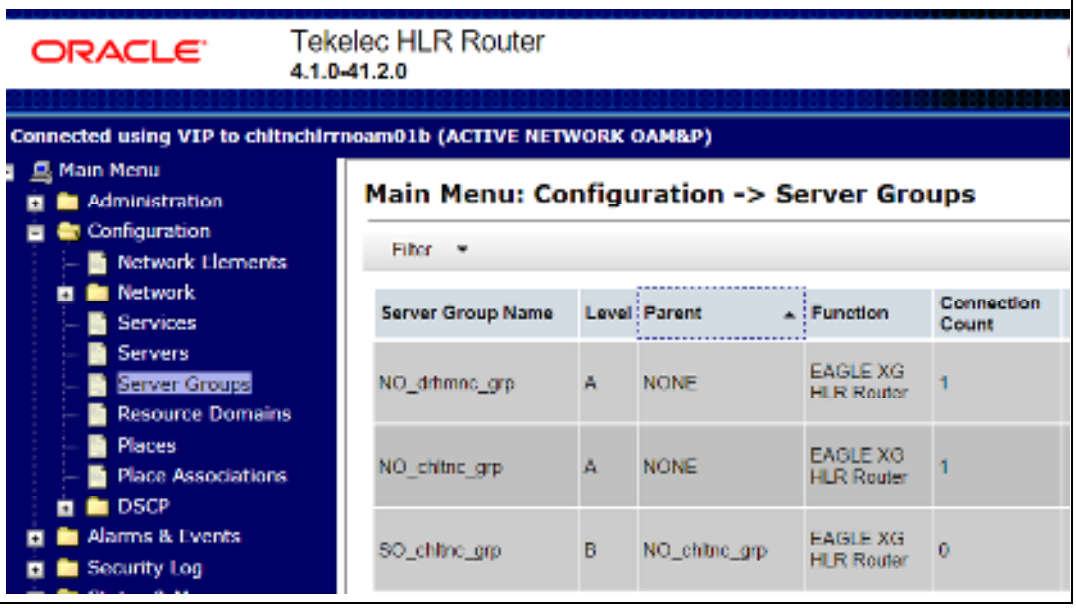
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

IF THIS PROCEDURE FAILS, CONTACT MY ORACLE SUPPORT AND ASK FOR ASSISTANCE.

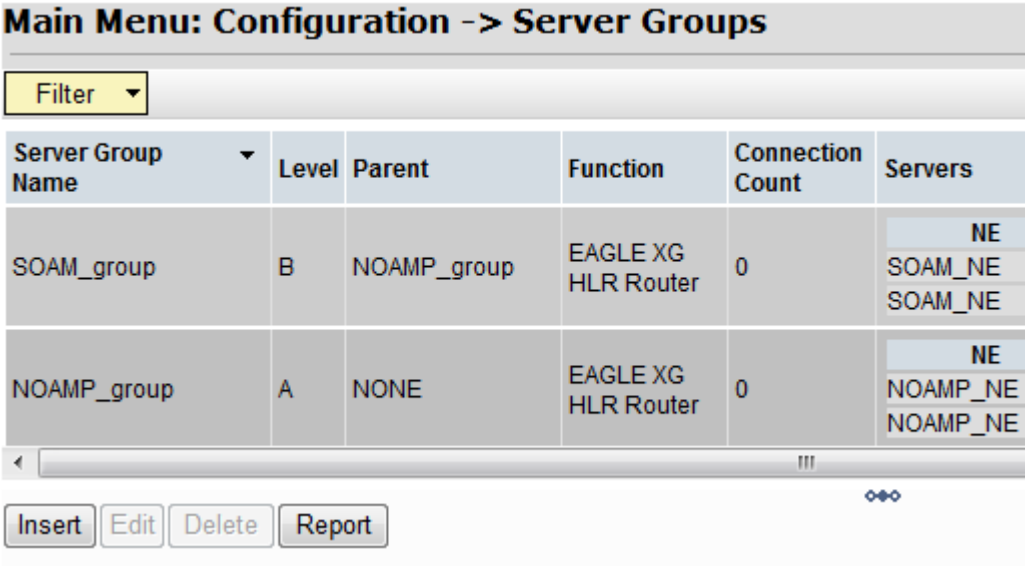
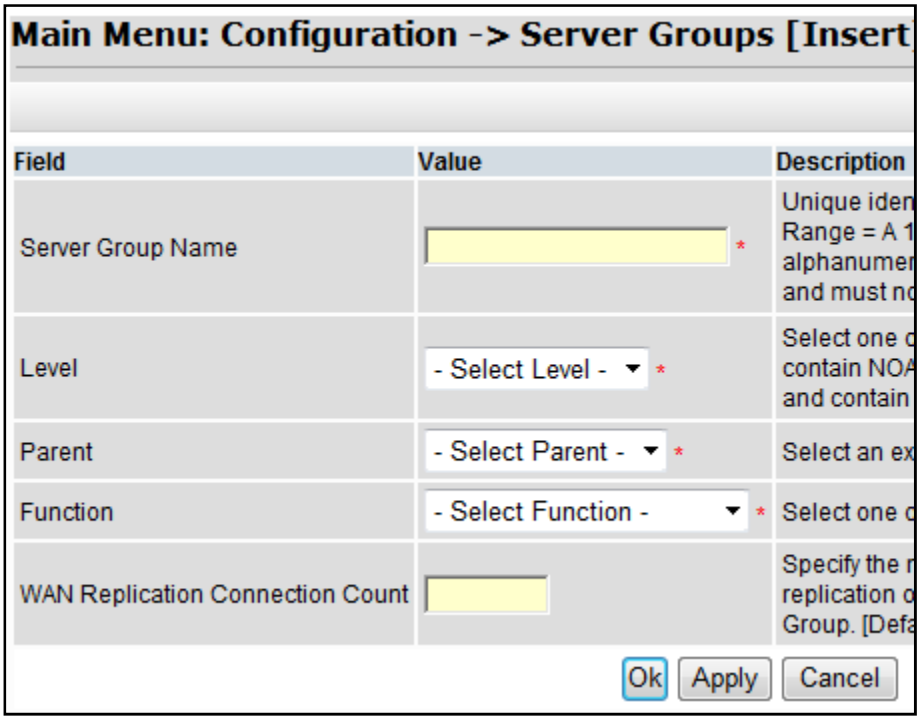
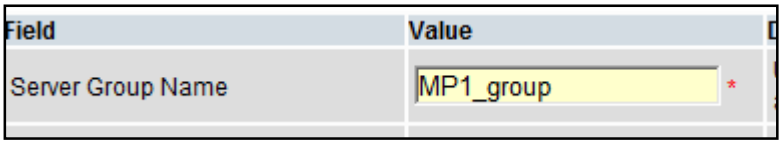
Procedure 18: Configuring MP Server Groups

Step	Procedure	Result
1. ☐	**Active NOAM VIP:** Launch an approved web browser and connect to the **XMI Virtual IP Address (VIP)** of the **Active NOAM site** using "https://"	

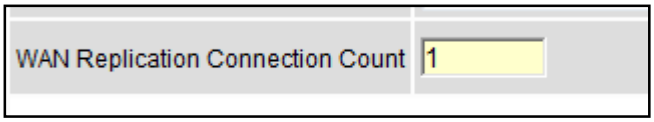
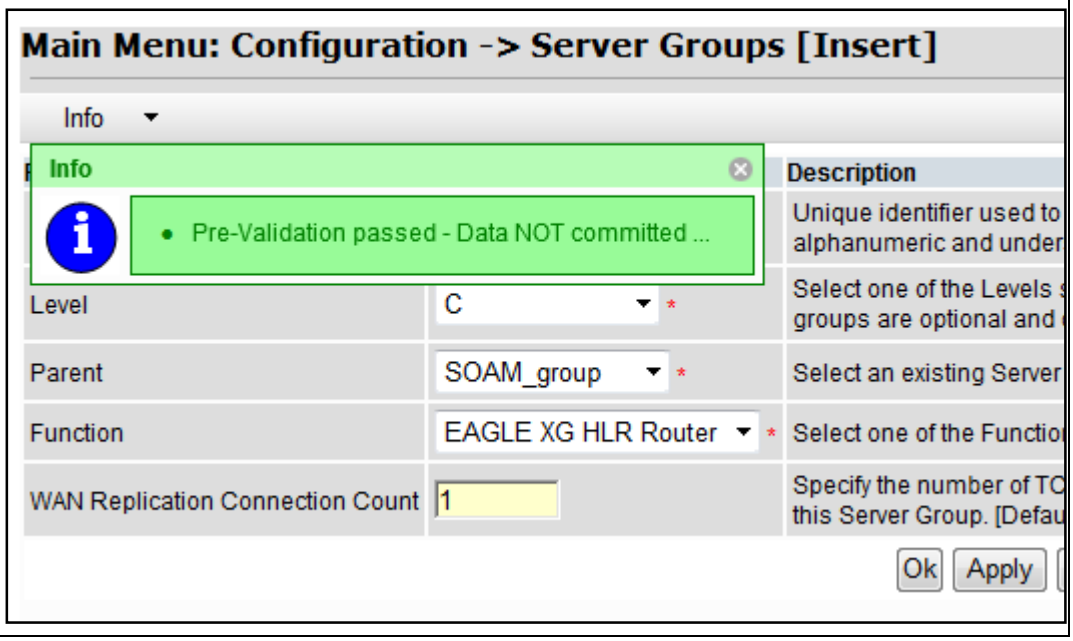
Procedure 18: Configuring MP Server Groups

Step	Procedure	Result
2. ☐	**Active NOAM VIP:** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	
3. ☐	**Active NOAM VIP:** The user should be presented the Main Menu as shown on the right.	
4. ☐	**Active NOAM VIP:** Select… **<u>Main Menu</u>** → **Configuration** → ***Server Groups***	

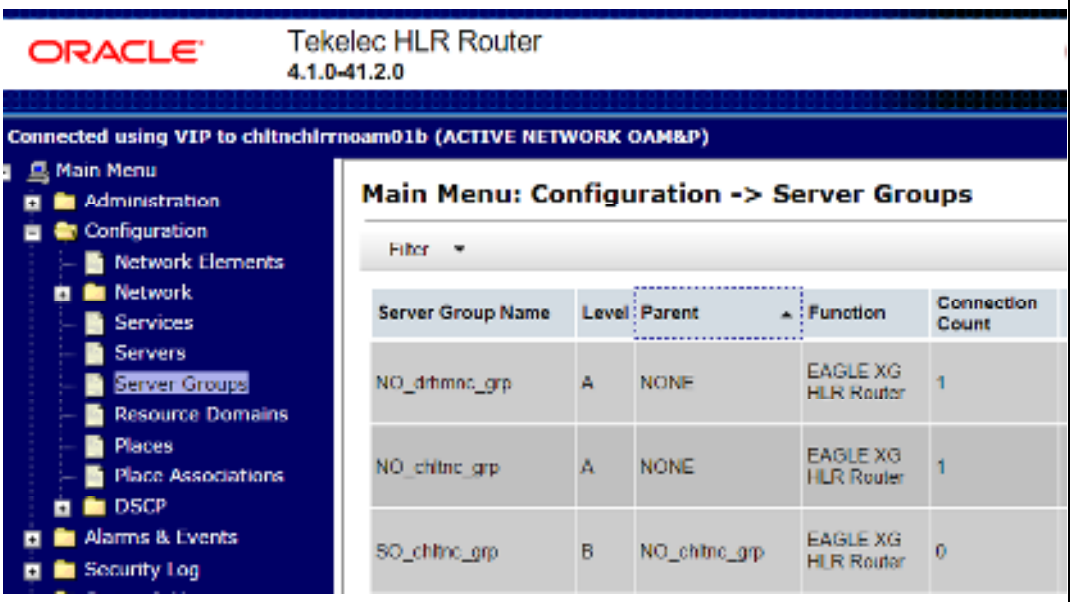
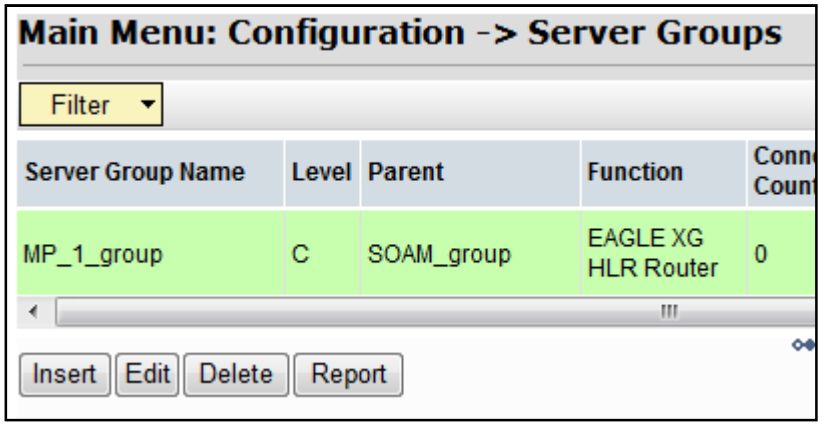
Procedure 18: Configuring MP Server Groups

Step	Procedure	Result
5. ☐	**Active NOAM VIP:** **1)** The user will be presented with the **"Server Groups"** configuration screen as shown on the right. **2)** Select the **"Insert"** dialogue button from the bottom left corner of the screen. **NOTE:** *The user may need to use the vertical scroll-bar in order to make the **"Insert"** dialogue button visible.*	
6. ☐	**Active NOAM VIP:** The user will be presented with the **"Server Groups [Insert]"** screen as shown on the right	
7. ☐	**Active NOAM VIP:** Input the **Server Group Name**.	

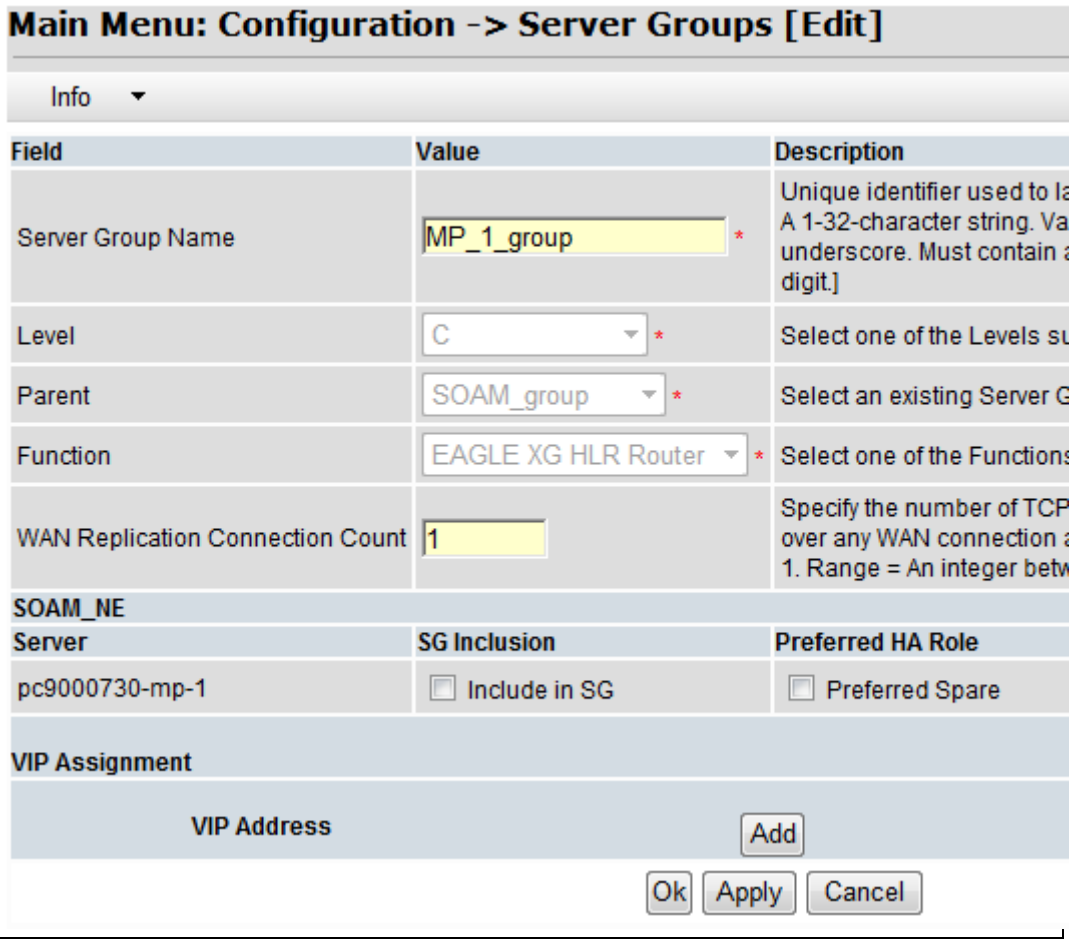
Procedure 18: Configuring MP Server Groups

Step	Procedure	Result
8. ☐	**Active NOAM VIP:** Select **"C"** on the **"Level"** pull-down menu.	
9. ☐	**Active NOAM VIP:** Select the desired SOAM server group on the **"Parent"** pull-down menu.	
10. ☐	**Active NOAM VIP:** Select "**EAGLE XG HLR Router**" on the "**Function**" pull-down menu.	
11. ☐	**Active NOAM VIP:** Enter a **WAN Replication Connection Count of "1"**	
12. ☐	**Active NOAM VIP:** **1)** The user should be presented with a banner information message stating **"Pre-Validation passed"**. **2)** Select the **"OK"** button to commit the data.	

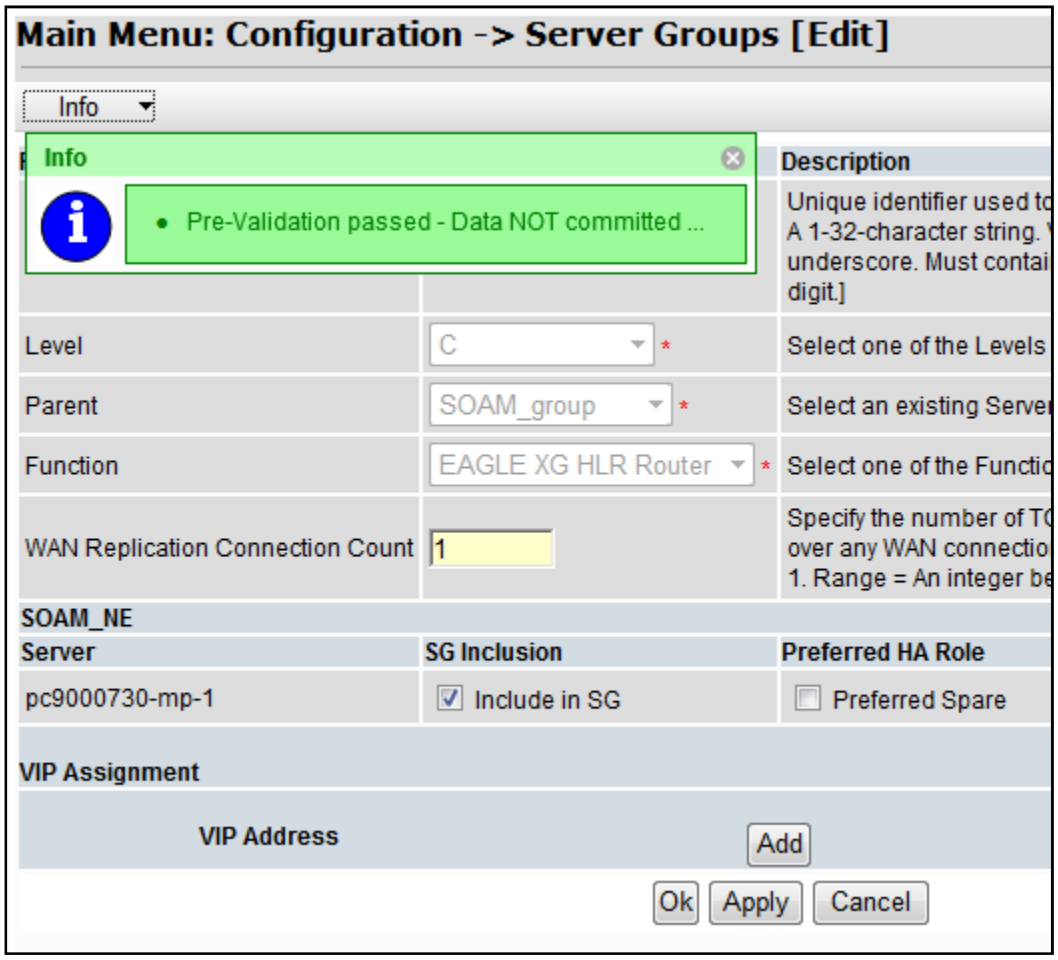
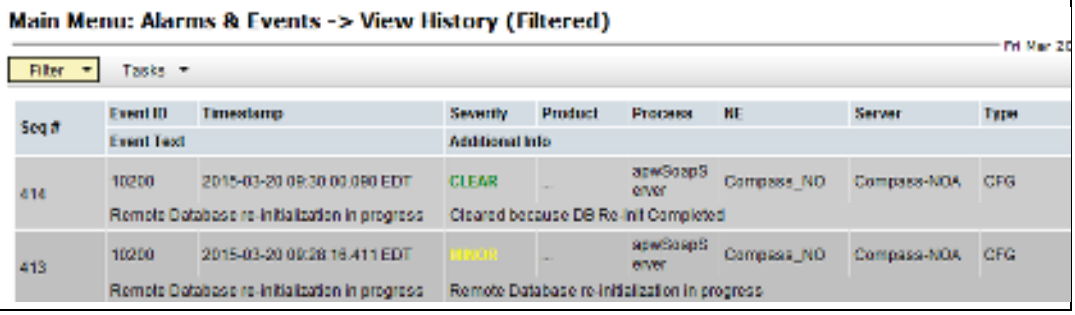
Procedure 18: Configuring MP Server Groups

Step	Procedure	Result
13. ☐	**Active NOAM VIP:** Select… **<u>Main Menu</u>** **→ Configuration** ***→ Server Groups***	
14. ☐	**Active NOAM VIP:** **1)** Select the MP Server Group associated with the MP being installed. **2)** Select the **"Edit"** dialogue button from the bottom left corner of the screen.	

