

**Oracle® Communications
Tekelec Platform**

IPv6 Migration Guide

Software Upgrade Procedure

Release 7.0.x

E54704-02

February 2015

Copyright © 2013, 2015, Oracle and/or its affiliates. All rights reserved.

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

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

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

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

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

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

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

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



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

Prior to upgrading any system, log on to [My Oracle Support](#) and review any Technical Service Bulletins (TSBs) that relate to this procedure. Then inform Oracle Support of your upgrade.

To contact Oracle Support by phone, refer to the [Oracle Support Contacts Global Directory](#) to retrieve your country-specific phone number.

Table of Contents

1 INTRODUCTION.....5

1.1 Purpose and Scope.....5

1.2 Product Summary.....5

1.3 References5

 1.3.1 External.....5

1.4 Glossary5

1.5 Conventions.....7

1.6 Component Descriptions.....7

1.7 Software Release Numbering7

1.8 Recommendations8

1.9 Supported Browsers and Versions8

2 GENERAL DESCRIPTION.....9

2.1 Process Summary9

2.2 Supported Upgrade Paths.....9

2.3 Migration Timeline.....9

3 MIGRATION OVERVIEW.....10

3.1 Required Materials10

3.2 Pre-Migration Overview.....10

3.3 Migration Execution Overview.....10

3.4 Post Migration Overview10

3.5 Backout Procedure Overview.....11

3.6 Harvest IPv4 Overview.....11

3.7 Log Files.....11

4 MIGRATION PREPARATION13

4.1 Hardware Preparation13

4.2 Software Migration Preparations.....14

 4.2.1 Network.....14

 4.2.2 Management Servers14

 4.2.3 C7000 Enclosures15

 4.2.4 Services16

5 SOFTWARE MIGRATION PROCEDURES17

5.1 Configure Switches18

5.2 Configure Management Server Dual IP Stack.....27

5.3 Configure Enclosure Dual IP Stack.....33

5.4 Migrate PM&C IP addressing.....42

5.5 Migration Completion56

6 HARVEST IPV461

6.1 Harvest PM&C addresses.....61

6.2 Harvest Enclosure addresses65

6.3 Harvest Management Server addresses71

6.4 Harvest Switch addresses.....76

6.5 Harvest Completion.....79

7 RECOVERY PROCEDURES	80
7.1 Backout Setup	80
7.2 Backout Execution.....	80
8 HEALTH CHECK PROCEDURES	89
APPENDIX A. SWOPS SIGN OFF	91
APPENDIX B. CUSTOMER SIGN-OFF	92
APPENDIX C. LOCATE PRODUCT DOCUMENTATION ON THE ORACLE TECHNOLOGY NETWORK SITE.....	93

List of Figures

Figure 1. Migration Process.....	9
Figure 2. Migration Time Line.....	9

List of Tables

Table 1. Glossary.....	5
Table 2. Supported Internet Browsers and Versions	8
Table 3. Pre-Migration Overview.....	10
Table 4. Migration Execution Overview.....	10
Table 5. Post Migration Overview	11
Table 6. Backout Procedure Overview.....	11
Table 7. Harvest IPv4 Overview	11

List of Procedures

Procedure 1. Configure Network Devices.....	18
Procedure 2 Configure Management Server	27
Procedure 3 Configure Enclosures	33
Procedure 4. Reconfigure PM&C	42
Procedure 5 Finish Migration	56
Procedure 6 Harvest PM&C IPv4 addresses	61
Procedure 7 Harvest Enclosure IPv4 addresses	65
Procedure 8 Harvest iLO IPv4 addresses.....	71
Procedure 9 Harvest Management Server IPv4 addresses.....	73
Procedure 10 Harvest Network IPv4 addresses	76
Procedure 11 Finish Harvest.....	79
Procedure 12 PM&C Recovery Preparation.....	81
Procedure 13 Management recovery	83
Procedure 14 Network Recovery	87
Procedure 15 Health Check	89

1 Introduction

The migration of deployed platforms from an IPv4 address space to IPv6 will occur over time. Customers need a path for reconfiguring applications, on their own schedule. Therefore IPv6 migration will be offered as a procedure independent of software upgrade procedures.

1.1 Purpose and Scope

This document describes the procedures to reconfigure platform components managed with PM&C to enable dual stack IPv4 and IPv6 networking, and add IPv6 addresses to existing platform switches and interfaces. In addition, procedures are provided to remove the IPv4 addressing and services on some interfaces.

This procedure documents how to transition in service platform components to IPv6 addresses. It is not intended for initial deployments. The platform should be fully configured using IPv4 addressing.

The audience for this document includes those responsible for managing and administering the platform. The reader is assumed to be familiar with HP c7000 enclosures, RMSs, and the PM&C application.

1.2 Product Summary

This procedure targets platform components hosted on c7000 enclosures and RMS servers and managed with the PM&C application. Application requirements are not addressed. This includes application specific servers, VM guests, and network devices in c7000 enclosures or RMS servers.

The primary focus of this procedure is networking. The PM&C application requires the Platform “management” and “control” networks, and optionally a dedicated “netBackup” network. Application networks must be migrated separately. The platform management network is a routed network that is used to access system components. The control network is a private non-routed network that is used for managing target RMS and c7000 blades servers. Since this control network is private, it will *not* be migrated to IPv6. Furthermore, the PM&C OS Install feature requires IPv4 for PXE boot functionality on the control network.