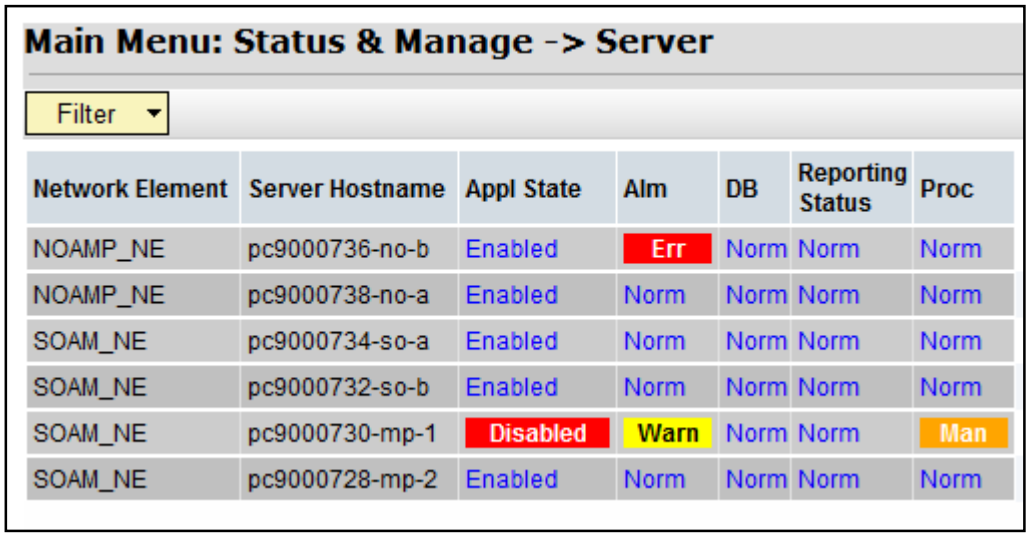
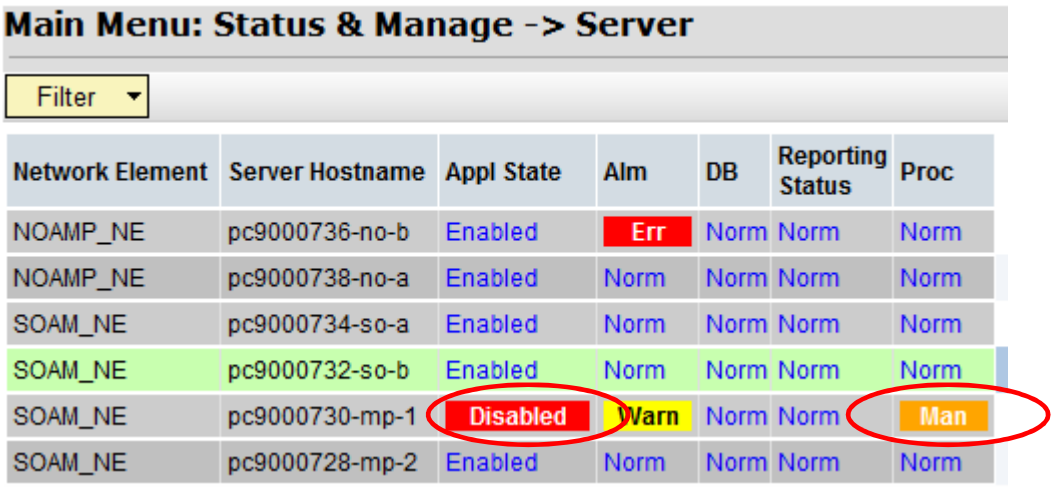
Procedure 18: Configuring MP Server Groups

Step	Procedure	Result
15. ☐	**Active NOAM VIP:** The user will be presented with the **"Configuration → Server Groups [Edit]"** screen as shown on the right	

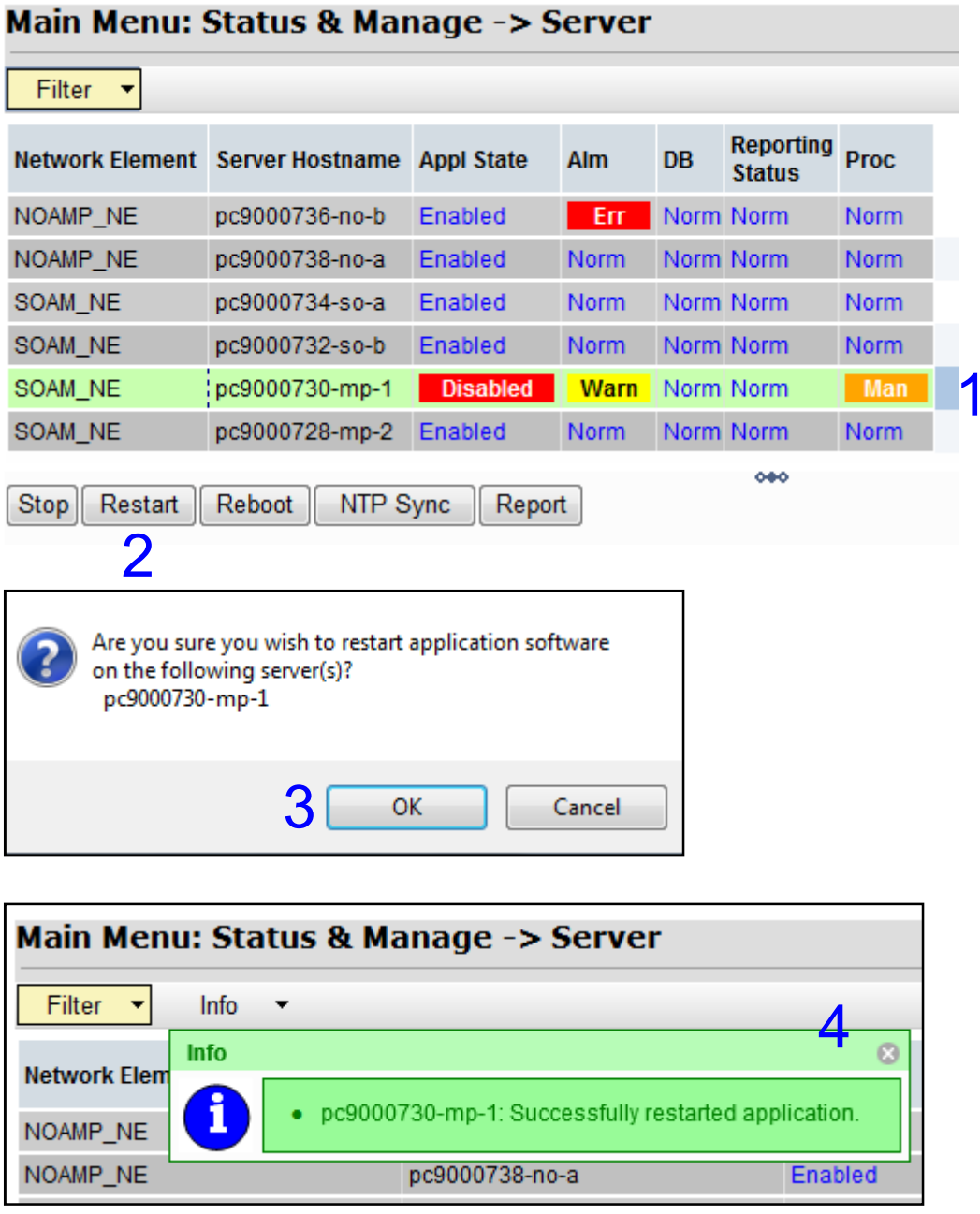
Procedure 18: Configuring MP Server Groups

Step	Procedure	Result
16. ☐	**Active NOAM VIP:** **1)** To add MP server to the server group, select the checkbox for **SG Inclusion**. When checked, the server will be included in the server group. **Note:** Only one MP is allowed per group. **2)** The user should be presented with a banner information message stating **"Pre-Validation passed"**. **3)** Select the **"OK"** dialogue button to commit the data.	
17. ☐	**NOAM VIP:** Wait for Remote Database Alarm to Clear for the MP.	Now that the Message Processor has been placed within a Server Group it must establish DB replication with the Active SOAM server. It may take several minutes for this process to be completed. Wait for alarm **10200 Remote Database re-initialization in progress** to clear for the MP before proceeding. Navigate to **Main menu->Alarms & Events->View Active** 

Procedure 18: Configuring MP Server Groups

Step	Procedure	Result
18. ☐	Repeat **Steps 4 - 17** of this procedure for each MP server installed in the same SOAM Network Element, ***using a unique group for each MP.*** **"Check off"** the associated **Check Box** for each MP as it is completed. **Primary Site:** ☐ MP-1 ☐ MP-2 ☐ MP-3 ☐ MP-4 ☐ MP-5 **Disaster Recovery Site (Optional):** ☐ MP-1 ☐ MP-2 ☐ MP-3 ☐ MP-4 ☐ MP-5	
19. ☐	**Active NOAM VIP:** Select… **<u>Main Menu</u>** → **Status & Manage** → ***Server***	
20. ☐	**Active NOAM VIP:** Verify that each MP: The "**Appl State**" shows "**Disabled**" The **"DB & Reporting Status"** columns all show **"Norm"** The **"Proc"** column should show **"Man"**.	

Procedure 18: Configuring MP Server Groups

Step	Procedure	Result
21. ☐	**Active NOAM VIP:** **1)** Using the mouse, select a **"MP"** hostname. The line entry should now be highlighted in **GREEN**. **2)** Select the **"Restart"** dialogue button from the bottom left corner of the screen. **3)** Click the **"OK"** button on the confirmation dialogue box. **4)** The user should be presented with a confirmation message (in the banner area) for the **"MP"** stating: **"Successfully restarted application"**. **NOTE:** *The user may need to use the vertical scroll-bar in order to make the **"Restart"** dialogue button visible.*	

Procedure 18: Configuring MP Server Groups

Step	Procedure	Result
22. ☐	**Active NOAM VIP:** Select… **Main Menu** → **Status & Manage** → ***Server***	
23. ☐	**Active NOAM VIP:** Verify that the **"Appl State"** now shows **"Enabled"** Verify that the **"Alm, DB, Reporting Status & Proc"** status columns all show **"Norm"** for the **"MP"**.	**Main Menu: Status & Manage -> Server** Filter Network Element / Server Hostname / Appl State / Alm / DB / Reporting Status / Proc NOAMP_NE / pc9000736-no-b / Enabled / Err / Norm / Norm / Norm NOAMP_NE / pc9000738-no-a / Enabled / Norm / Norm / Norm / Norm SOAM_NE / pc9000734-so-a / Enabled / Norm / Norm / Norm / Norm SOAM_NE / pc9000732-so-b / Enabled / Norm / Norm / Norm / Norm SOAM_NE / pc9000730-mp-1 / Enabled / Norm / Norm / Norm / Norm
24. ☐	**Repeat Steps 19 through 23 of this procedure for each additional MP server installed on the SOAM NE.** **"Check off"** the associated **Check Box** for each MP as it is completed. **Primary Site:** ☐ MP-1 ☐ MP-2 ☐ MP-3 ☐ MP-4 ☐ MP-5 **Disaster Recovery Site (Optional):** ☐ MP-1 ☐ MP-2 ☐ MP-3 ☐ MP-4 ☐ MP-5	
25. ☐	**Optional: Repeat this procedure for the Disaster Recovery MP servers.**	
THIS PROCEDURE HAS BEEN COMPLETED		

7.7 Configure MP Signaling Interfaces (All SOAM Sites)

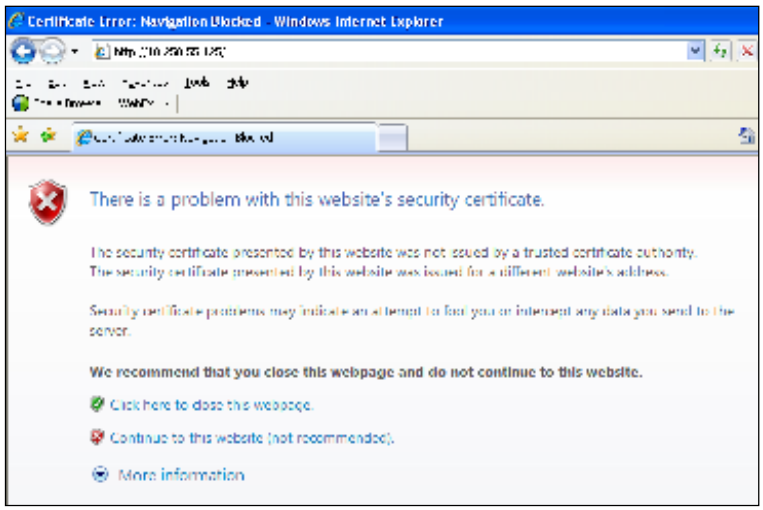
This procedure configures XSI-1 and XSI-2 IP Interfaces plus (OPTIONAL: XSI-3 and XSI-4) and adds the XSI signaling routes for all MP Servers

Requirements: Procedure 18: Configuring MP Server Groups has been completed.

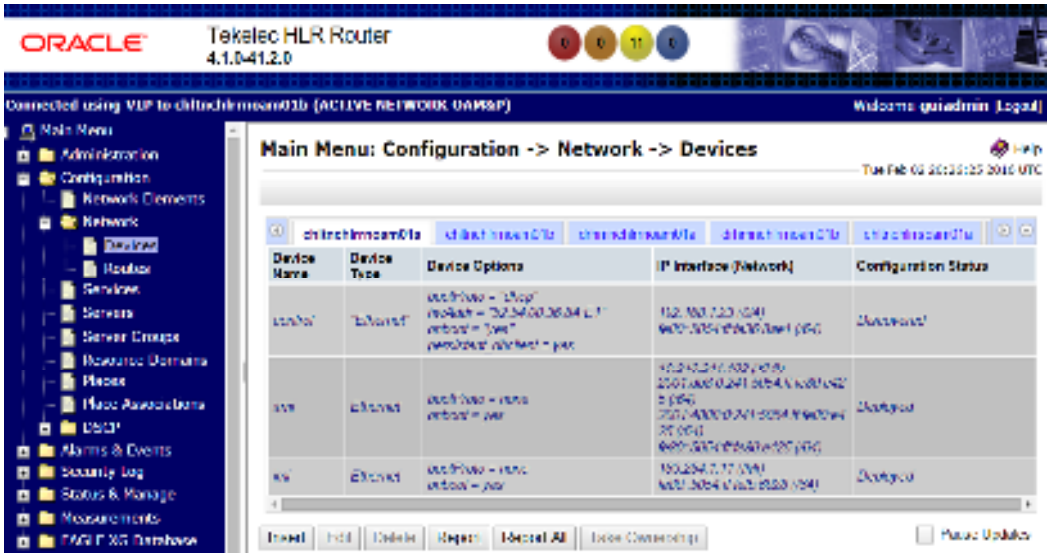
Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

IF THIS PROCEDURE FAILS, PLEASE CONTACT ORACLE'S CUSTOMER CARE CENTER FOR THE ASSISTANCE.

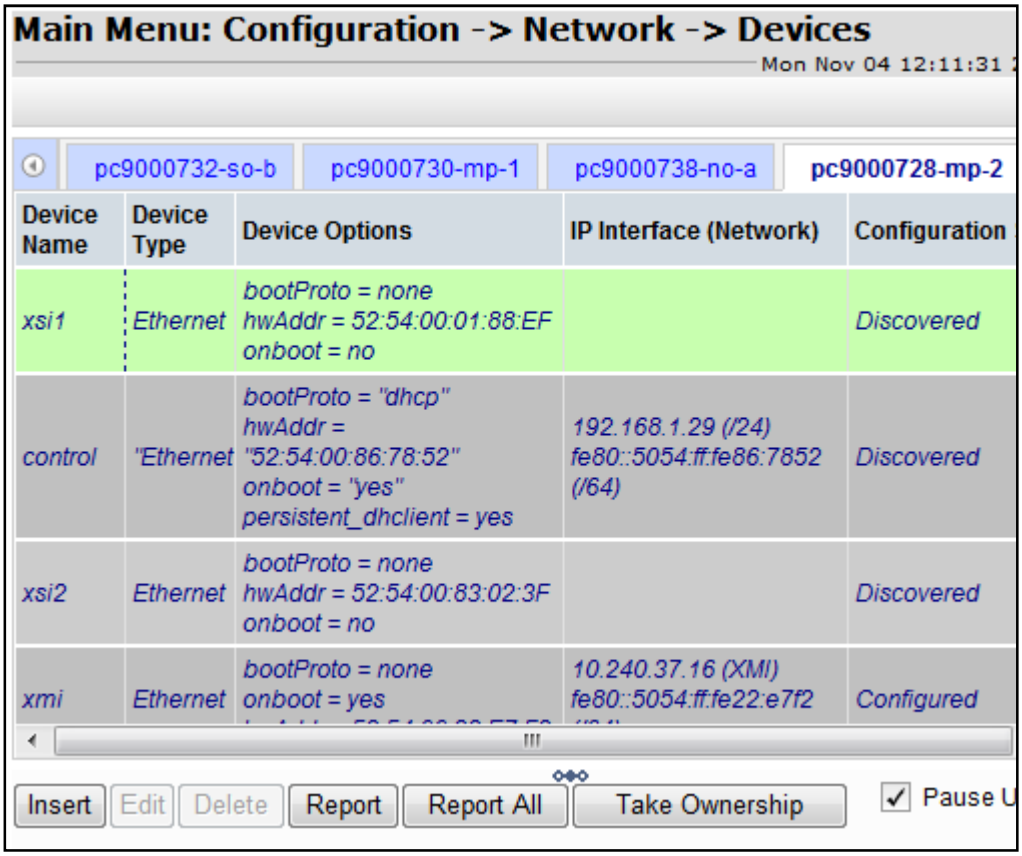
Procedure 19: Configure MP Signaling Interfaces

Step	Procedure	Result
1. ☐	**Active NOAM VIP** Launch an approved web browser and connect to the **XMI Virtual IP Address (VIP)** of the **Active NOAM site** using "https://"	
2. ☐	**Active NOAM VIP** The user should be presented the login screen shown on the right. Login to the GUI using the default user and password.	

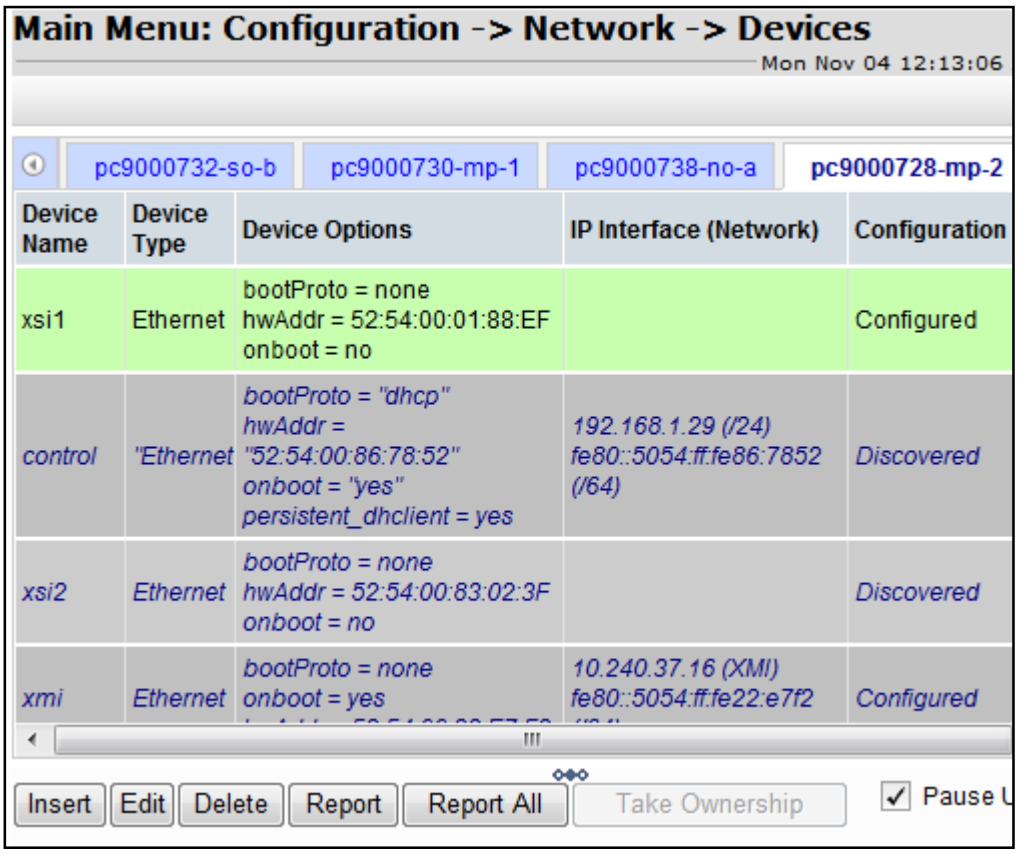
Procedure 19: Configure MP Signaling Interfaces

Step	Procedure	Result
3. ☐	**Active NOAM VIP** The user should be presented the HLRR Main Menu as shown on the right.	
4. ☐	**Active NOAM VIP** Select… **<u>Main Menu</u>** **→ Configuration** **→ *Network*** **→ *Devices***	

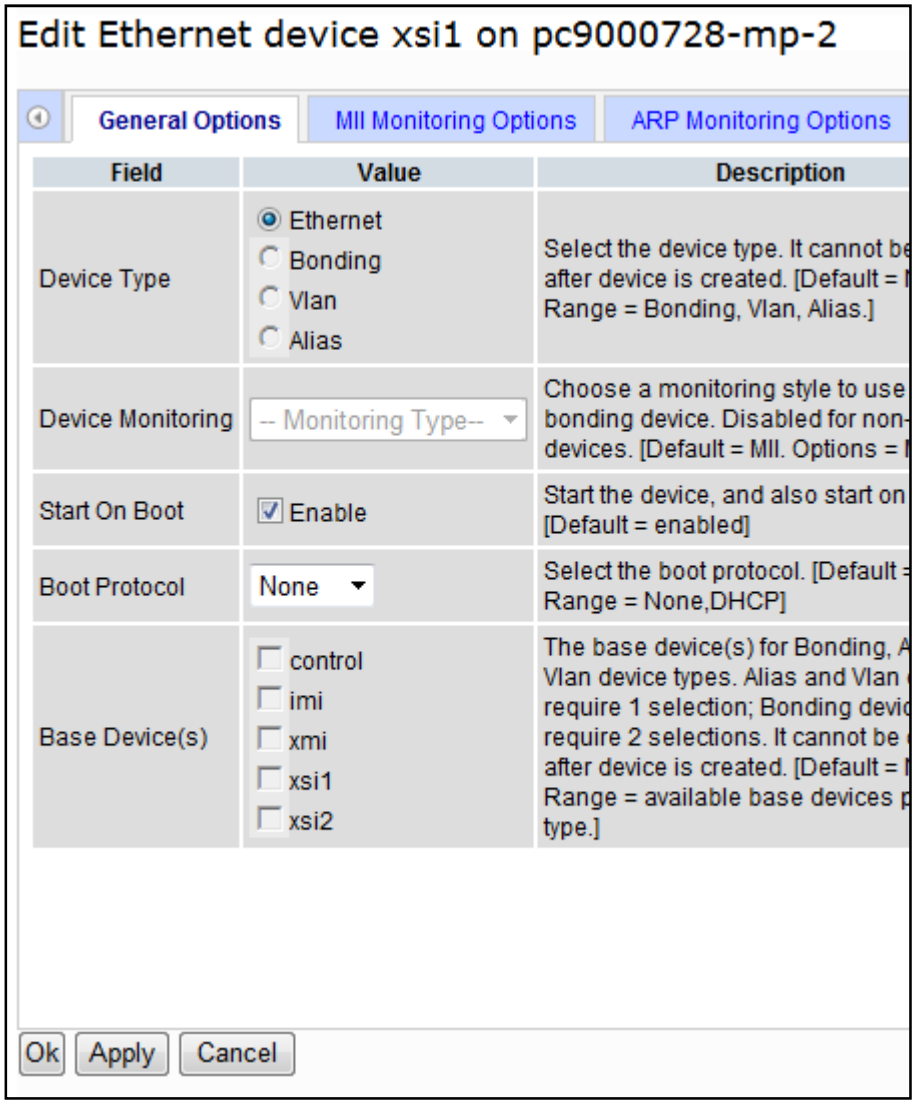
Procedure 19: Configure MP Signaling Interfaces

Step	Procedure	Result
5. ☐	**Active NOAM VIP** Take ownership of the XSI 1 device for the desired MP.	Click on the desired **MP** tab. Select the **XSI 1** device. Output similar to that shown below may be observed. 

Procedure 19: Configure MP Signaling Interfaces

Step	Procedure	Result
6. ☐	**Active NOAM VIP** Edit the XSI 1 device for the desired MP.	Click on the desired **MP** tab. Select the **XSI 1** device. Output similar to that shown below may be observed. Select the **Edit** button at the bottom of the screen. 

Procedure 19: Configure MP Signaling Interfaces

Step	Procedure	Result
7. ☐	**Active NOAM VIP** Enable "Start On Boot"	Click on the **General Options** tab. Check the **Start on Boot** check box (to make it enabled). Output similar to that shown below may be observed. 

Procedure 19: Configure MP Signaling Interfaces

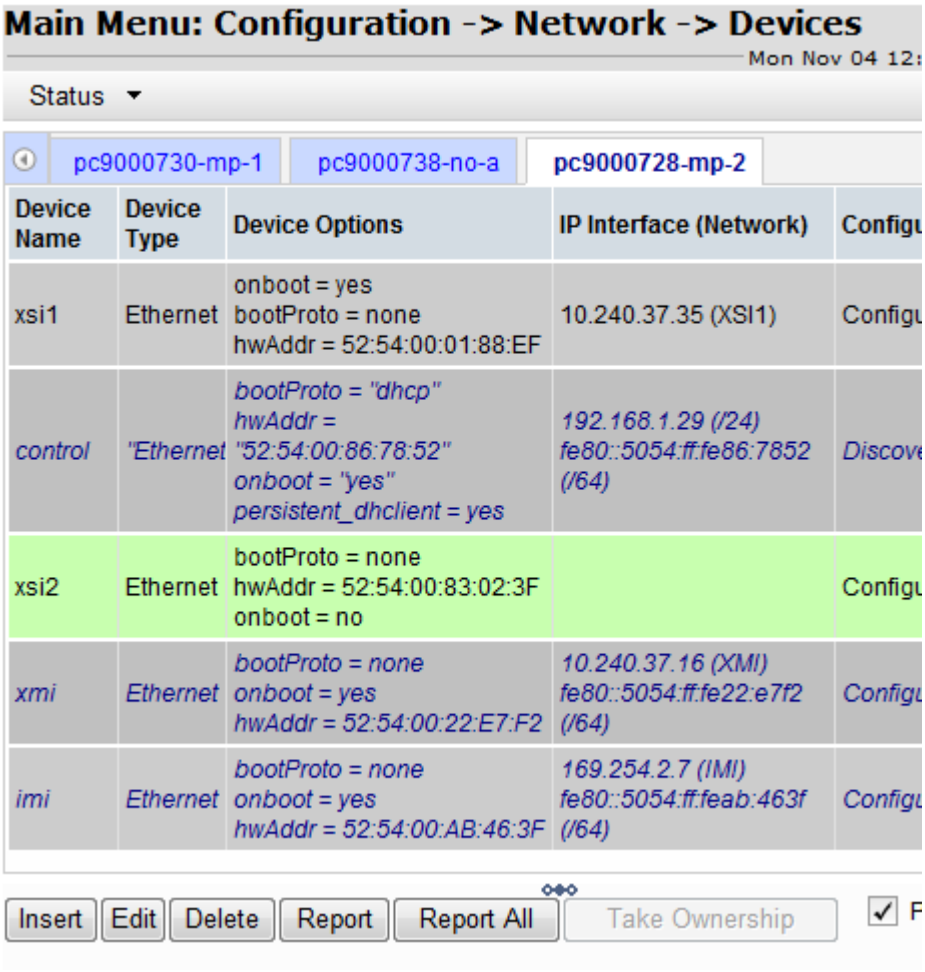
Step	Procedure	Result
8. ☐	**Active NOAM VIP** Add an XSI1 IP Address.	Click on the **IP Interfaces** tab. Click the **Add Row** button. Enter the **XSI1 Signaling IP Address.** Set the Network Name to **XSI1** from the pull-down list. Click on the **Ok** button. Output similar to that shown below may be observed. 

Procedure 19: Configure MP Signaling Interfaces

Step	Procedure	Result
9. ☐	**Active NOAM VIP** Take ownership of the XSI 2 device for the desired MP.	Click on the desired **MP** tab. Select the **XSI 2** device. Click on the **Take Ownership** button. Output similar to that shown below may be observed. **Main Menu: Configuration -> Network -> Devices** Mon Nov 04 pc9000732-so-b | pc9000730-mp-1 | pc9000738-no-a | pc9000 Device Name / Device Type / Device Options / IP Interface (Network) / Co xsi1 / Ethernet / onboot = yes, bootProto = none, hwAddr = 52:54:00:01:88:EF / 10.240.37.35 (XSI1) / Co *control* / *"Ethernet* / *bootProto = "dhcp"*, *hwAddr = "52:54:00:86:78:52"*, *onboot = "yes"*, *persistent_dhclient = yes* / *192.168.1.29 (/24)*, *fe80::5054:ff:fe86:7852 (/64)* / *Dis* *xsi2* / *Ethernet* / *bootProto = none*, *hwAddr = 52:54:00:83:02:3F*, *onboot = no* / / *Dis* *xmi* / *Ethernet* / *bootProto = none*, *onboot = yes*, *hwAddr = 52:54:00:22:E7:F2* / *10.240.37.16 (XMI)*, *fe80::5054:ff:fe22:e7f2 (/64)* / *Co* *imi* / *Ethernet* / *bootProto = none*, *onboot = yes*, *hwAddr = 52:54:00:AB:46:3F* / *169.254.2.7 (IMI)*, *fe80::5054:ff:feab:463f (/64)* / *Co* Insert | Edit | Delete | Report | Report All | Take Ownership

Procedure 19: Configure MP Signaling Interfaces

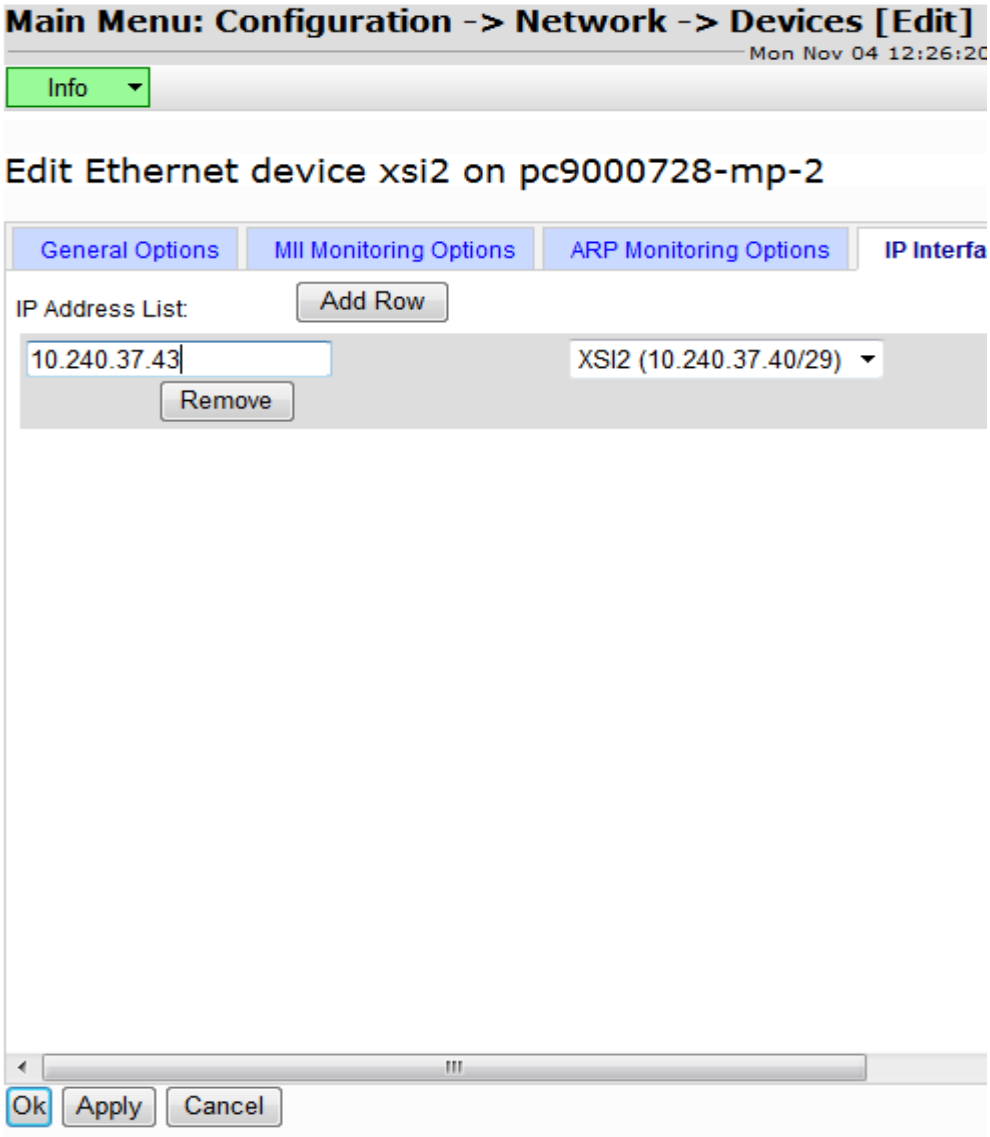
Step	Procedure	Result
10. ☐	**Active NOAM VIP** Edit the XSI 2 device for the desired MP.	Click on the desired **MP** tab. Select the **XSI 2** device. Click on the **Edit** button. Output similar to that shown below may be observed.



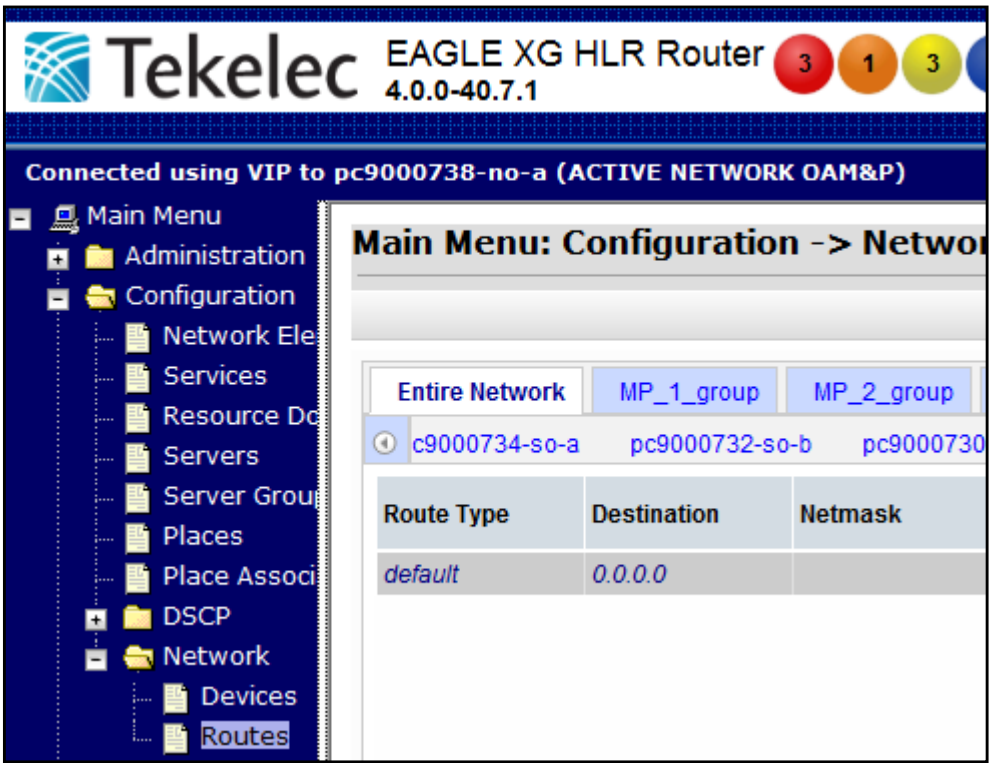
Procedure 19: Configure MP Signaling Interfaces

Step	Procedure	Result
11. ☐	**Active NOAM VIP** Enable "Start On Boot"	Click on the **General Options** tab. Check the **Start on Boot** check box (to make it enabled). Output similar to that shown below may be observed.