1.3 References

1.3.1 External

The following references capture the source material used to create this document.

- [1] *Oracle Communications Tekelec Platform 7.0.x Configuration Guide*, E53486, Current revision

1.4 Glossary

This section lists terms and acronyms specific to this document.

Table 1. Glossary

Acronym/Term	Definition
Activity	Subset of events that support a task.
Backout	The process to take a system back to a state prior to the beginning of the procedure
Control Network	An address space that is used by PM&C to manage devices. No global IPv6 addresses are required on this network

Table 1. Glossary

Acronym/Term	Definition
EBIPA	Enclosure Bay IP Addressing
External documentation	Documentation delivered to a customer, also called “customer documentation.”
Go-No-Go Step	A step that is defined as a decision point to continue or not continue the MOP execution. At this step, both customer and Oracle representative review the current MOP progress and decide whether there is enough time left in the Maintenance Window to complete the MOP and/or, if required, run the Back-Out Procedure.
iLO	Integrated Lights Out remote management port
Internal documentation	Documentation created and used internally to Oracle, often as source material for external documentation.
Management Network	An address space used by Platform utilities and PM&C to discover and manage devices. This is not to be confused with any Application Management (OAM) networks.
Method of Procedure	Set of specific customer and site instructions that define and describe the work to be completed along with the specific procedures (tasks + activities + steps) by which the work is to be performed. A MOP contains both non-technical as well as technical information. Some information is confidential between Oracle and the identified customer.
netBackup Network	The netBackup application often uses a dedicated network, and may require host or network routes.
OA	HP Onboard Administrator
OS	Operating System (e.g. TPD)
OTN	Oracle Technology Network Location of released customer documentation
PM&C	Platform Management & Configuration application
Procedure	Tasks + activities + steps
Procedure table	Table that provides numbered steps with checkboxes
RMS	Rack Mount Server A standalone compute server, not a bladed server in a c7000 enclosure.
Rollback	The process to take a system from a Target Release back to a Source Release including preservation of databases and system configuration.
SLAAC	Stateless Address Auto-configuration
SNMP	Simple Network Management Protocol
Step	Specific work instruction that supports the completion of an activity.
Task	Broad description of activities that need to occur.
TVOE	Tekelec Virtual Operating Environment

1.5 Conventions

Refer to the following example for procedural conventions used in this document. Multiple servers are involved in procedures in this manual. Some steps in the procedures begin with the name or type of server to which the step applies.

Each step has a checkbox for every command within the step that the technician should check to keep track of the progress of the procedure.

The title box describes the operations to be performed during that step.

Each command that the technician is to enter is in 9 point Lucida Console font

1 <input type="checkbox"/>	ServerX: Login	\$ ssh user@somehost
2 <input type="checkbox"/>	display switch hostname	Run command that displays output \$ sudo netConfig --device=<variable> getHostname
3 <input type="checkbox"/>	Verify output	myName

For commands containing site specific variables, the command will use syntax of *<variable>* within the command. The italicized string in angle brackets should be replaced appropriately. The output, shown in unshaded steps, may show site specific configuration information. Therefore the output step often does not contain the same command responses as you will see.

GUI screen captures are always shown with example inputs without additional formatting. In general, text input on a GUI view should be replaced appropriately. GUI controls will be identified using bolded 9 point **Lucida Console** font of the button name or label.

1.6 Component Descriptions

The components addressed include the Management Server, HP c7000 enclosures, TVOE host, PM&C guest, and network devices. Network devices include c7000 enclosure and aggregations switches.

1.7 Software Release Numbering

This procedure is only applicable to Platform 7.0 or newer. The PM&C application must be on a current 6.0 release or newer.

1.8 Recommendations

The migration may be performed in phases over time, rather than in a single maintenance window. Configuring the dual IP stack on the network equipment may be done before reconfiguring the PM&C application. Application migration may be a subsequent procedure.

1.9 Supported Browsers and Versions

This procedure requires accessing services using IPv6, so the installer's host to execute the procedure must have IPv6 access to the platform.

Table 2. Supported Internet Browsers and Versions

Product Release	Supported Browsers	Versions
PM&C 6.0	Microsoft Internet Explorer	8, 9 or 10
HP OA/iLO	Microsoft Internet Explorer	8 or above
HP OA/iLO	Firefox	3.6 or above

2 General Description

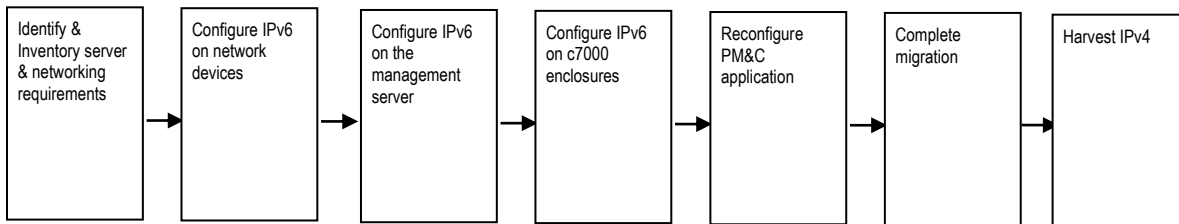
The IPv6 migration is a software reconfiguration procedure involving several components. It also involves procedures that may be executed over extended timeframes.

2.1 Process Summary

Figure 1 shows the major parts of this procedure, from inventory to a final health check.

My Oracle Support (MOS) <https://support.oracle.com> is your initial point of contact for all product support 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>.

Figure 1. Migration Process



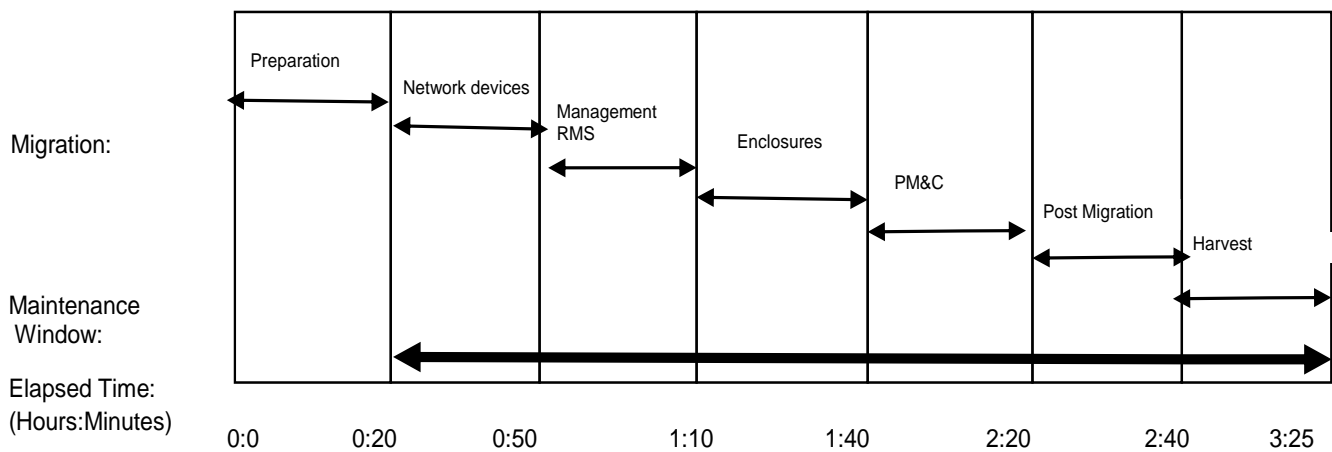
2.2 Supported Upgrade Paths

This migration procedure does not involve a software upgrade. The PM&C server must be at version 6.0 or above, and all components satisfy Platform 7.0 or above requirements.

2.3 Migration Timeline

The following shows an example timeline that assumed a single c7000 enclosure and one RMS.

Figure 2. Migration Time Line



3 Migration Overview

The basic process and approximate time required to migrate a platform to IPv6 address spaces, and to optionally backout in case of error, are shown in the tables in this section.

Migration of applications shall be coordinated with or executed in parallel with the platform migration to ensure that all work is performed within the maintenance window. Note that several variables affect the times shown in the tables – the timing values shown are estimates only. The time estimates here assume a single c7000 enclosure. Scale these times if you are migrating multiple enclosures.

These procedures introduce IPv6 addresses and transition services from IPv4 to IPv6, to setup a dual IP stack and leave IPv4 services. Transition of customer services such as DNS, NTP, SNMP must be coordinated prior to this procedure. Removal of the IPv4 addresses is executed in the Harvesting procedures. In most cases, IPv4 addresses and services are left configured, and harvested at a future time.

3.1 Required Materials

There are no additional materials required for this process.

3.2 Pre-Migration Overview

The pre-migration procedures shown in this table may be executed outside of the maintenance window.

Table 3. Pre-Migration Overview

Phase/Procedure #	Elapsed Time (Hrs:Min)		Downtime (Hrs:Min)		Activity	Impact
	This Step	Cum.	This Step	Cum.		
Software preparation	20	20	0	0	Collect information	None

3.3 Migration Execution Overview

The procedures shown in this table must be executed in the maintenance window.

Table 4. Migration Execution Overview

Phase/Procedure #	Elapsed Time (Hrs:Min)		Downtime (Hrs:Min)		Activity	Impact
	This Step	Cum.	This Step	Cum.		
Procedure 1	30	50	0	0	Configure network devices	Add IPv6 stack
Procedure 2	20	1:10	0	0	Configure management server	Add IPv6
Procedure 3	30	1:40	0	0	Configure enclosures	Add IPv6, OA reset
Procedure 4	40	2:20	5	5	Configure PM&C	Application restart

3.4 Post Migration Overview

The post-migration procedures shown in this table must be executed in the maintenance window.

Table 5. Post Migration Overview

Phase/Procedure #	Elapsed Time (Hrs:Min)		Downtime (Hrs:Min)		Activity	Impact
	This Step	Cum.	This Step	Cum.		
Procedure 5	20	2:40	0	5	Cleanup and verification	None

3.5 Backout Procedure Overview

If necessary, the backout procedures shown in this table must be executed in the maintenance window. This procedure is only applicable before IPv4 harvesting.

Table 6. Backout Procedure Overview

Phase/Procedure #	Elapsed Time (Hrs:Min)		Downtime (Hrs:Min)		Activity	Impact
	This Step	Cum.	This Step	Cum.		
Procedure 12	15	2:55	5	10	Recover PM&C	Application restart
Procedure 13	20	3:15	0	10	Recover OA and servers	Reset OAs
Procedure 14	20	3:35	0	10	Recover network	Network reloads

3.6 Harvest IPv4 Overview

Harvesting IPv4 addresses must be executed in the maintenance window. It is assumed this will be done in a separate window after an extended acceptance period. Therefore this is shown as a discrete procedure.