Procedure 19: Configure MP Signaling Interfaces

Step	Procedure	Result
12. ☐	**Active NOAM VIP** Add an XSI 2 IP Address.	Click on the **IP Interfaces** tab. Click the **Add Row** button. Enter the **XSI2 Signaling IP Address.** Set the Network Name to **XSI2** from the pull-down list. Click on the **Ok** button. Output similar to that shown below may be observed. 
13. ☐	**Optional for DL380 Servers Only: Repeat steps 4-8 to add XSI-3 and XSI-4.**	

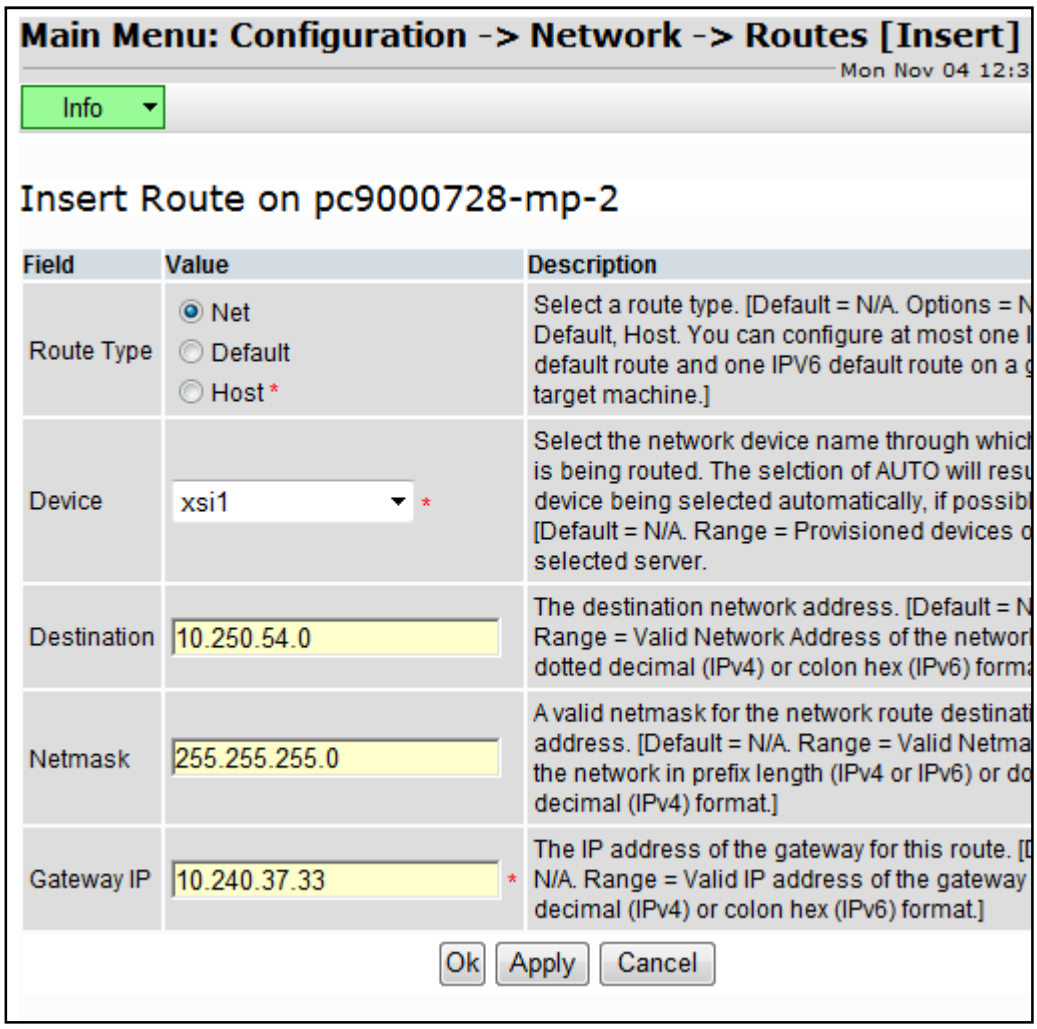
Procedure 19: Configure MP Signaling Interfaces

Step	Procedure	Result
14. ☐	**Repeat STEPS 4 through 12 (optional 13) for each MP.** • **"Check off"** the associated **Check Box** as each MP is completed. **Primary Site:** ☐ MP-1 ☐ MP-2 ☐ MP-3 ☐ MP-4 ☐ MP-5 **Disaster Recovery Site (Optional):** ☐ MP-1 ☐ MP-2 ☐ MP-3 ☐ MP-4 ☐ MP-5	
15. ☐	**Active NOAM VIP** Select… **Main Menu** → **Configuration** → ***Network*** → ***Routes***	

Procedure 19: Configure MP Signaling Interfaces

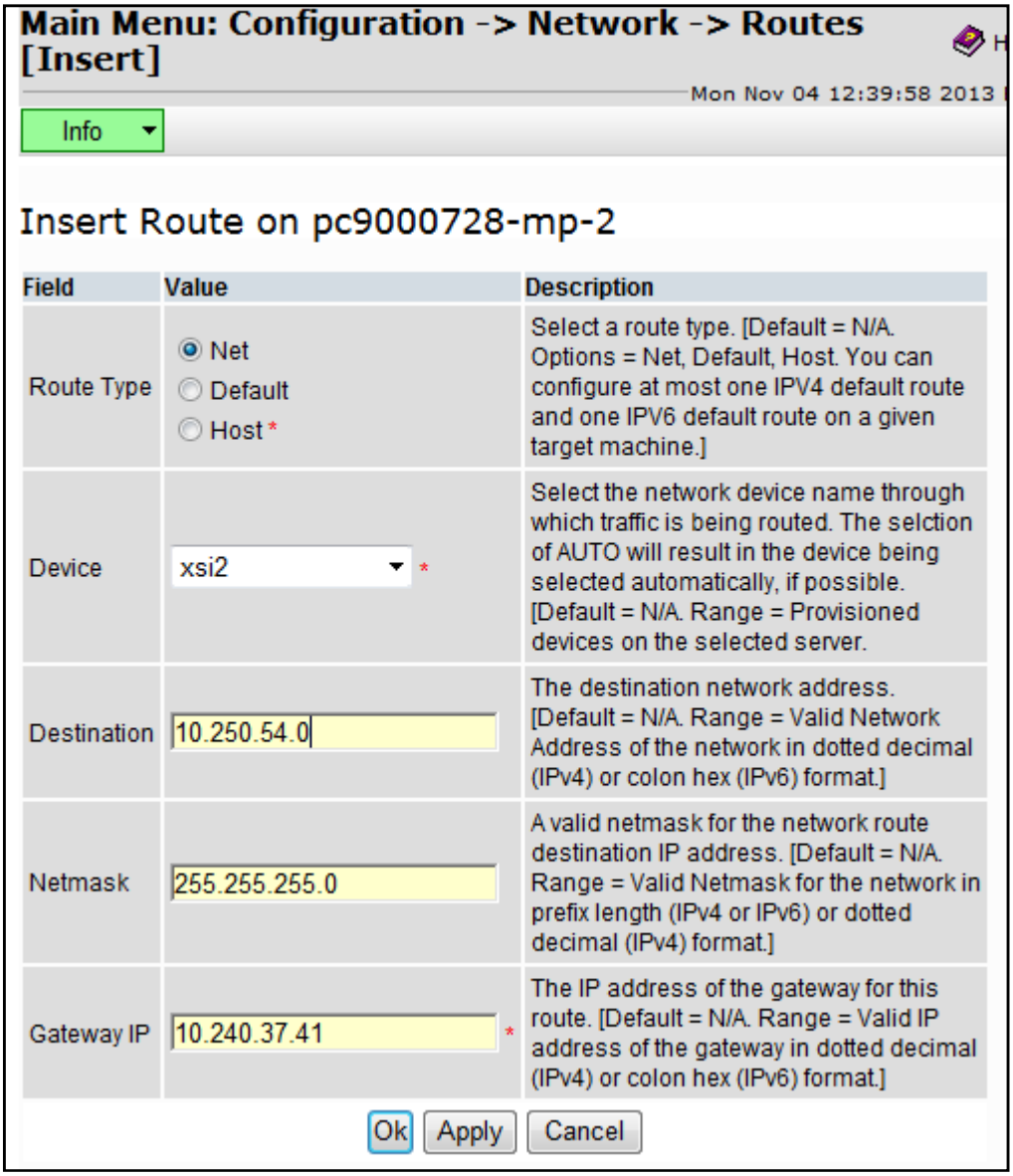
Step	Procedure	Result
16. ☐	**Active NOAM VIP** Insert a new route for the MP.	Click on the desired **MP** tab. Output similar to that shown below may be observed.  Click on the **Insert** button

Procedure 19: Configure MP Signaling Interfaces

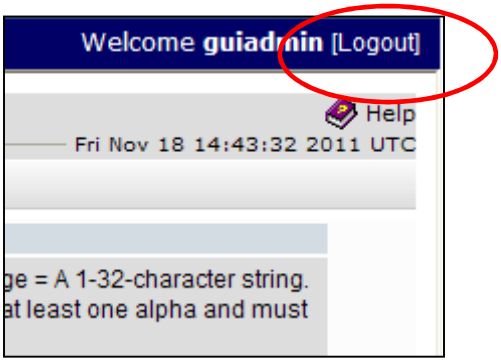
Step	Procedure	Result
17. ☐	**Active NOAM VIP** Add XSI1 signaling route to MP	Set **Route Type** to desired value Set **Device** to **XSI1** Enter **Destination, Netmask** and **Gateway IP** values for XSI1. Click **Apply** button. Output similar to that shown below may be observed. 

Procedure 19: Configure MP Signaling Interfaces

Step	Procedure	Result
18. ☐	**Active NOAM VIP** Add XSI2 signaling route to MP	Set **Route Type** to desired value Set **Device** to **XSI2** Enter **Destination, Netmask** and **Gateway IP** values for XSI2. Click **Apply** button. Output similar to that shown below may be observed.
19. ☐	**Optional for DL380 Servers Only: Repeat steps 15-17 to add routes for XSI-3 and XSI-4.**	

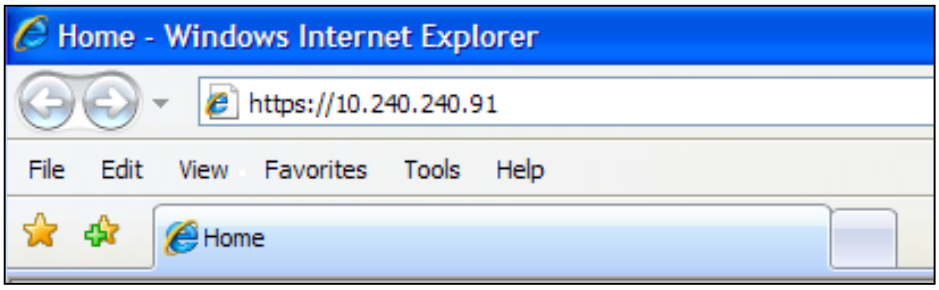
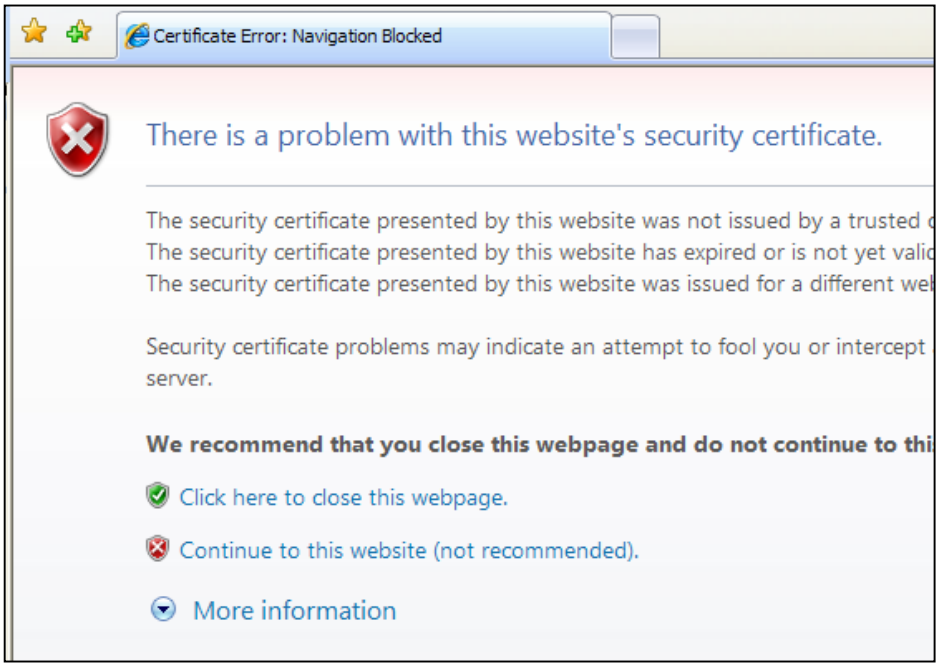


Procedure 19: Configure MP Signaling Interfaces

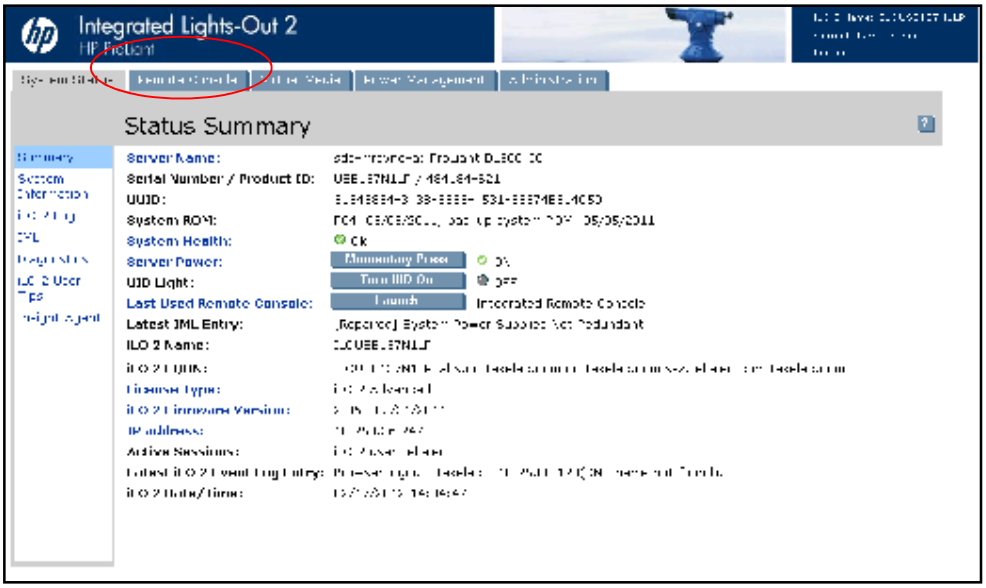
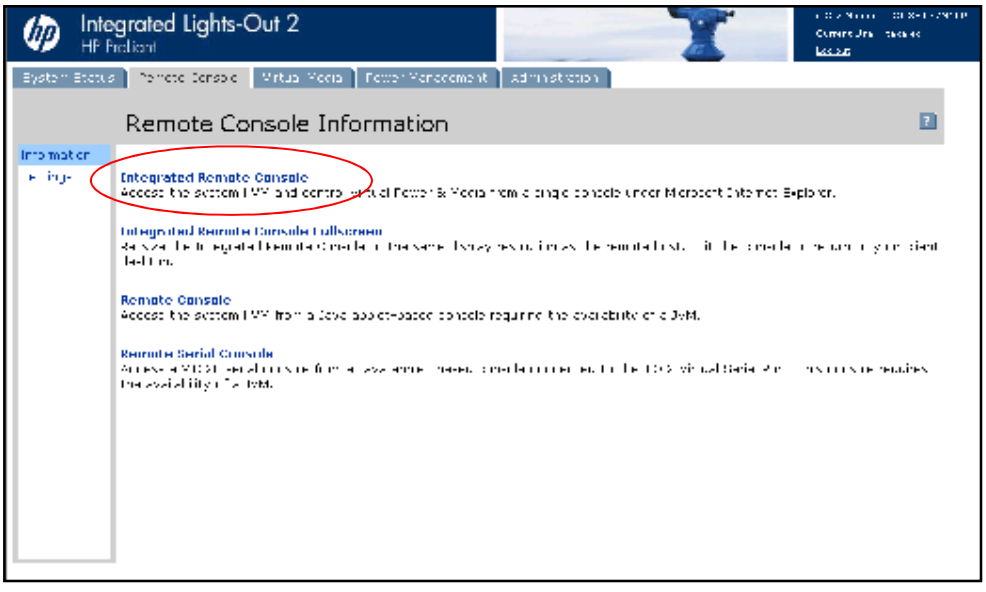
Step	Procedure	Result
20. ☐	**Repeat steps 16-18 (Optional 19) for each MP.** **"Check off"** the associated **Check Box** for each MP as it is completed. **Primary Site:** ☐ MP-1 ☐ MP-2 ☐ MP-3 ☐ MP-4 ☐ MP-5 **Disaster Recovery Site (Optional):** ☐ MP-1 ☐ MP-2 ☐ MP-3 ☐ MP-4 ☐ MP-5	
21. ☐	**Optional: Repeat procedure for Disaster Recovery MPs**	
22. ☐	**Active NOAM VIP:** Click the **"Logout"** link on the HLRR server GUI.	
THIS PROCEDURE HAS BEEN COMPLETED		

Appendix A. Accessing the iLO VGA Remote Console Window

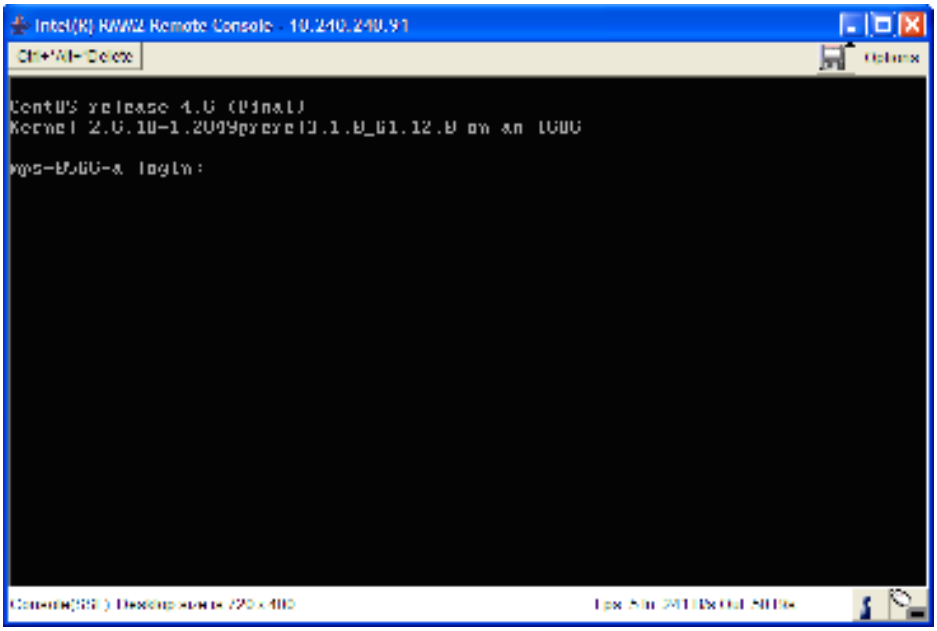
Appendix A: Accessing the iLO VGA Remote Console Window

Step	Procedure	Result
1. ☐	Launch an approved web browser and connect to the iLO interface **NOTE:** *Always use https:// for iLO GUI access.* *Use the default iLO IP address.*	
2. ☐	The web browser will display a warning message regarding the Security Certificate.	
3. ☐	Select the option to "Continue to the website (not recommended)	

Appendix A: Accessing the iLO VGA Remote Console Window

4. ☐	Login to the iLO console	
5. ☐	The iLO GUI is displayed. Select the "**Remote Console**" tab in the upper left corner of the GUI.	
6. ☐	The Remote Console Information GUI is displayed Click on the "**Integrated Remote Console**" option	

Appendix A: Accessing the iLO VGA Remote Console Window

7. ☐	The iLO Console window is displayed. **NOTE:** *The console window resembles an MS-DOS window but DOES NOT have a scroll-back buffer.*	
THIS PROCEDURE HAS BEEN COMPLETED		

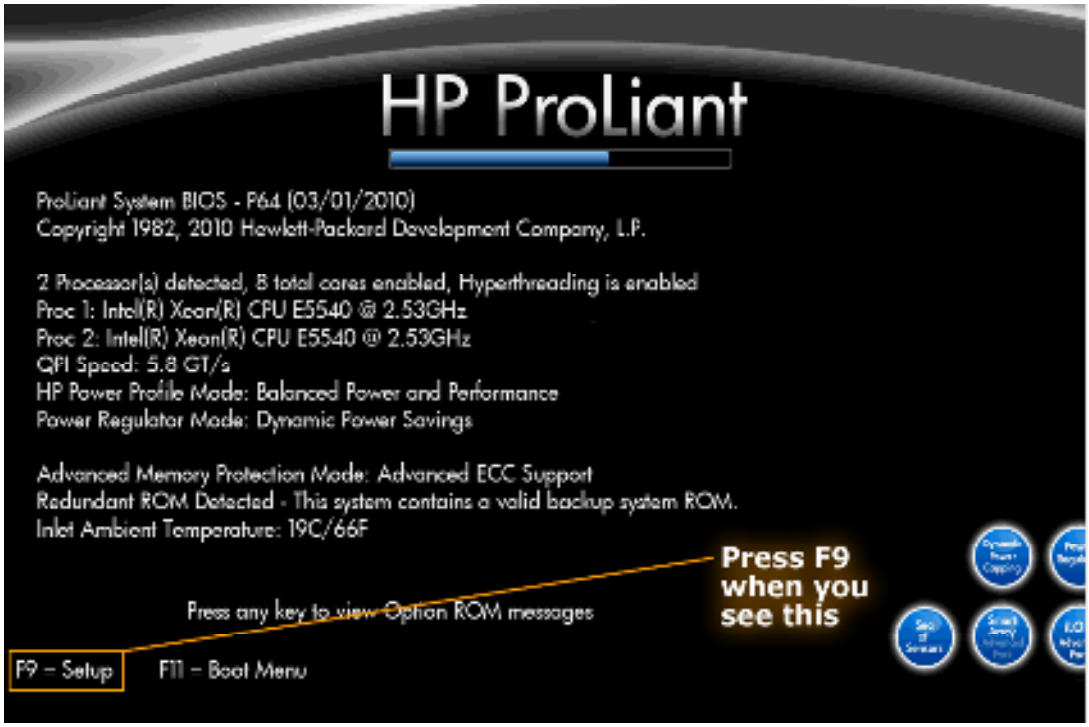
Appendix B. HP DL360 Configure CMOS Clock, BIOS Settings, and iLO IP Address