Table 7. Harvest IPv4 Overview

Phase/Procedure #	Elapsed Time (Hrs:Min)		Downtime (Hrs:Min)		Activity	Impact
	This Step	Cum.	This Step	Cum.		
Procedure 6	15	15	5	5	Configure PMC&C	Application restart
Procedure 7	20	35	0	5	Configure enclosures	
Procedure 9	20	55	0	5	Configure management server	
Procedure 10	15	1:05	0	5	Configure network devices	
Procedure 11	5	1:10	0	5	Verify	

3.7 Log Files

Commands executed during the migration are *not* logged automatically. Session logging requirements are left to the discretion of the application procedure. The `script` command or client side logging may be used for shell sessions. GUI interactions must be implied from various log and audit files. Log files may be subject to rotation, thus deletion. Procedures

do not preserve these on external hosts. In addition to session logging, logs in the following directories contain information that may be necessary to resolve issues:

- TVOE: /var/TKLC/log/netAdm/
- PM&C: /var/TKLC/log/netAdm/
- PM&C: /var/TKLC/smac/logs/

4 Migration Preparation

- Perform inventory and environment discovery to identify components and networking requirements.
- Perform pre-migration system health checks to establish that the system is fit to migrate.

4.1 Hardware Preparation

No hardware or firmware upgrade is required. Hardware limitations exists, such as HP G6 ILO2, or Cisco 3020 switches, All platforms must be on a supported software and firmware release, and be IPv6 capable. If older equipment not qualified for IPv6 exists, contact Oracle Support.

4.2 Software Migration Preparations

All platform components must be compatible for platform 7.0 or later releases. The components include c7000 enclosure OAs, enclosure devices, RMS hardware, RMS iLOs, and network devices.

The PM&C application is a necessary component, and must be on a supported 6.0 or later release.

The `appRev` utility may be used on TPD based hosts to determine the version. Consult release notes to identify additional requirements:

```
$ sudo appRev
```

4.2.1 Network

Record the network information here. Only the new IPv6 platform management network is required. Other platform networks, e.g. for **NetBackup**, are necessary only if they are currently defined. The control network is not migrated. Application networks are not covered by this procedure.

Additional routing information may also be required, e.g. Virtual Routing information if it is provided by customer devices, or host or network routes. The customer should provide the following information.

SLAAC for IPv6 auto configuration is not used by default. All IPv6 addresses and routes should be collected and explicitly provisioned as static.

Network	Server Credentials			
	VLAN ID	IPv6 Network	IPv6 Prefix	IPv6 gateway
Management				
NetBackup (optional)				

Routing information on the TVOE management host and PM&C guest may be displayed with:

```
$ ip -4 r
```

Current routing on switches is displayed with:

```
$ netConfig --device=<deviceName> listRoutes
```

Host & type or function	IPv6 destination	IPv6 gateway

4.2.2 Management Servers

The management RMS that hosts the PM&C application as a guest must be migrated. If a layer 3 aggregation switch is managed, it must be migrated also. Switch access credentials should be available, but only for unforeseen issues. The following information is required:

Server Type	Server Credentials			
	Login	Password	IPv4 Address	IPv6 Address
Management Server iLO				
Management Server TVOE OS	admusr			

Server Type	Server Credentials			
	Login	Password	IPv4 Address	IPv6 Address
PM&C guest OS	admusr			
Aggregation switch “A”				
Aggregation switch “B”				
Application Server(s) iLO				

Application RMS servers will not be reconfigured, but the iLO interfaces on the Platform Management networks should be migrated with this procedure. The RMS iLO is used by PM&C to manage the service, thus should be performed with this procedure. RMS host interfaces must be configured with application specific procedures.

The management RMS OS is configured with two or three platform network bridges that need identified. Typically, they use descriptive names, e.g. “management” or “control”. Applications typically add additional bridges. From this TVOE host, the following command will display the bridge names that can be used to help identify devices:

```
$ sudo netAdm show --type=Bridge
```

TVOE Bridge	Bridge Name
Management	
NetBackup (optional)	

4.2.3 C7000 Enclosures

The system may include multiple c7000 enclosures. For each c7000 enclosure, the below information is required. The enclosures may be displayed from the PM&C GUI or with the command:

```
$ sudo pmaccli getProvEnclosures
```

The Enclosure may have multiple interconnect devices, but only the primary “A” and “B” switches in bays 1 and 2 are migrated within this platform procedure. Additional interconnect devices are dedicated for application use, so they should be migrated with application specific procedures. EBIPA addresses should be allocated for each device bay, but EBIPA interconnect addresses may be applied only to populated bays. Switch access credentials should be recorded, but are only required for unforeseen issues.

Server Type	Server Credentials			
	Login	Password	IPv4 Address	IPv6 Address
c7000 Enclosure OA “A”				
c7000 Enclosure OA “B”				
EBIPA for device iLOs				
EBIPA for interconnects				
Enclosure switch “A”				
Enclosure switch “B”				
Other interconnect devices				

4.2.4 Services

The following services may be used by the platform. If IP addresses are used rather than hostnames resolved by a name service, document the IPv6 addresses below. Name service resolution for services supporting IPv4 and IPv6 is outside the scope of this procedure and is assumed to resolve as desired by the customer.

Service	Service Credentials			
	Login	Password	IPv4 Address	IPv6 Address
DNS primary				
DNS secondary				
NTP 1				
NTP 2				
NTP 3				
LDAP				
SNMP notification target				

5 Software Migration Procedures

To contact Oracle Support by phone, refer to the [Oracle Support Contacts Global Directory](#).

Before beginning the migration, users must perform a system health check. Refer to section 8. This check only ensures that the system does not have any known issues. Performing the system health check determines alarms present in the system, however the procedure may proceed with alarms raised; Contact Oracle support.

Please read the following notes on procedures:

- Procedure completion times shown here are estimates. Times may vary due to differences in user experience, and user preparation.
- Command steps that require user entry are indicated with shaded step numbers.
- Shaded area within response steps must be verified to successfully complete that step.
- Where possible, EXACT command response outputs are shown. EXCEPTIONS are as follows:
 - When explicitly documented as an example.
 - System-specific configuration information such as *addresses*, *hostnames*, and *system features*.
- After completing each step and at each point where data is recorded from the screen, the technician performing the upgrade must initial each step. A check box should be provided.
- Captured data is required for future support reference if no Oracle service technician is present during the procedure.

**** WARNING ****

Some of the procedural steps must be executed on multiple devices. In particular, the network configuration typically must be performed on pairs of switches, or over a variable number of enclosures. Other steps may require multiple commands for duplicated services, e.g. NTP or SNMP.

5.1 Configure Switches

This procedure will add IPv6 addresses on the Aggregation and Enclosure switches, using the **netConfig** utility. This procedure requires that the **netConfig** has been properly setup on the PMAC (or Management server) during system installation and subsequent upgrade activities. For information about **netConfig** setup, see Reference [1].

Note that this procedure has optional steps to handle either Layer 2 or Layer 3 Aggregation switch configurations, as well as deployments without Oracle provided/managed aggregation switches.

Procedure 1. Configure Network Devices

S T E P	Use this procedure to configure IPv6 on network devices. Estimated time of completion: 30 minutes <i>Check off (✓) each step as it is completed. Shaded steps indicate: gray = input, white = output, black = Go-No-Go.</i>	
	Task	Description
1 <input type="checkbox"/>	PM&C: Login	Login to the PM&C host on the management server \$ ssh admusr@<PM&C_IPv4_Address>
2 <input type="checkbox"/>	Backup netConfig data	Backup the pre-migration netConfig repository \$ sudo cp -p /usr/TKLC/plat/etc/TKLCnetwork-config/model.xml /var/TKLC/smac/backup/model.xml-premigrate
3 <input type="checkbox"/>	List backup services	Display the SSH services defined to netConfig for backup. \$ sudo netConfig --repo listServices grep -C 1 ssh
4 <input type="checkbox"/>	Identify service name	Note the name of the service on the PM&C server by the Host address (in the example below, “pmacSCP”): <div style="margin-left: 40px;"> Service Name: pmacSCP Type: ssh Host: 10.240.72.40 </div> <p>Typically, a single SSH service is defined, however other services such as TFTP may be used. After the service name is identified, use the same command to list all properties, including the userid:</p> \$ sudo netConfig --repo showService name=<service>

Procedure 1. Configure Network Devices

<p>5 <input type="checkbox"/></p>		<pre>Service Name: pmacSCP Type: ssh Host: 10.240.72.40 Options: password: FC076474A8F1ECB8 user: pmacuser</pre> <p>Record the service and user name here.</p> <p>netConfig backup service: _____</p> <p>netConfig backup userid: _____</p>
<p>6 <input type="checkbox"/></p>	<p>List aggregation switches</p>	<p>If aggregations switches are managed, find their names in netConfig. Otherwise, skip to step 8. (Supported aggregation switches are Cisco 4948E or 4948E-F):</p> <pre>\$ sudo netConfig --repo listDevices grep -B3 4948E</pre>
<p>7 <input type="checkbox"/></p>	<p>Identify aggregation switches</p>	<p>Note the names of the devices found (in the example below, “aggA” and “aggB”). Record in step 10:</p> <pre>Device: aggB Vendor: Cisco Model: 4948E-F -- Device: aggA Vendor: Cisco Model: 4948E-F</pre> <p>The following command may be useful to help resolve devices:</p> <pre>\$ sudo netConfig --repo showDevice name=<device></pre>
<p>8 <input type="checkbox"/></p>	<p>List enclosure switches</p>	<p>Find all enclosure switch names in netConfig. (Supported enclosure switches are HP 6120 or 6125) :</p> <pre>\$ sudo netConfig --repo listDevices grep -B3 -e 6120 -e 6125</pre>
<p>9 <input type="checkbox"/></p>	<p>Identify enclosure switches</p>	<p>Note the names of the devices found (in the example below, “en1swA” and “en1swB”). Record in step 10:</p> <pre>Device: en1swA Vendor: HP Model: 6120 -- Device: en1swB Vendor: HP Model: 6120</pre>