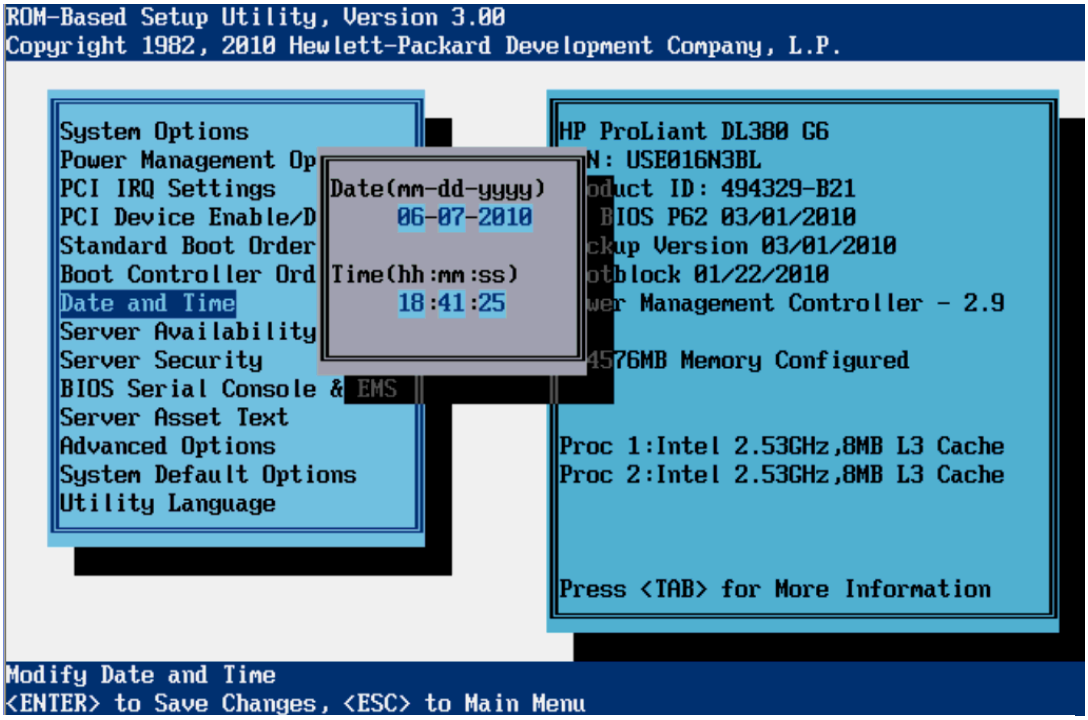
This procedure will configure the HP DL360 CMOS Clock, set the BIOS setting and configure the iLO IP Address.

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

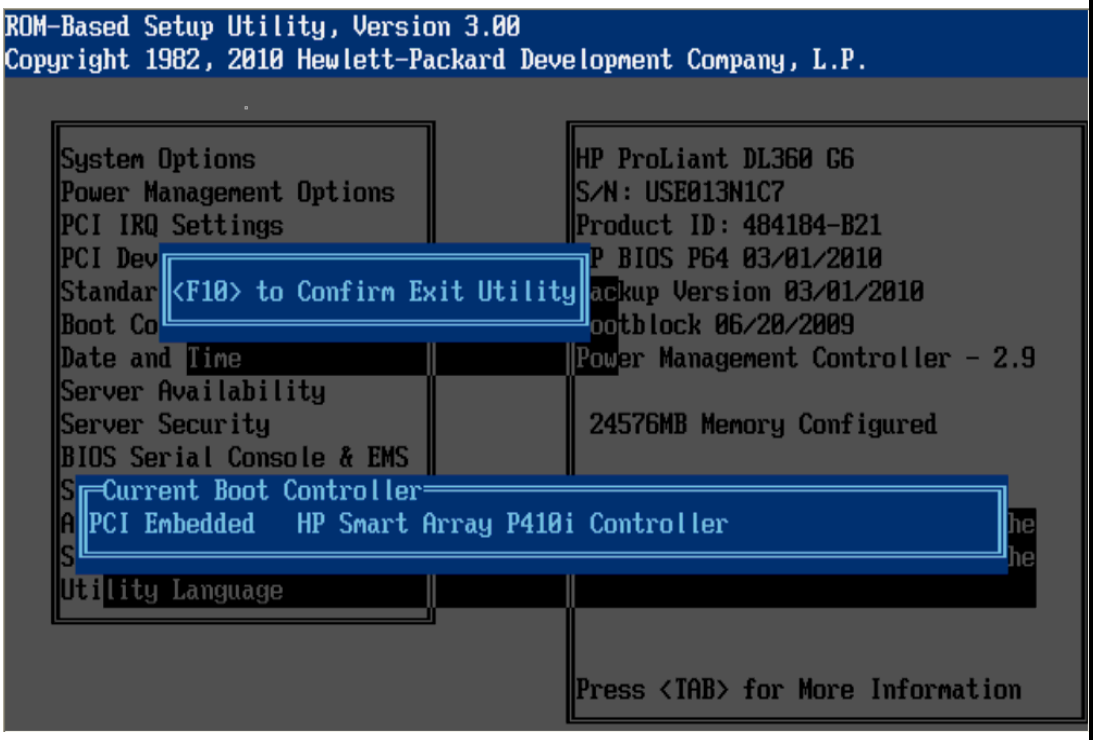
IF THIS PROCEDURE FAILS, CONTACT ORACLE CUSTOMER CARE CENTER AND ASK FOR ASSISTANCE.

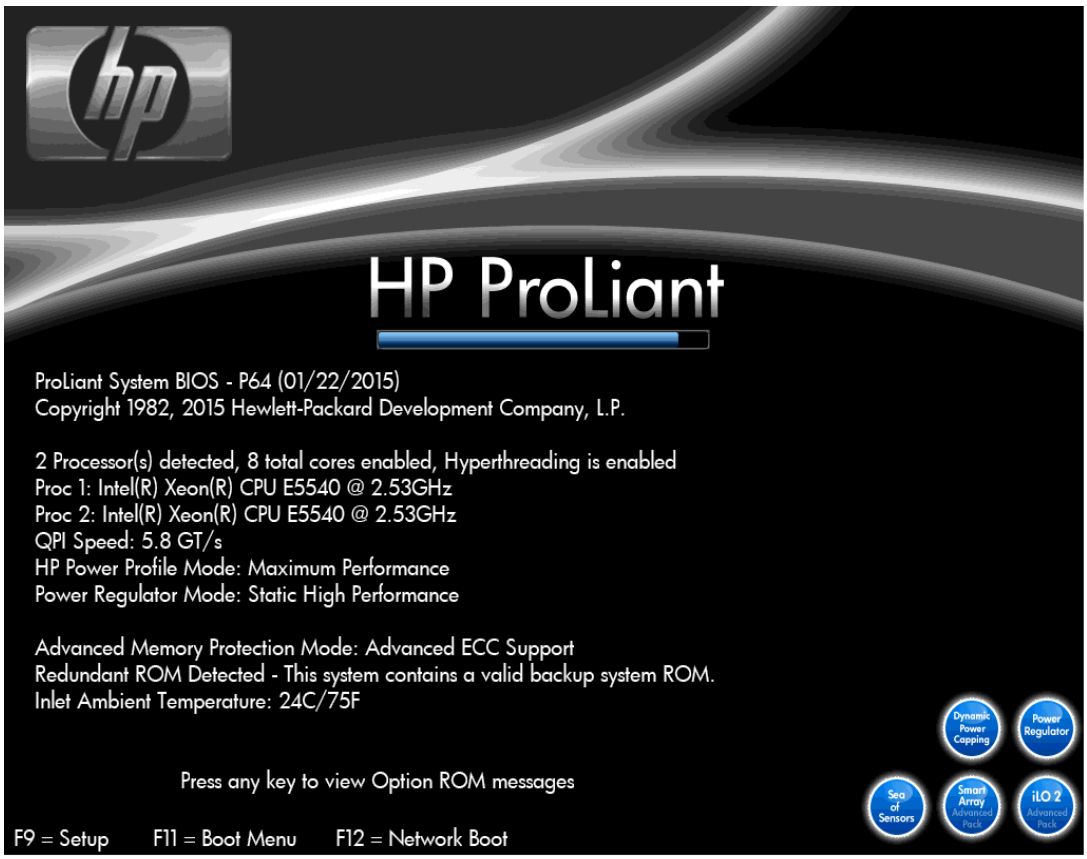
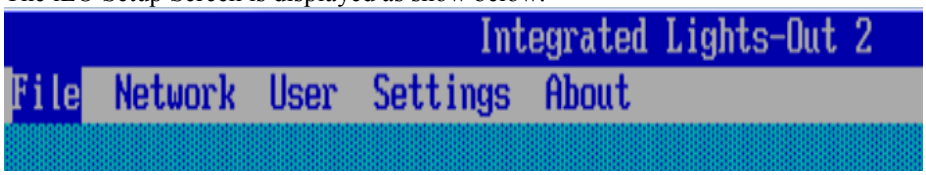
Appendix B: HP DL360 Configure CMOS Clock, BIOS Settings, and iLO IP Address

Step	In this procedure you will configure BIOS settings for a DL360 and set the iLO IP address.	
1. ☐	Access the HP DL360 server's console.	Connect to the HP DL360 server's console using one of the access methods described in **Section 2.3.**
2. ☐	Access the Server BIOS	Reboot the server. This can be achieved by pressing and holding the power button until the server turns off, then after approximately 5-10 seconds press the power button to enable power. As soon as you see **F9=Setup** in the lower left corner of the screen, press **[F9]** to access the BIOS setup screen. You may be required to press [F9] 2-3 times. The F9=Setup will change to F9 Pressed once it is accepted. See example below.  **Expected Result:** ROM-Based Setup Utility is accessed and the ROM-Based Setup Utility menu will be displayed.

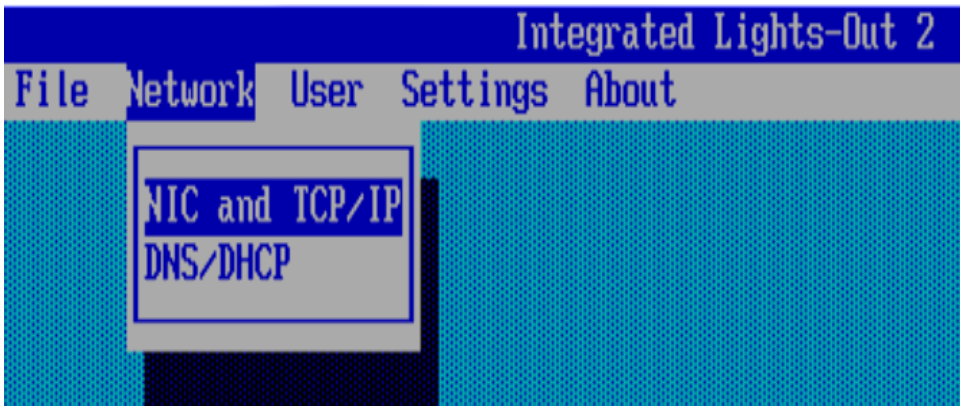
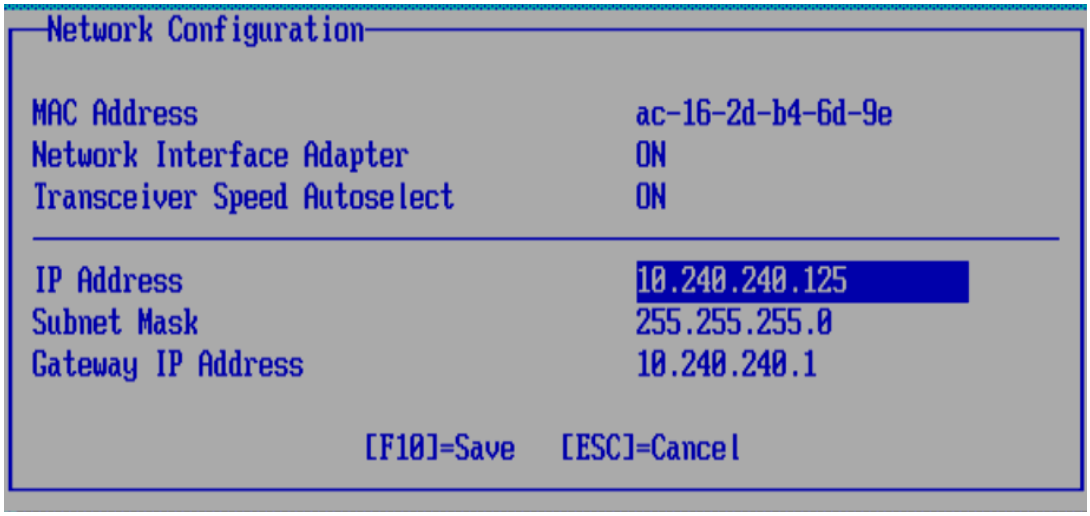
3. ☐	Set DL360 Server CMOS Clock	Scroll to *Date and Time* and press **[ENTER]** Set the date and time and press **[ENTER]**.  **Expected Result:** Correct Time & Date is set.
4. ☐	Configure iLO serial port settings	The serial ports on HP DL360 G6 rack mount servers need to be configured so the serial port used by the BIOS and TPD are connected to the "VSP" on the iLO. This will allow the remote administration of the servers without the need for external terminal servers. If this configuration has not been completed correctly and the server rebooted, the syscheck "syscheck -v hardware serial" test will fail. Select **System Options** option and press **[ENTER]**. Select **Serial Port Options** option and press **[ENTER]**. Change **Embedded Serial Port** to **COM2** and press **[ENTER]**. Change **Virtual Serial Port** to **COM1** and press **[ENTER]**. Press <ESC> two times

Appendix B: HP DL360 Configure CMOS Clock, BIOS Settings, and iLO IP Address

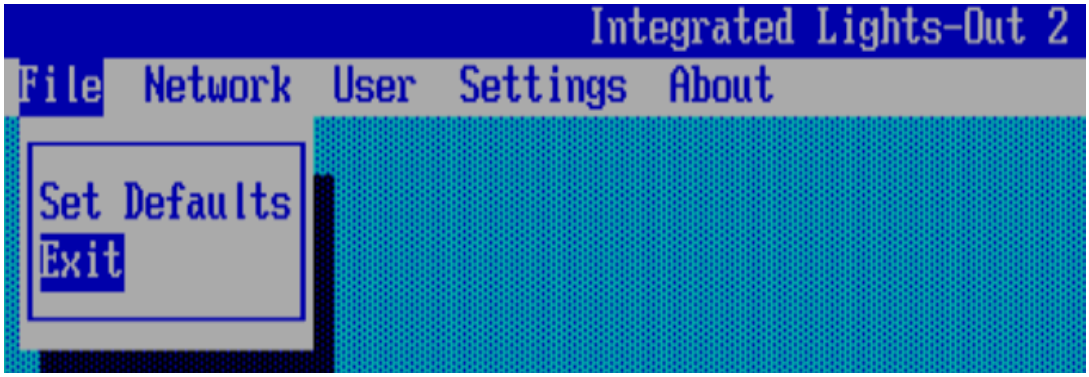
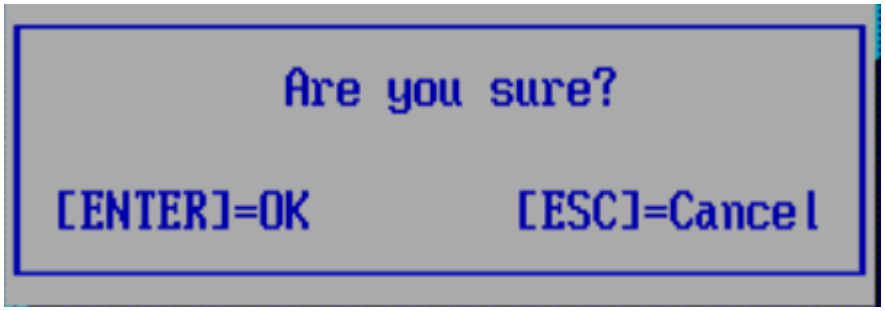
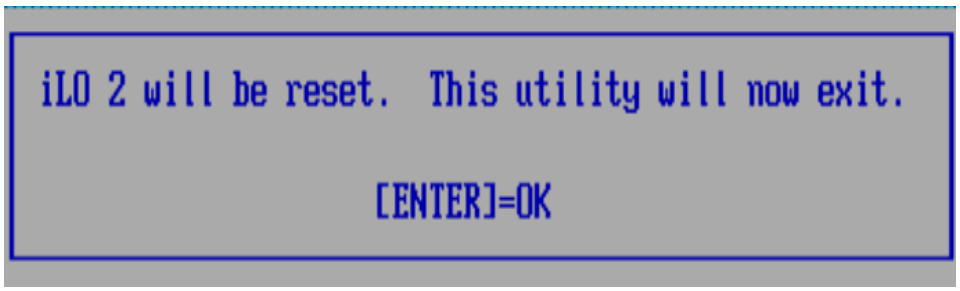
5. ☐	Configure Power Management Options settings	The Power Management Options on HP DL360 G6 rack mount servers need to be configured for optimum software performance. Select **Power Management Options** option and press **[ENTER]**. Select **HP Power Profile** option and press **[ENTER]**. Change it to **Maximum Performance** and press **[ENTER]**. Press <ESC> two times
6. ☐	Save Configuration and Exit	Press **[F10]** to save the configuration and exit. The server will reboot  **Expected Result:** Settings are saved and server reboots.