Procedure 1. Configure Network Devices

<p>10 <input type="checkbox"/></p>	<p>Identify all switches</p>	<p>Platform aggregation switches, and each enclosure’s device in bay 1 and 2 found in the previous steps will be configured. Either of the following commands may be used to gather more information:</p> <pre>\$ sudo netConfig --repo listDevices \$ sudo netConfig --repo showDevice name=<device></pre> <p>Record the names of these devices (e.g. “Cisco 4948 agg switch A” => “aggA”). Check off the Backup box to track progress in the next step.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Backup</th> <th style="text-align: left;">Device</th> <th style="text-align: left;">netConfig name</th> </tr> </thead> <tbody> <tr><td><input type="checkbox"/></td><td></td><td></td></tr> <tr><td><input type="checkbox"/></td><td></td><td></td></tr> <tr><td><input type="checkbox"/></td><td></td><td></td></tr> <tr><td><input type="checkbox"/></td><td></td><td></td></tr> <tr><td><input type="checkbox"/></td><td></td><td></td></tr> <tr><td><input type="checkbox"/></td><td></td><td></td></tr> <tr><td><input type="checkbox"/></td><td></td><td></td></tr> <tr><td><input type="checkbox"/></td><td></td><td></td></tr> <tr><td><input type="checkbox"/></td><td></td><td></td></tr> </tbody> </table> <p>Refer to this list in future steps requiring operations on all switches.</p>	Backup	Device	netConfig name	<input type="checkbox"/>			<input type="checkbox"/>			<input type="checkbox"/>			<input type="checkbox"/>			<input type="checkbox"/>			<input type="checkbox"/>			<input type="checkbox"/>			<input type="checkbox"/>			<input type="checkbox"/>		
Backup	Device	netConfig name																														
<input type="checkbox"/>																																
<input type="checkbox"/>																																
<input type="checkbox"/>																																
<input type="checkbox"/>																																
<input type="checkbox"/>																																
<input type="checkbox"/>																																
<input type="checkbox"/>																																
<input type="checkbox"/>																																
<input type="checkbox"/>																																
<p>11 <input type="checkbox"/></p>	<p>Backup the devices</p>	<p>Perform a backup of <i>all</i> aggregation and enclosure switches recorded in step 10 using the service name found in step 5. The filename option should specify a unique name for each of the backups¹:</p> <pre>\$ sudo netConfig --device=<name> backupConfiguration service=<service> filename=<device>-premigrate</pre>																														
<p>12 <input type="checkbox"/></p>	<p>Add IPv6 address</p>	<p>Add the IPv6 management address to each device. Refer to Section 4.2.2 and 4.2.3.</p> <p>For aggregation devices, use the following command with the management VLAN ID:</p> <pre>\$ sudo netConfig --device=<name> setInterface interface=VLAN<id> ip=<device_IPv6_address></pre> <p>For enclosure devices use:</p> <pre>\$ sudo netConfig --device=<name> setInterface interface=management ip=<device_IPv6_address></pre>																														

¹ Backup files depend upon the service. SSH backup files are stored in the home directory of the “user” specified in the netConfig service. TFTP backup services should have a “dir” option in the netConfig service definition.

Procedure 1. Configure Network Devices

<p>13 <input type="checkbox"/></p>	<p>Verify</p>	<p>For aggregation devices: \$ sudo netConfig --device=<name> getInterface interface=VLAN<id></p> <p>For enclosure devices: \$ sudo netConfig --device=<name> getInterface interface=management</p>
<p>14 <input type="checkbox"/></p>	<p>Determine virtual L3 routing</p>	<p>Layer 3 aggregation switches typically use Virtual Routing when configured as Layer 3 devices. If an IPv4 virtual route exists, an IPv6 one must also be defined.</p> <p>Display the non-application VLANs from Section 4.2.1 with this command: \$ sudo netConfig --device=<name> getVR interface=VLAN<id></p>
<p>15 <input type="checkbox"/></p>	<p>Identify VR Group and Track ID</p>	<p>The lack of any output means no virtual routing is necessary; skip to step 27. Otherwise continue. Use the Group and Track indexes in the output for <groupID> and <trackID> respectively:</p> <pre>Group: 1 HelloTime: = (1.000 1.000) Preemption: enabled State: Backup VIP: 10.240.72.38</pre>
<p>16 <input type="checkbox"/></p>	<p>Determine tracking objects</p>	<p>Each Virtual Router in an L3 deployment should track an uplink using a tracking object. Identify the existing tracking objects: \$ sudo netConfig --device=<name> listTrackingObject</p> <pre>Group: = (<trackID> <trackID>)</pre>
<p>17 <input type="checkbox"/></p>	<p>Record the VR group that tracks each object</p>	<p>For each of the tracking objects identified in the previous step, execute the following command and record which virtual routers are tracking the object. Record the vlan <id> and <groupID> for the given <trackID>: \$ sudo netConfig --device=<name> getTrackingObject id=<trackID></p> <pre>Interface: GE47 Tracked by: VRRP Vlan<id> <groupID> Status: Down</pre> <p>Note: More than one virtual router may track a single tracking object. It is important to record all virtual routers (vlan id and group id) that track each tracking object.</p>

Procedure 1. Configure Network Devices

<p>18 <input type="checkbox"/></p>	<p>Add the virtual router</p>	<p>Run the same command² on both mated aggregations switches for all required VLANs (active or standby states do not need to be examined; execute in either order):</p> <pre>\$ sudo netConfig --device=<name> addVR interface=VLAN<id> id=<groupID> track=<trackID> addrType=autoconfig priority=100 preempt=yes</pre>
<p>19 <input type="checkbox"/></p>	<p>Verify new virtual router</p>	<p>On both aggregations switches, the following command should report the same virtual IPs:</p> <pre>\$ sudo netConfig --device=<name> getVR interface=VLAN<id></pre>
<p>20 <input type="checkbox"/></p>	<p>Record IPv6 virtual IPs</p>	<p>Within the output will be the State, and VIP addresses for both IPv4 and IPv6:</p> <pre>Standby: local Group: = (1 1) Hellotime: = (1.000 1.000) Preemption: = (enabled enabled) Priority: 100 State: = (Active Active) VIP: = (FE80::5:73FF:FEA0:1 10.240.72.38) </pre> <p>If the states are not Active or Standby, wait 10 seconds and try again.</p> <p>Record the link local addresses³:</p> <p>management IPv6 VIP: _____</p> <p>If netBackup is used, VIP: _____</p>

² The “Type=autoconfig” is an option of the HSRP configuration, and does not imply that SSLAC is enabled.

³ The IPv6 virtual routing may use a link-local IPv6 VIP. This value is selected by the switch. In this step, we determine the value assigned by the switch, so it can be used later for configuring default routes on the hosts using this network.

Procedure 1. Configure Network Devices

<p>21 <input type="checkbox"/></p>	<p>Verify the virtual router(s) are tracking the appropriate objects.</p>	<p>For each tracking object identified in the previous step, verify the correct virtual routers are tracking the object: \$ sudo netConfig --device=<name> getTrackingObject id=<trackID> Interface: GE47 Tracked by: = (VRRP Vlan<id> <groupID> HSRP Vlan<id> <groupID>) Status: Up</p>
<p>22 <input type="checkbox"/></p>	<p>Identify IPv4 Routes</p>	<p>Identify all of the IPv4 routes that are configured. \$ sudo netConfig --device=<name> listRoutes Netmask: = (255.255.255.0 255.255.255.255) Network: = (192.168.0.0 0.0.0.0) Next Hop: = (192.168.1.1 192.168.2.1)</p>
<p>23 <input type="checkbox"/></p>	<p>Configure matching IPv6 Routes</p>	<p>Configure IPv6 routes where needed. Run the following command for each network requiring an IPv6 route: \$ sudo netConfig --device=<name> addRoute network=<ipv6 network>/<prefix length> nexthop=<ipv6 address> Example, for the default route: \$ sudo netConfig --device=<name> addRoutes network=::/0 nexthop=fd1d::1 Note: If the nexthop is a linklocal address (fe80::/64) an interface is required. The interface used should be the vlan interface of the network where the linklocal address exists and should use the following format: \$ sudo netConfig --device=<name> addRoutes network=fd1d::/1%VLAN2 nexthop=fe80::1</p>

Procedure 1. Configure Network Devices

<p>24</p> <p><input type="checkbox"/></p>	<p>Verify the routes</p>	<p>Verify the routes have been configured: \$ sudo netConfig --device=<name> listRoutes Interface: VLAN2 Netmask: = (255.255.255.0 255.255.255.255) Network: = (192.168.0.0 0.0.0.0 2001:DB8::/32 ::/0) Next Hop: = (192.168.1.1 192.168.2.1 FD0D:DEBA:D97C:FF1:5054:FF:FE3A:FC2B FE80::1 FD0D::1)</p> <p>Note: In the example above, Interface: VLAN2 corresponds to the route with the linklocal nexthop.</p>
<p>25</p> <p><input type="checkbox"/></p>	<p>Verify Network</p>	<p>The preceding step is executed on <i>both</i> aggregation switches. After both switches are configured, the Active or Standby State should be associated with a single switch. i.e. if for a given VLAN, all 4 states are State = Active, or none are Active stop and contact Oracle support.</p> <p>As an optional test, ping the newly assigned addresses on the Aggregation switche. This may be done from the installer’s laptop, another switch, or external hosts, depending upon IPv6 support and the current configuration. The follows assumes a Linux client:</p> <p>For each switch:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Verify the management interface: \$ ping6 -c 5 <IPv6_Address> <input type="checkbox"/> Verify any IPv6 Virtual Route interfaces on management VLANs using VIPs recorded in step 16 (Link local addresses often must be scoped to a specific interface): \$ ping6 -I <interface> -c 5 <IPv6_Virtual_Address>
<p>26</p> <p><input type="checkbox"/></p>		<p>IPv6 networking is now configured on the network devices. The rest of this procedure is optional, and may depend upon the customer’s support. SNMP alarming requirements for IPv6 and/or IPv6 should be understood.</p>