7. ☐	Access the iLO Setup Screen.	The RMS Server will reboot and after a few minutes the HP Prolaint Graphic will be displayed. As soon as you see the **F12=Network Boot** option appears in the lower center of the screen, press **[F8]** to access the iLO setup screen. You may be required to press [F8] 2-3 times. See example below. 
8. ☐	iLO Setup Screen	The iLO Setup Screen is displayed as show below: 

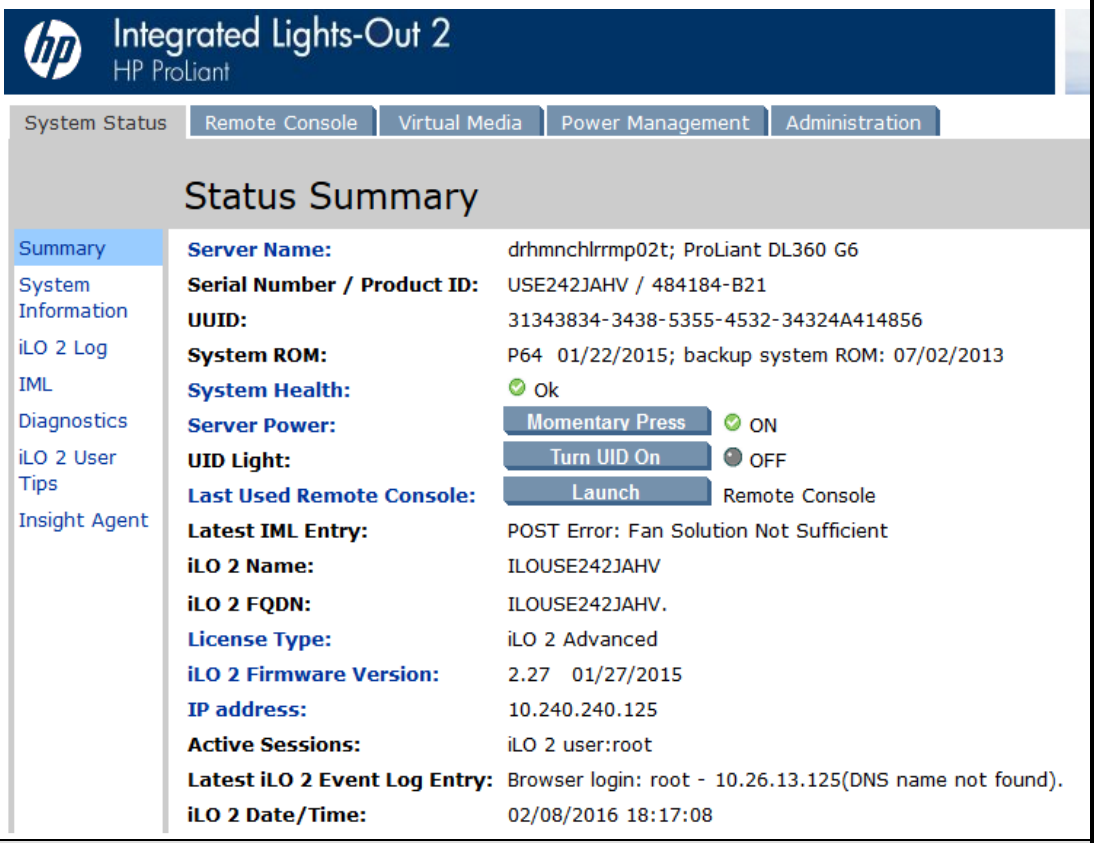
Appendix B: HP DL360 Configure CMOS Clock, BIOS Settings, and iLO IP Address

9. ☐	Set the iLO IP address	Select the **Network** pulldown and highlight **NIC and TCP/IP** and press the **<enter>** key**:** 
10. ☐	Set the iLO IP address	The iLO IP configure screen is displayed. Make the following settings by highlighing them: Network Interface Adapter: **ON** Transceiver Speed Autoselect: **ON** IP Address: **IP Address from NAPD Documentation** Subnet Mask: **IP Address from NAPD Documentation** Gateway Address: **IP Address from NAPD Documentation** Select the **<F10>** key to **Save** the settings. 

Appendix B: HP DL360 Configure CMOS Clock, BIOS Settings, and iLO IP Address

11. ☐	iLO Setup Screen	Exit the iLO Setup Screen by selecting **File** and hightlighting **Exit,** then pressing **<enter>** on the keyboard. 
12. ☐	iLO Setup Screen	Select **<enter>** on the keyboard to exit the iLO Setup Screen. 
13. ☐	iLO Setup Screen	Select **<enter>** on the keyboard to exit the iLO Setup Screen and reset the iLO interface. 
14. ☐	Server Command Interface	The iLO connection will be closed and the server will reboot.

Appendix B: HP DL360 Configure CMOS Clock, BIOS Settings, and iLO IP Address

15. ☐	iLO GUI Interface	Login into the iLO GUI using Internet Explorer with the ip address entered in step 10. 
16. ☐	iLO GUI Interface	iLO GUI Interface is displayed: 
THIS PROCEDURE HAS BEEN COMPLETED		

Appendix C. Creating Temporary External IP Address for Accessing HLRR GUI

This procedure creates a temporary external IP address that will be used for accessing the HLRR GUI prior to configuring the first HLRR server. This procedure assumes that the user has access to the ILO and can access an external (XMI) network at the customer site.

Appendix C: Creating Temporary External IP Address for Accessing HLRR GUI

Step	In this procedure you will configure a temporary external IP Address for NOAM Server A for the 1st NOAM site. The user will use this IP Address in a web browser to access the GUI to configure the first HLRR server.	
1. ☐	**PMAC Server:** Connect to the PMAC Server Console.	Connect to the PMAC server's console using one of the access methods described in **Section 2.3.** Use the PMAC_Management_ip_address that was entered in **Procedure 4 Deploying PMAC, Step 3.**
2. ☐	**PMAC Server:** **1)** Access the command prompt. **2)** Log into the PMAC server as the "**admusr**" user..	login as: admusr admusr@10.250.xx.yy's password: **<admusr_password>** Last login: Mon Jul 30 10:33:19 2012 from 10.25.80.199 [admusr@pmac-pc9040833 ~]$
3. ☐	**PMAC Server:** SSH into the NOAM-A server using the Control IP Address	Using an SSH client such as putty, ssh to the NOAM-A server using admusr credentials and the <NOAM-A Control IP Address> from **Procedure 11:** Configure TVOE Host's Network on all Rack Mount Servers. [admusr@pmac-pc9040833 ~]$ ssh 192.168.1.xx admusr@192.168.1.20's password: **<admusr_password>**
4. ☐	**NOAM Server A:** Output similar to that shown on the right will appear as the server access the command prompt.	***** TRUNCATED OUTPUT ***** VPATH=/opt/TKLCcomcol/runcm5.16:/opt/TKLCcomcol/cm5.16 PRODPATH= RELEASE=5.16 RUNID=00 VPATH=/var/TKLC/rundb:/usr/TKLC/appworks:/usr/TKLC/awpcommon:/usr/TKLC/awptransportmgr:/usr/TKLC/awpss7:/usr/TKLC/exhr PRODPATH=/opt/comcol/prod RUNID=00 [admusr@pc9040833-no-a ~]$

Appendix C: Creating Temporary External IP Address for Accessing HLRR GUI

5. ☐	**NOAM Server A:** Set XMI interface IP address from the NAPD documentation to temporarily access the HLRR GUI.	Verify the management network by running the following command **Note:** The output below is for illustrative purposes only. The example output below shows the management bridge configured. $ **sudo /usr/TKLC/plat/bin/netAdm query --device=xmi** Protocol: none On Boot: yes IP Address: 10.250.51.80 Netmask: 255.255.255.0 $ If the xmi IP address and netmask have 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. Set xmi IP address $ **sudo /usr/TKLC/plat/bin/netAdm add --device=xmi** **--address=<XMI_IP_Address_for_NO_A>** **--netmask=<XMI_netmask> --onboot=yes --bootproto=none** Interface xmi updated
6. ☐	**NOAM Server A:** Add a route to the temporary XMI interface	Note: The output below is for illustrative purposes only. The example output below shows the control bridge configured. $ **sudo /usr/TKLC/plat/bin/netAdm query -route=default --device=xmi** Routes for TABLE: main and DEVICE: xmi * NETWORK: default GATEWAY: 10.250.51.1 $ 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. $ **sudo /usr/TKLC/plat/bin/netAdm add --route=default** **--gateway=<XMI_gateway> --device=xmi** Route to xmi added
7. ☐	**NOAM Server A:** Restart the network on the server	Restart the server by running the following: $ **service network restart**

Appendix C: Creating Temporary External IP Address for Accessing HLRR GUI

8. ☐	**NOAM Server A:** Wait a few minutes and then ping the default gateway to ensure connectivity.	$ **ping <XMI_IP_Address_for_default_gateway>** $
9. ☐	**NOAM Server A:** Log off the NOAM-A Server	[admusr@hostname1260476221 ~]$ **exit** Connection to 192.168.1.20 closed. [admusr@hostname1260476221 ~]
10. ☐	**PMAC Server:** Log off the PMAC Server	[admusr@hostname1260476221 ~]$ **exit**
11. ☐	**The user can now launch an approved web browser and connect to https://<XMI_IP_Address_for_NO_A> to access the HLRR NOAM-A GUI using the temporary IP address.**	
THIS PROCEDURE HAS BEEN COMPLETED		

Appendix D. Creating an XML file for Installing HLRR Network Elements

HLRR Network Elements can be created by using an XML configuration file. The HLRR software image (*.iso) contains two examples of XML configuration files for "NO" (Network OAM&P) and "SO" (System OAM) networks. These files are named **HLRR_NOAM_NE.xml** and **HLRR_SOAM_NE.xml** and are stored on the **/usr/TKLC/exhr/xml** directory. The customer is required to create individual XML files for each of their HLRR Network Elements. The format for each of these XML files is identical. Below is an example of the HLRR_NOAM_NE.xml file. The highlighted values are values that the user must update.

NOTE: *The **Description** column in this example includes comments for this document only. **Do not include** the Description column in the actual XML file used during installation.*

Table 4 - HLRR 4.1 XML NOAM Network Element Configuration File

XML File Text	Description
<networkelement>	
<name>**NOAM_NE**</name>	Unique identifier used to label a Network Element. [Range = 1-32 character string. Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit.]
<ntpservers>	
<ntpserver>**10.250.32.10**</ntpserver>	IP Address of the first NTP server. There must be at least one NTP server IP address defined.
<ntpserver>**10.250.32.51**</ntpserver>	IP Address of second NTP server, if it exists; otherwise, this line must be deleted.
</ntpservers>	
<networks>	
<network>	
<name>XMI</name>	Name of customer external network. **Note**: Do NOT change this name.
<vlanId>**3**</vlanId>	The VLAN ID to use for this VLAN. [Range = 2-4094.]
<ip>**10.250.39.16**</ip>	The network address of this VLAN [Range = A valid IP address]
<mask>**255.255.255.240**</mask>	Subnetting to apply to servers within this VLAN
<gateway>**10.250.39.17**</gateway>	The gateway router interface address associated with this network [Range = A valid IP address]
<isDefault>true</isDefault>	Indicates whether this is the network with a default gateway. [Range = true/false]
</network>	
<network>	
<name>IMI</name>	Name of customer internal network. **Note**: Do NOT change this name.
<vlanId>**4**</vlanId>	The VLAN ID to use for this VLAN. [Range = 2-4094.]
<ip>**169.254.2.0**</ip>	The network address of this VLAN [Range = A valid IP address]
<mask>**255.255.255.0**</mask>	Subnetting to apply to servers within this VLAN
<gateway>**169.254.2.1**</gateway>	The gateway router interface address associated with this network [Range = A valid IP address]
<isDefault>false</isDefault>	Indicates whether this is the network with a default gateway. [Range = true/false]
</network>	
</networks>	
</networkelement>	

Appendix E. 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 5 - List of Selected Time Zone Values

Time Zone Value	Description	Universal Time Code (UTC) Offset
Etc/UTC	GMT	0
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 F. Attaching an ISO Image to a Server using the iLO

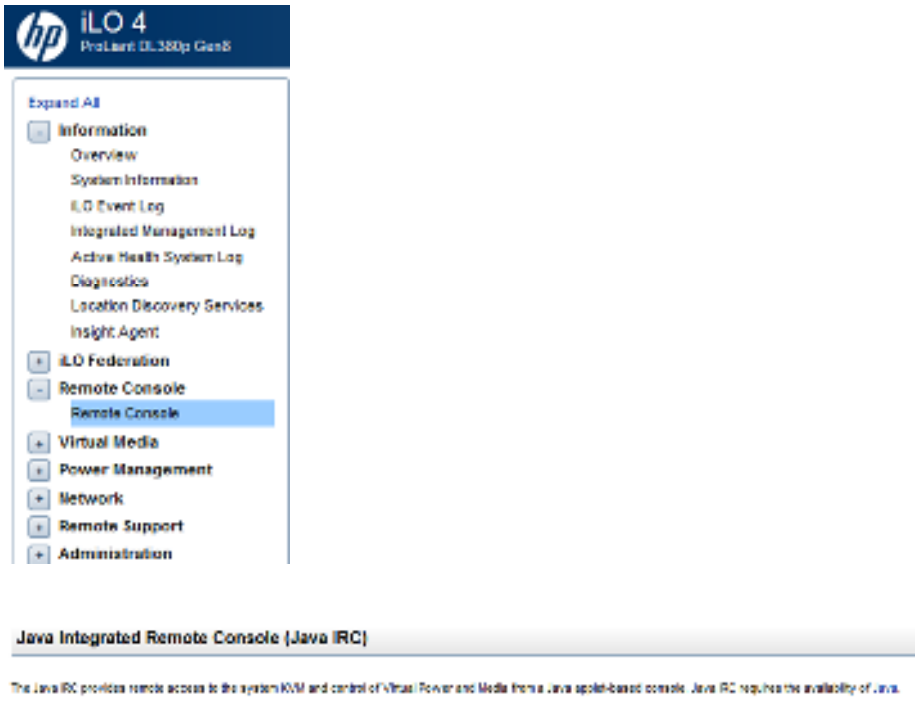
As an alternative to mounting the ISO image via USB, the user may also mount the ISO via the iLO for HP rack mount servers.

Appendix F HP DL380 Servers Mounting the ISO image via iLO4

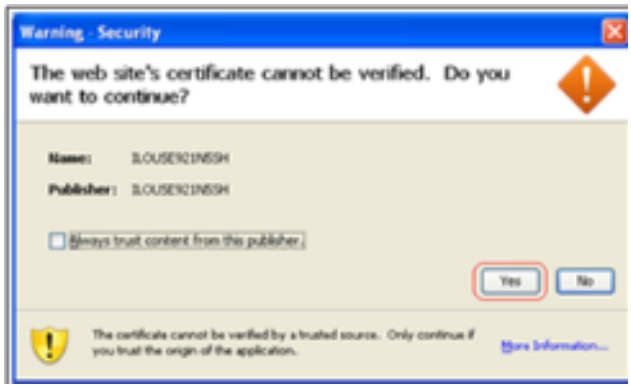
This procedure describes the steps needed to attach an ISO image to a server using the iLO4 for HP DL 380 servers.

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

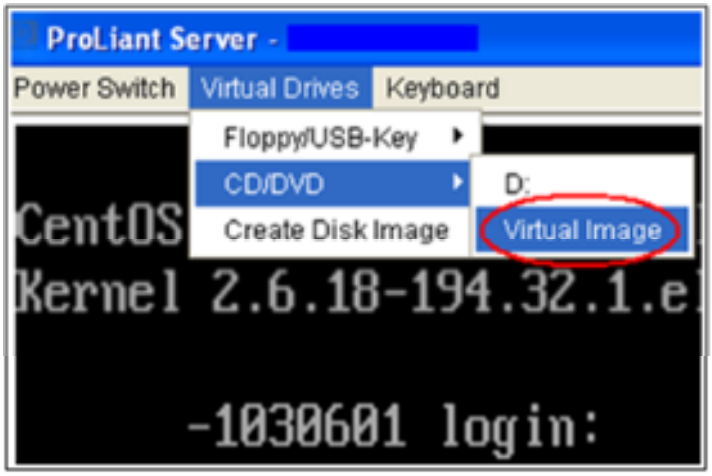
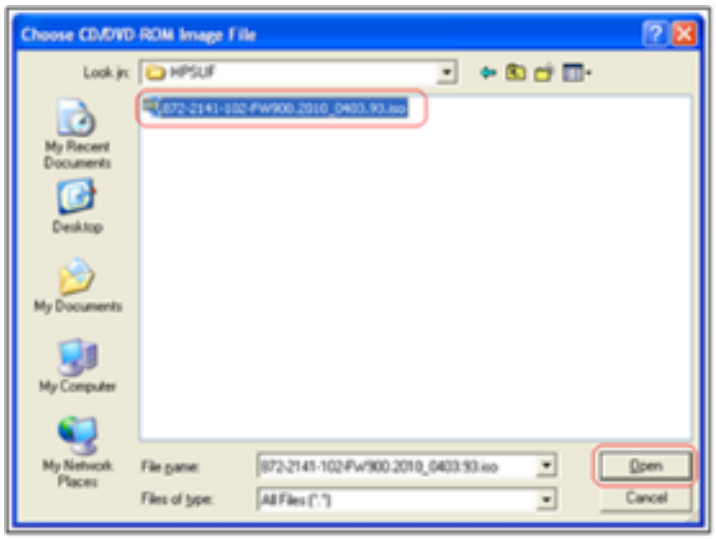
If this procedure fails, contact My Oracle Support (MOS). Refer to **Appendix L -** MY ORACLE SUPPORT (MOS) for further assistance.

STEP #	Procedure	Result
1 ☐	**iLO 4 Web GUI:** Launch Remote Console	Launch the Java Integrated Remote Console applet. On the menu to the left navigate to the **Remote Console** page. Under Java Integrated Remote Console (Java IRC), click **Launch** 

Appendix F HP DL380 Servers Mounting the ISO image via iLO4

2 ☐	**iLO 4 Web GUI:** Java Security Prompt	Acknowledge Security Warning. If a dialog similar to the one below is presented, click **Yes** to acknowledge the issue and proceed 

Appendix F HP DL380 Servers Mounting the ISO image via iLO4

3 ☐		Click on the **Virtual Drives** drop down menu. Go to **CD/DVD**, then click on **Virtual Image**  Navigate to the location of the ISO image file specified by the procedure which referenced this appendix.  Select the desired file and click **Open**.

Appendix F HP DL380 Servers Mounting the ISO image via iLO4

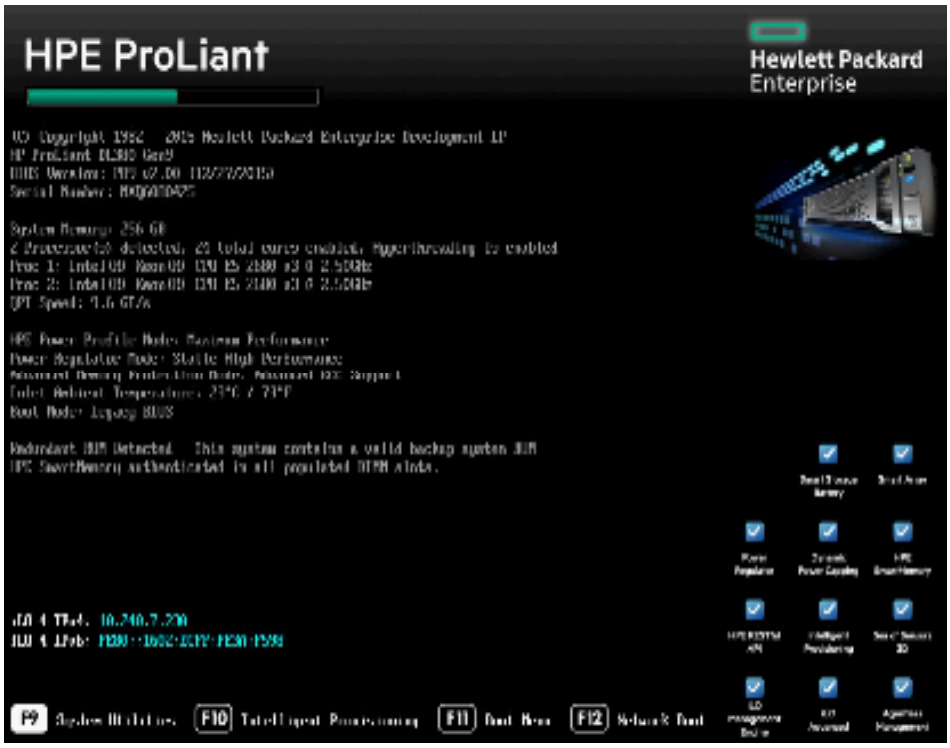
4 ☐		Verify Virtual Image Connection. At the bottom of the remote console window, there should now be a green highlighted drive icon and **Virtual M** written next to it. 

Appendix G. Configure the HP DL380 Server CMOS Clock/BIOS Settings

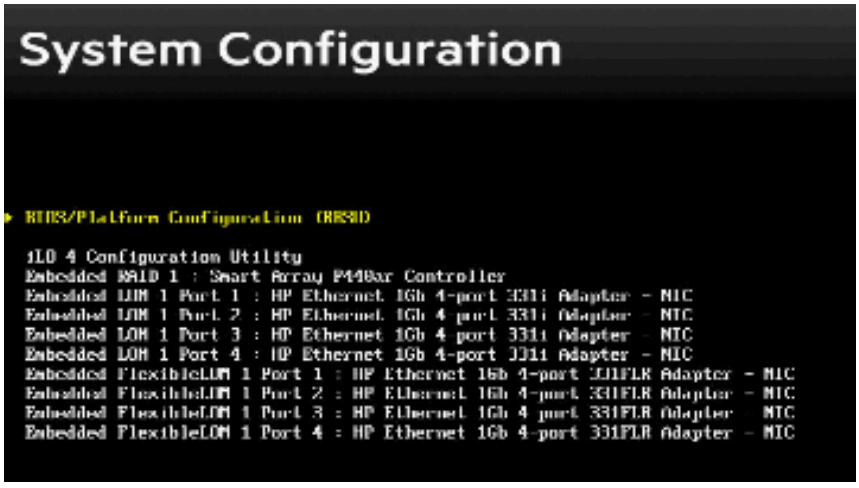
Follow these steps to configure HP DL 380 (Gen9) server CMOS Clock and BIOS settings.

The HP Gen 9 systems can have UEFI boot enabled. Since TPD is configured to use the Legacy BIOS option, rack mount Gen9s should have their BIOS settings checked before IPM. Rack mount servers should also have the iLO serial port configured at this time. Directions for both settings are provided below.

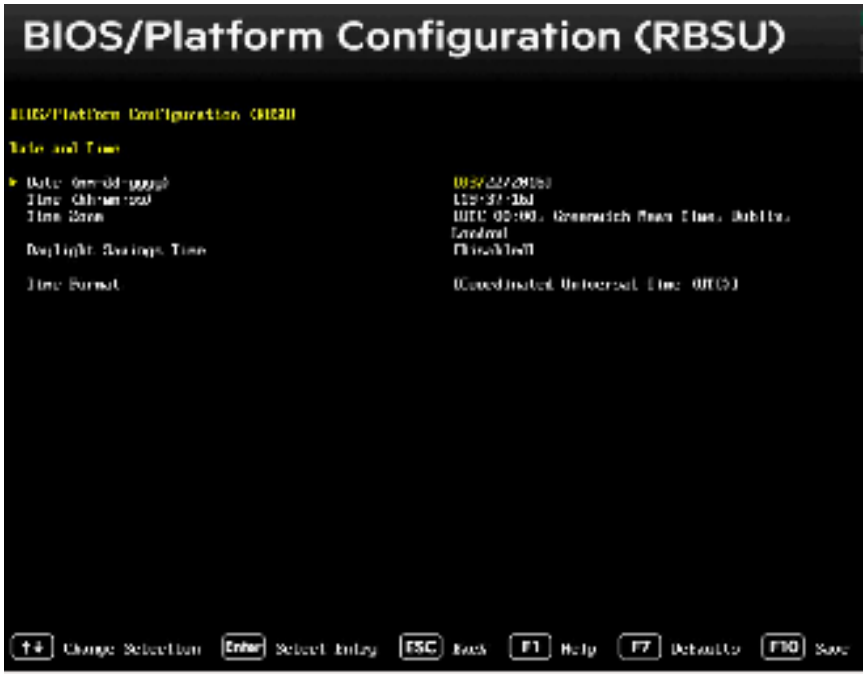
Appendix G Configure HP DL380 Server CMOS Clock/BIOS Settings

S T E P S	This procedure explains the steps needed to configure the HP DL380 (Gen 9) server BIOS settings. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS), and ask for assistance.	
1 ☐	**HP Gen9 Server:** Connect VGA Monitor and USB Keyboard	Connect via a VGA monitor and USB keyboard to the back of the server.
2 ☐	**HP Gen9 Server:** Reboot	Reboot the server. After the server is powered on, press the **F9** key when prompted to access the **System Utilities Screen:** 

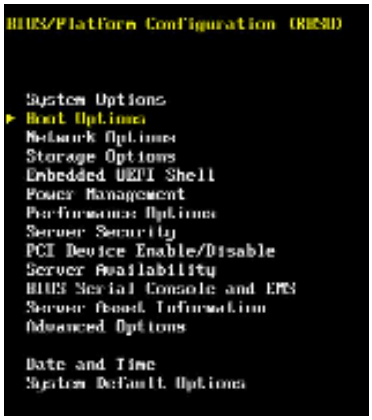
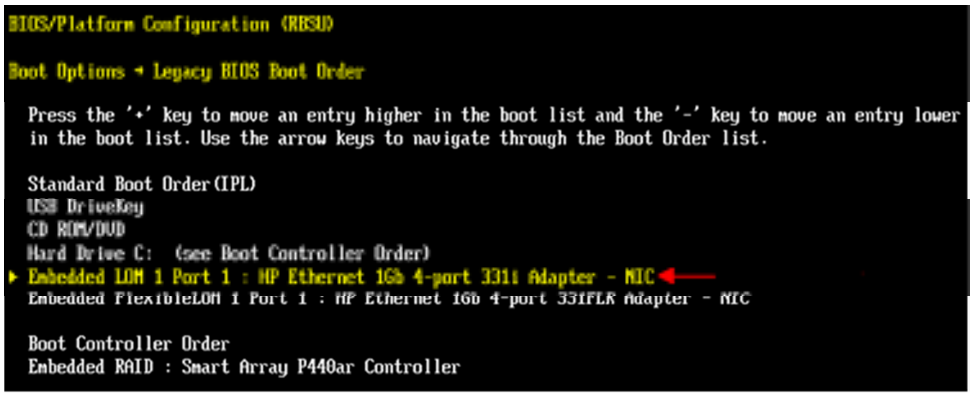
Appendix G Configure HP DL380 Server CMOS Clock/BIOS Settings

3 ☐	**HP Gen9 Server:** System Utilities	User will be presented with the **System Utilities Screen,** hightlight *System Configuration* and press the <Enter> key to select. 
4 ☐	**HP Gen9 Server:** System Configuration	User will be presented with the **System Configuration Screen,** hightlight *BIOS/Platform Configuration (RBSU)* and press the <Enter> key to select. 

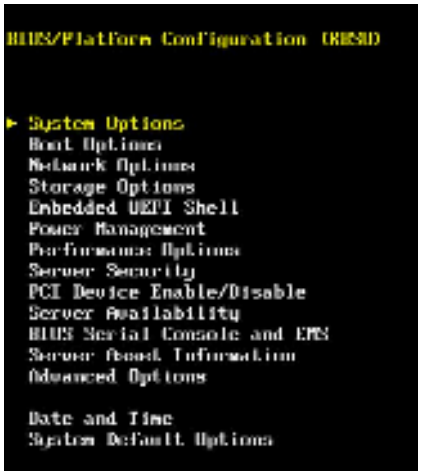
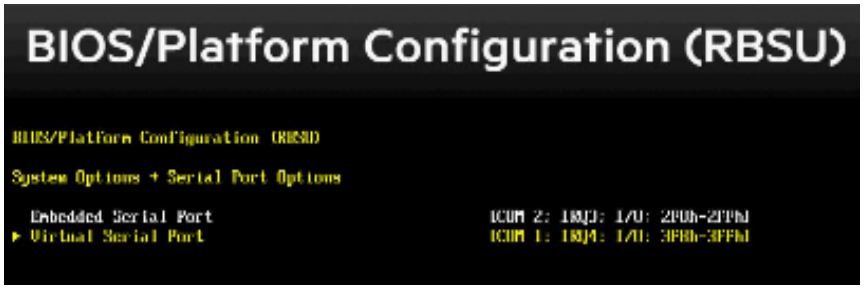
Appendix G Configure HP DL380 Server CMOS Clock/BIOS Settings

5 ☐	**HP Gen9 Server:** Select Date and Time	User will be presented with the **Bios/Platform Configuration Screen,** hightlight *Date and Time* option and press the <Enter> key to select. 
6 ☐	**HP Gen9 Server:** Enter Date, Time and Time Zone	User will be presented with the **Date and Time Screen,** set the *Date and Time to UTC (Greenwich Mean Time), the Time Zone to UTC, and the Time Format to Coordinated Universal Tim (UTC)* then select <F10> key to save your changes. After saving select the <ESC> key to return to the **Bios/Platform Configuration Screen.** 

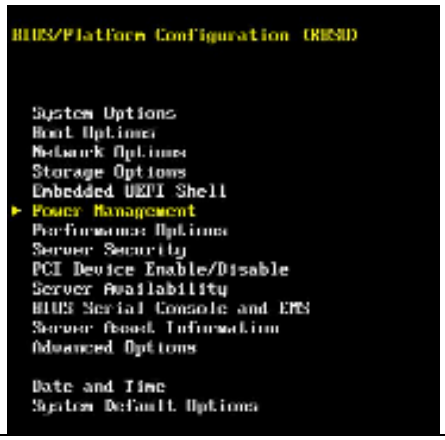
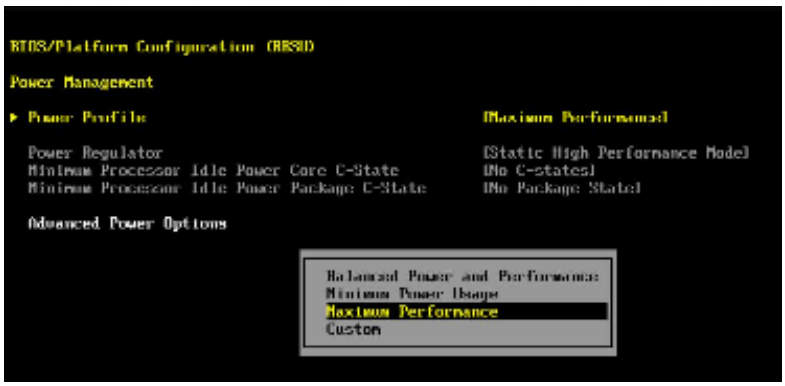
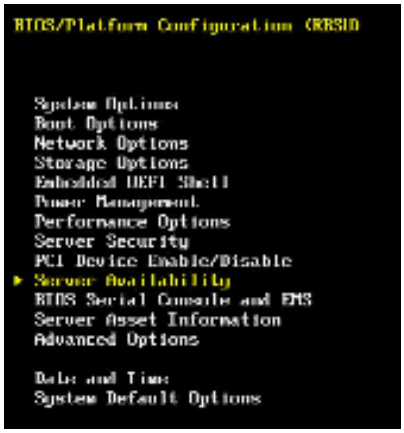
Appendix G Configure HP DL380 Server CMOS Clock/BIOS Settings

7 ☐	**HP Gen9 Server:** Select Boot Options	User will be presented with the **Bios/Platform Configuration Screen,** hightlight *Boot Options* and press the <Enter> key to select. 
8 ☐	**HP Gen9 Server:** Enter Boot Options	User will be presented with the **Boot Options Screen,** set the *Boot Mode to Legacy BIOS Mode*, *UEFI Optimized Boot to Disabled*, and *Boot Order Policy to Retry Boot Order Indefinitely*. Then select <F10> key to save your changes. Select the *Legacy BIOS Boot Order Option* and press the <Enter> key to select. 
9 ☐	**HP Gen9 Server:** Set Boot Order	The user will be presented with the **Legacy BIOS Boot Order Option Screen.** Ensure that, *USB DriveKey, CD ROM/DVD, Hard Dive C, Embedded LOM 1 Port 1, and Embedded FlexibleLOM 1 Port 1:* are set in that boot order, if not change them then select <F10> key to save your changes. After saving select the <ESC> key to return to the **Boot Options Screen.** 

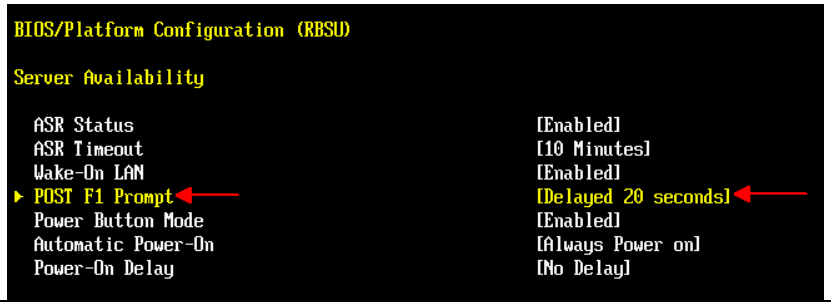
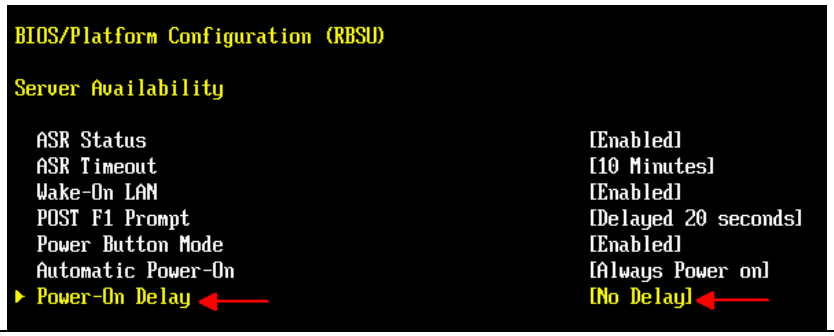
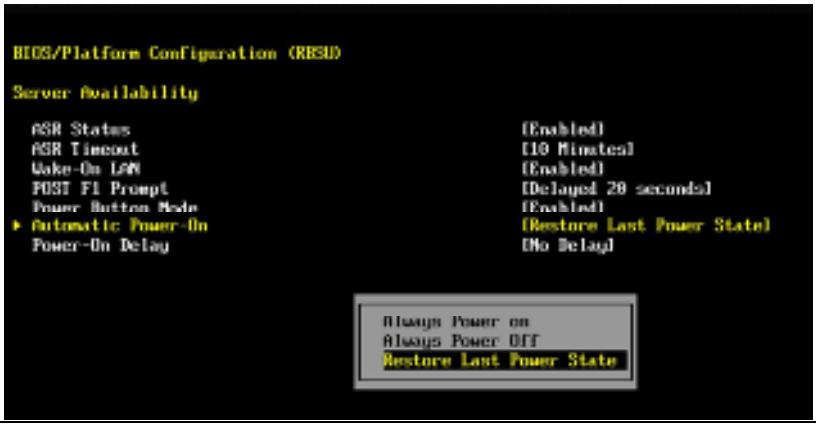
Appendix G Configure HP DL380 Server CMOS Clock/BIOS Settings

10 ☐	**HP Gen9 Server:** Select System Options	Select the <ESC> key again to return to the **Bios/Platform Configuration Screen,** highlight *System Options* and press the <Enter> key to select. 
11 ☐	**HP Gen9 Server:** Select Serial Port Options	The **System Options Screen** will be displayed, hightlight *Serial Port Options* and press the <Enter> key to select. 
12 ☐	**HP Gen9 Server:** Enter Serial Port Options	The **Serial Port Options Screen** will be displayed. Set the *Virtual Serial Port to COM1* and the *Embedded Serial Port to COM2* then select <F10> key to save your changes. After saving select the <ESC> key twice to return to the **Bios/Platform Configuration Screen.** 

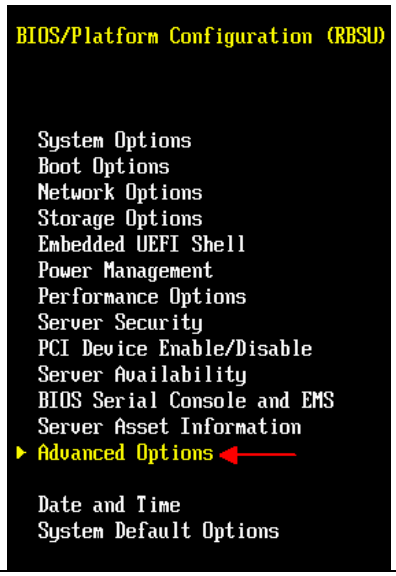
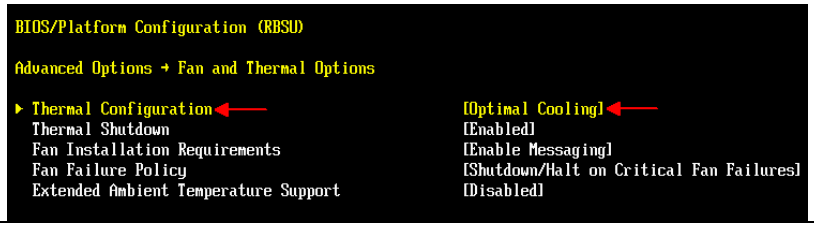
Appendix G Configure HP DL380 Server CMOS Clock/BIOS Settings

13 ☐	**HP Gen9 Server:** Select Power Management	From the **Bios/Platform Configuration Screen,** highlight *Power Management Option* and press the <Enter> key to select. 
14 ☐	**HP Gen9 Server:** Set Power Management to Max Performance	The **Power Management Screen** is displayed, select the *Power Profile of Maximum Performance* then select <F10> key to save your changes. After saving select the <ESC> key to return to the **Bios/Platform Configuration Screen.** 
15 ☐	**HP Gen9 Server:** Select Server Availability	From the **Bios/Platform Configuration Screen,** highlight *Server Availability Option* and press the <Enter> key to select. 

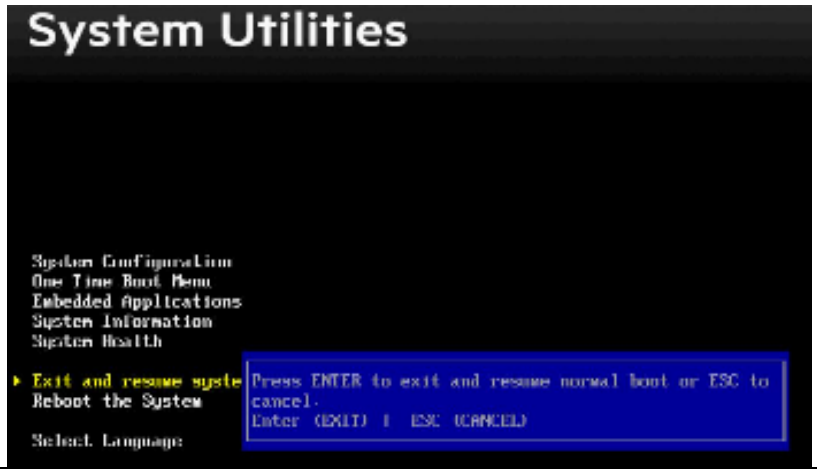
Appendix G Configure HP DL380 Server CMOS Clock/BIOS Settings

16 ☐	**HP Gen9 Server:** Set ASR Status	The **Server Availability Screen** is displayed, set *ASR Status to Enable.* 
17 ☐	**HP Gen9 Server:** Set POST F1 Prompt	Set *Delayed 20 seconds for POST F1 Prompt.* 
18 ☐	**HP Gen9 Server:** Set Power-On Delay	Set *No Delay for Power-On Delay.* 
19 ☐	**HP Gen9 Server:** Set Automatic Power On Options	Set *Restore Last Power State for Automatic Power-On* then press the <F10> key to save your changes. After saving select the <ESC> key to return to the **Bios/Platform Configuration Screen.** 

Appendix G Configure HP DL380 Server CMOS Clock/BIOS Settings

20 ☐	**HP Gen9 Server:** Select Advanced Options	From the **Bios/Platform Configuration Screen,** highlight *Advanced Options* and press the <Enter> key to select. 
21 ☐	**HP Gen9 Server:** Set Thermal Configuration	Set *Optimal Cooling for Thermal Configuration* then select <F10> key to save your changes. After saving select the <ESC> key to return to the **Bios/Platform Configuration Screen.** 
22 ☐	**HP Gen9 Server:** System Utilities	Select the <ESC> key to return to the **System Utilities Screen.** 

Appendix G Configure HP DL380 Server CMOS Clock/BIOS Settings

23 ☐	**HP Gen9 Server:** Exit and Boot server	From the **System Utilities Screen**, hightlight *Exit and resume system boot* and press the <Enter> key. The blue popup will be displayed, press <Enter> a second time to exit BIOS Setup and resume a normal boot. 

Appendix H. Setting the iLO/iLOM IP Address on DL380 Servers (iLO4)

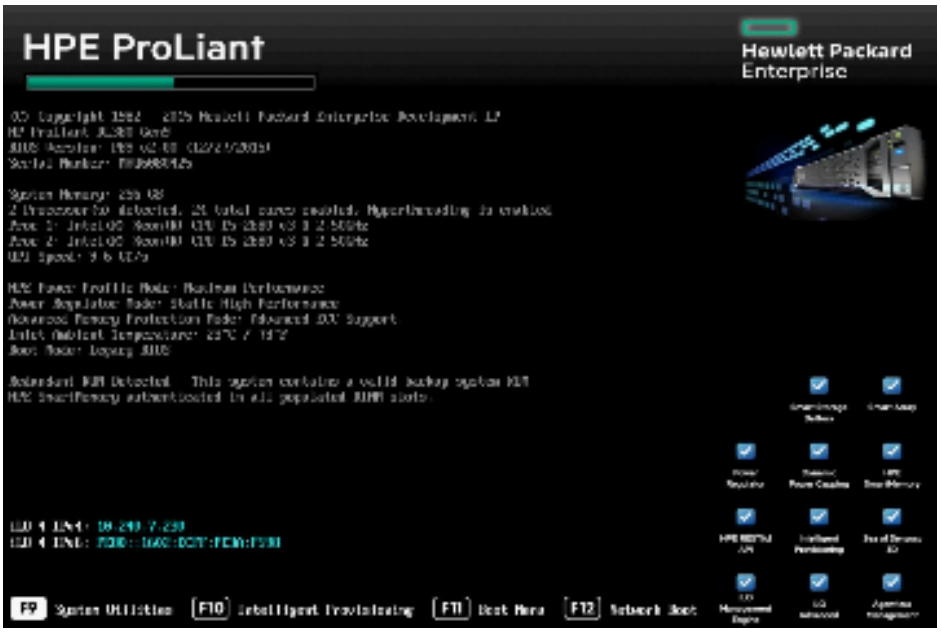
Follow these steps to set the HP DL 380 (Gen9) server iLO/iLOM IP Address.

Appendix H Setting the iLO/iLOM Address on DL380 Servers (iLO4)

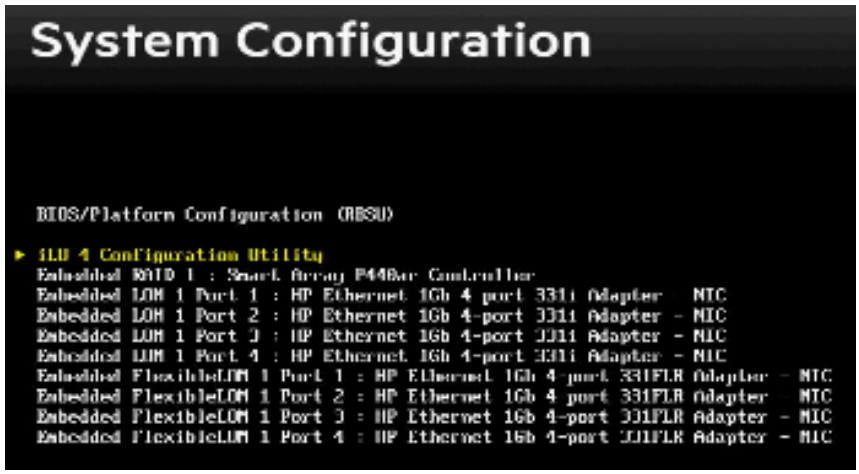
This procedure will set the IP address of the iLO on HP DL380 servers to the customer's network so that it can be accessed remotely.

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

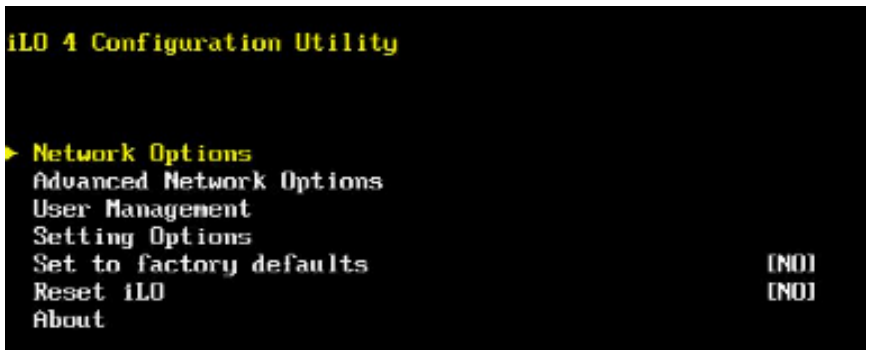
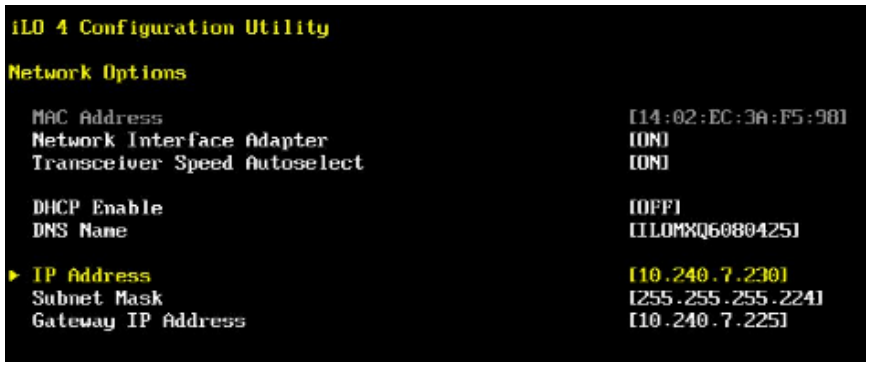
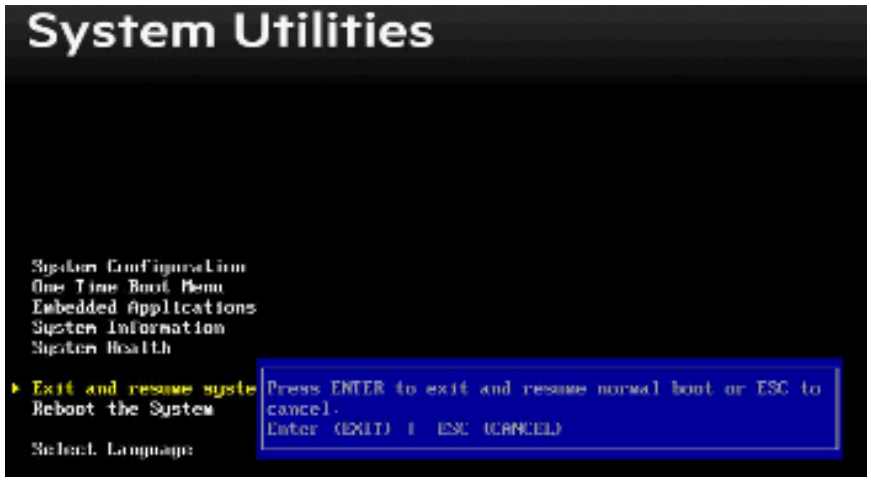
If this procedure fails, contact My Oracle Support (MOS), and ask for assistance.

STEP #	Procedure	Result
1 ☐	**HP Gen9 Server:** Access the System Utilities Screen	The RMS Server will reboot and after a few minutes the HPE Prolaint Graphic will be displayed. Press the **F9** key to access the **System Utilities Screen:** 

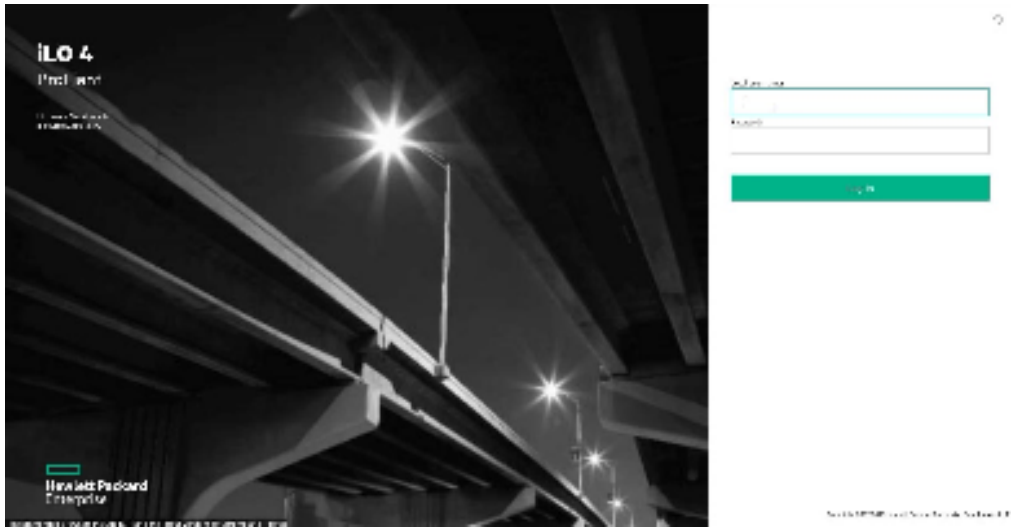
Appendix H Setting the iLO/iLOM Address on DL380 Servers (iLO4)

2 ☐	**HP Gen9 Server:** System Utilities	User will be presented with the **System Utilities Screen,** hightlight *System Configuration* and press the <Enter> key to select. 
3 ☐	**HP Gen9 Server:** Select iLO 4 Configuration Utility	User will be presented with the **System Configuration Screen,** hightlight *iLO 4 Configuration Utility* and press the <Enter> key to select. 

Appendix H Setting the iLO/iLOM Address on DL380 Servers (iLO4)

4 ☐	**HP Gen9 Server:** Select Network Options	User will be presented with the **iLO 4 Configuration Utility Screen,** hightlight *Network Options* and press the <Enter> key to select. 
5 ☐	**HP Gen9 Server:** Enter IP Address, Subnet Mask and Gateway IP Address	User will be presented with the **Network Options Screen,** set *DHCP Enable to OFF* then enter the *IP Address, Subnet Mask and Gateway IP Address* information provided by the cutomer from the NAPD documentation. Select the <F10> key to save your changes then select <Esc> three times to return to the **System Utilities Screen**. 
6 ☐	**HP Gen9 Server:** Exit System Utilities Screen and boot the server	From the **System Utilities Screen**, hightlight *Exit and resume system boot* and press the <Enter> key. The blue popup will be displayed, press <Enter> a second time to exit BIOS Setup and resume a normal boot. 

Appendix H Setting the iLO/iLOM Address on DL380 Servers (iLO4)

7 ☐	**HP Gen9 Server:** Login to the iLO GUI	After the server finishing booting, login into the iLO GUI using Internet Explorer with the IP Address entered in step 5 to verify operation of the new IP address. 
8 ☐	**HP Gen9 Server:** Verify that the iLO GUI is operational.	The iLO 4 GUI Interface is displayed: 
9 ☐	**HP Gen9 Server:** Exit iLO GUI	Select *Sign Out* in the upper right corner of the iLO GUI to exit. Setting of the iLO/iLOM IP address is now completed.

Appendix I. Creating a Bootable USB Drive on Linux

Appendix I Creating a Bootable USB Drive on Linux

S T E P S	This procedure will create a Bootable USB drive from a .usb file on a Linux Machine Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support and ask for assistance.	
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 the TVOE **.usb** file and copy it onto the local Linux machine (e.g. under /var/TKLC/upgrade)
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 **$ sudo dd if=<path_to_usb_image> of=/dev/sdb bs=4M oflag=direct** The boot building process will run for a period of time and return you to the command prompt. If no errors are displayed, then the process was successful.

Appendix J. Upgrade Cisco 4948 PROM

1. **Virtual PMAC/Management Server: Verify that the PROM image is on the PMAC.**
   If the appropriate image does not exist, copy the image to the server.

   Determine if the PROM image for the 4948E-F is on the system.

   $ **ls -al /var/TKLC/smac/image/**

   If the Prom firmware file exists, skip the remainder of this step and continue with the next step. If the file does not exist, copy the file from the Misc Firmware USB as specified by [6] HP Solutions Firmware Upgrade Pack Release Notes, Release 2.x.x (Min 2.2.9).

2. **Virtual PMAC/Management Server: Attach to switch console.**
   If upgrading the firmware on switch1A, connect serially to the switch by issuing the following command as admusr on the server:

   $ **sudo /usr/bin/console -M 192.168.1.4 -l platcfg switch1A_console**

   Enter platcfg@PMAC5000101's password: <platcfg_password>
   [Enter `^Ec?' for help]
   Press Enter
   If the switch is not already in enable mode ("switch#" prompt) then issue the "**enable**" command, otherwise continue with the next step.
   Switch> **enable**
   Switch#

   If upgrading the firmware on switch1B, connect serially to switch1B by issuing the following command as admusr on the PMAC server:
   $ **sudo /usr/bin/console -M 192.168.1.4 -l platcfg switch1B_console**

   Enter platcfg@PMAC5000101's password: <platcfg_password>
   [Enter `^Ec?' for help]
   Press Enter
   If the switch is not already in enable mode ("switch#" prompt), then issue the "**enable**" command, otherwise continue with the next step.
   Switch> **enable**
   Switch#

3. **Virtual PMAC/Management Server (switch console session): Configure port 40 on the 4948E-F switch.**
   To ensure connectivity, ping the management server's management vlan ip 192.168.1.1 address from the switch.

   If upgrading the firmware on **switch1A**, use these commands:
   Switch# **conf t**
   Switch(config)# **vlan 1**
   Switch(config-vlan)# **int vlan 1**
   Switch(config-if)# **ip address 192.168.1.2 255.255.255.0**
   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)# **end**
   Switch# **write memory**

   If upgrading the firmware on **switch1B**, use these commands:
   Switch# conf t
   Switch(config)# **vlan 1**

Switch(config-vlan)# **int vlan 1**
Switch(config-if)# **ip address 192.168.1.3 255.255.255.0**
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)# **end**
Switch# **write memory**

Switch# **ping 192.168.1.1**
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, 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, double check that the procedure was completed correctly by repeating all steps up to this point. If after repeating those steps, ping is still unsuccessful, contact My Oracle Support.

4. **Virtual PMAC/Management Server (Switch console session): Upgrade PROM**
   Switch# **copy tftp: bootflash:**
   Address or name of remote host []? **192.168.1.1**
   Source filename []? **<PROM_image_file>**
   Destination filename [<PROM_image_file>]? **[Enter]**
   Accessing tftp://192.168.1.1/<PROM_image_file>...
   Loading <PROM_image_file> from 192.168.1. (via Vlan1): !!!!!!!!!!!!!!!!!!! [OK– 45606 bytes]
   45606 bytes copied in 3.240 secs (140759 bytes/sec)
   Switch#

5. **Virtual PMAC/Management Server (Switch console session): Reload the switch**
   Switch# **reload**
   System configuration has been modified. Save? [yes/no]: **no**
   Proceed with reload? [confirm] **[Enter]**
   === Boot messages removed ===
   Type **[Control-C]** when ***Type control-C to prevent autobooting*** is displayed on the screen.

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

7. **Virtual PMAC/Management Server (Switch console session): Verify Upgrade**
   The switch will reboot when the firmware upgrade completes. Allow it to boot up and wait for the following line to be printed:
   Press RETURN to get started!
   Would you like to terminate autoinstall? [yes]: **[Enter]**
   Switch> **show version | include ROM**
   ROM: 12.2(44r)SGA11
   System returned to ROM by reload
   Review the output and look for the ROM version. Verify that the version is the desired new version. If the switch does not boot properly or has the wrong ROM version, contact My Oracle Support.

8. **Return to the step that directed you here from Procedure 9, 4948E-F Configuration Procedure.**

Appendix K. Backup Cisco 4948E-F Aggregation Switch

Application username and password for creating switch backups must be configured on the PMAC management server prior to executing this procedure.

Variable	Value
<switch_backup_user>	admusr
<switch_backup_user_password >	Refer to TR006061 Password Dragon [10] for this value.
<switch_name> hostname of the switch	hostname of the switch
<switch_backup_directory>	/usr/TKLC/smac/etc/switch/backup

These commands are to be executed on the PMAC server connected to the switches that are to be backed up.

1. Verify switch is at least initialized correctly and connectivity to the switch by verifying hostname
   $ **sudo /usr/TKLC/plat/bin/netConfig --device=< switch1A or switch1B > getHostname**

   Hostname: switch1A or 1B

2. Run command "netConfig --repo showService name=ssh_service" and look for ssh service.
   $ **sudo /usr/TKLC/plat/bin/netConfig --repo showService name=ssh_service**
   Service Name: ssh_service
   Type: ssh
   Host: 192.168.1.1
   Options:
   password: C20F7D639AE7E7
   user: admusr

3. Verify existence of the backup directory.
   $ **sudo /bin/ls -al /usr/TKLC/smac/etc/switch/backup**

   If the output contains ls: cannot access /usr/TKLC/smac/etc/switch/backup: No such file or directory create the directory with:
   $ **sudo /bin/mkdir -p /usr/TKLC/smac/etc/switch/backup**

   Change directory permissions:
   $ **sudo /bin/chmod 777 /usr/TKLC/smac/etc/switch/backup**

4. Execute the backup command
   $ **sudo /usr/TKLC/plat/bin/netConfig --device=switch1A backupConfiguration service=ssh_service filename=switch1A-backup**

   $ **sudo /usr/TKLC/plat/bin/netConfig --device=switch1B backupConfiguration service=ssh_service filename=switch1B-backup**

5. Verify both switch configurations were backed up by cat admusr and inspect its contents to ensure it reflects the latest known good switch configurations. Then, copy the files over to the backup directory.

   $ **sudo /bin/ls -al ~admusr**

   ```
   -rw-------  1 admusr admgrp 8926 Feb 4 19:03 switch1A-backup
   -rw-------  1 admusr admgrp   70 Feb 4 19:03 switch1A-backup.info
   -rw-------  1 admusr admgrp 8926 Feb 4 19:03 switch1B-backup
   -rw-------  1 admusr admgrp   70 Feb 4 19:03 switch1B-backup.info
   ```

$ **sudo /bin/cat ~admusr/ <switch1A or switch1B>-backup***

$ **sudo /bin/chmod 644 ~admusr/*backup***

```
-rw-r--r-- 1 admusr admgrp 8926 Feb 4 19:03 switch1A-backup
-rw-r--r-- 1 admusr admgrp   70 Feb 4 19:03 switch1A-backup.info
-rw-r--r-- 1 admusr admgrp 8926 Feb 4 19:03 switch1B-backup
-rw-r--r-- 1 admusr admgrp   70 Feb 4 19:03 switch1B-backup.info
```

$ **sudo /bin/mv -i ~admusr/*backup* /usr/TKLC/smac/etc/switch/backup/**

6. **PMAC:** Perform PMAC application backup from command line.

   $ **sudo /usr/TKLC/smac/bin/pmacadm backup**

   PMAC backup been successfully initiated as task ID 7

   Note: The backup runs as a background task. To check the status of the background task use the PMAC GUI Task Monitor page. The result should eventually be "PMAC Backup successful" and the background task should indicate "COMPLETE".

   Note: The "pmacadm backup" command uses a naming convention which includes a date/time stamp in the file name (Example file name: backupPmac_20111025_100251.pef). In the example provided, the backup file name indicates that it was created on 10/25/2011 at 10:02:51 am server time.

7. **PMAC:** Verify the Backup was successful

   Note: If the background task shows that the backup failed, then the backup did not complete successfully. STOP and contact My Oracle Support by referring to the *1.4 My Oracle Support (MOS)* section of this document.

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

9. Repeat steps ***Step 1*, *Step 4*-*Step 8*** for each switch to be backed up.

Appendix L. MY ORACLE SUPPORT (MOS)

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

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

1. Select 2 for New Service Request
2. Select 3 for Hardware, Networking and Solaris Operating System Support
3. Select 2 for Non-technical issue

You will be connected to a live agent who can assist you with MOS registration and provide Support Identifiers. Simply mention you are a Tekelec Customer new to MOS. MOS is available 24 hours a day, 7 days a week, 365 days a year.

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

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:
• A total system failure that results in loss of all transaction processing capability
• Significant reduction in system capacity or traffic handling capability
• Loss of the system's ability to perform automatic system reconfiguration
• Inability to restart a processor or the system
• Corruption of system databases that requires service affecting corrective actions
• Loss of access for maintenance or recovery operations
• Loss of the system ability to provide any required critical or major trouble notification

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

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

7. Access the OHC site at http://docs.oracle.com.
8. Click Industries.
9. Under the Oracle Communications subheading, click the Oracle Communications documentation link.
10. The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
11. Click the Product and then the Release Number. A list of the entire documentation set for the selected product and release appears.
12. To download a file to your location, right-click the PDF link, select Save target as (or similar command based on your browser), and save to a local folder.