Procedure 1. Configure Network Devices

<p>27 <input type="checkbox"/></p>	<p>IPv4 service disposition</p>	<p>The host based IPv4 services may be deleted, or left in service. The customer determines when services will be migrated; therefore the rest of this procedure is optional. If all IPv4 services will be left configured, continue to the next procedure.</p> <p>Note: If Layer 3 VRs were defined, IPv4 VIPs are always left configured. Host based services may be removed, but host networking is left in a dual stack mode.</p>
<p>28 <input type="checkbox"/></p>	<p>Show NTP</p>	<p>For each switch, show current NTP servers.</p> <p>\$ sudo netConfig --device=<name> listNTP</p>
<p>29 <input type="checkbox"/></p>	<p>Add IPv6 NTP</p>	<p>If NTP is not used, skip to step 32; otherwise, for each switch, add the NTP servers documented in Section 4.2.4. There may be multiple NTP servers.</p> <p>Aggregation switches do not support NTP over IPv6.</p> <p>For HP 6210 switches, use: \$ sudo netConfig --device=<name> addNTP server=<IPv6_server> priority=3</p> <p>For HP 6215 switches switches, use: \$ sudo netConfig --device=<name> addNTP server=<IPv6_server></p>
<p>30 <input type="checkbox"/></p>	<p>Remove IPv4 NTP</p>	<p>For each switch, remove the old IPv4 service:</p> <p>Note: Leave Aggregation IPv4 NTP services if defined.</p> <p>\$ sudo netConfig --device=<name> deleteNTP server=<IPv4_server></p>
<p>31 <input type="checkbox"/></p>	<p>Verify NTP</p>	<p>For each switch, verify NTP servers.</p> <p>\$ sudo netConfig --device=<name> listNTP</p>
<p>32 <input type="checkbox"/></p>	<p>Show current SNMP</p>	<p>\$ sudo netConfig --device=<name> listSNMPNotify</p>
<p>33 <input type="checkbox"/></p>	<p>Note IPv4 addresses and community strings</p>	<p>If no output is displayed, skip to step 36; otherwise continue to replace the IPv4 addresses with IPv6. Since there is no editSNMP, you must delete the old and add the new, using the Auth and options here.</p> <pre>Host: = (10.240.72.40) Auth: =(Public)</pre>
<p>34 <input type="checkbox"/></p>	<p>Add IPv6 SNMP targets</p>	<p>For each device with an SNMP IPv4 SNMP destination, add the IPv6 target documented in Section 4.2.4:</p> <p>\$ sudo netConfig --device=<name> addSNMPNotify host=<IPv6_target> auth=<community></p>

Procedure 1. Configure Network Devices

35 <input type="checkbox"/>	Remove IPv4 SNMP targets	Optionally remove the SNMP IPv4 SNMP destinations shown in step 32: \$ sudo netConfig --device=<name> deleteSNMPNotify host=<IPv4_target> auth=<community>
36 <input type="checkbox"/>	Show syslog	\$ sudo netConfig --device=<name> listRemoteLogging
37 <input type="checkbox"/>	Note IPv4 addresses	If no output is displayed, skip to step 40; otherwise continue to replace the IPv4 addresses with IPv6. You must delete the old and add the new remote host. server: 10.240.72.40
38 <input type="checkbox"/>	Add IPv6	For each device with an IPv4 syslog destination, add the IPv6 target documented in Section 4.2.4: HP 6120 switches do not support IPv6 syslog. \$ sudo netConfig --device=<name> addRemoteLogging server=<IPv6_Address>
39 <input type="checkbox"/>	Remove IPv4	Optionally remove the IPv4 syslog destinations shown in step 36: Note: Leave HP 6120 IPv4 syslog services if defined. \$ sudo netConfig --device=<name> deleteRemoteLogging server=<IPv4_Address>
40 <input type="checkbox"/>	Logout	\$ exit
---End of Procedure---		

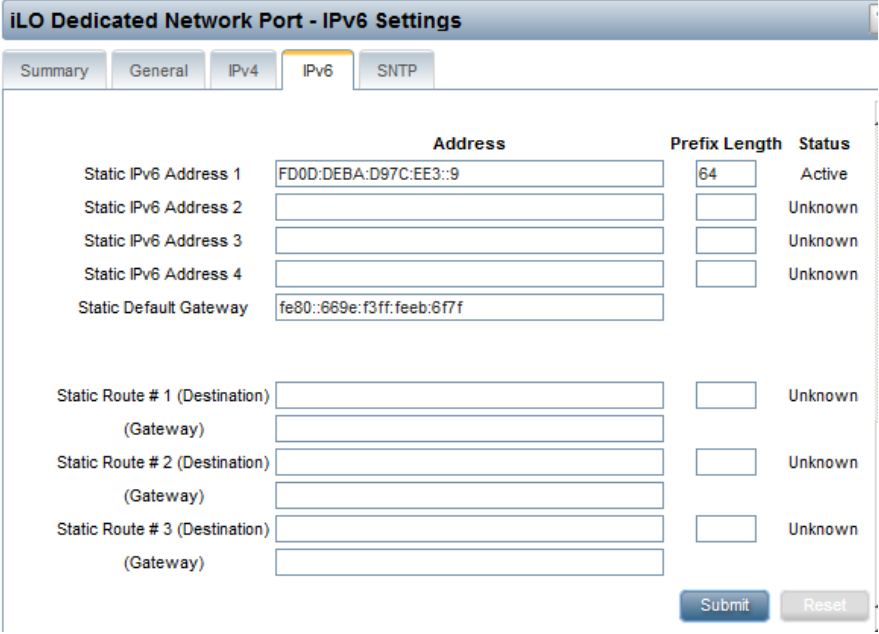
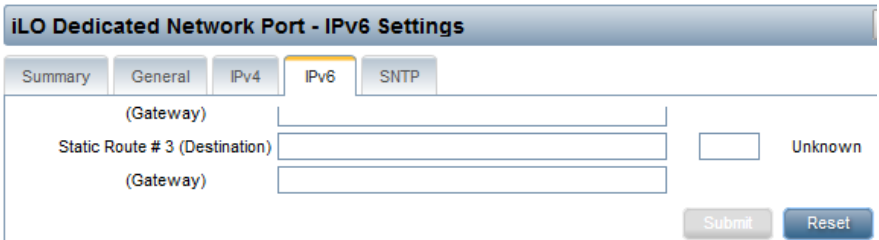
5.2 Configure Management Server Dual IP Stack

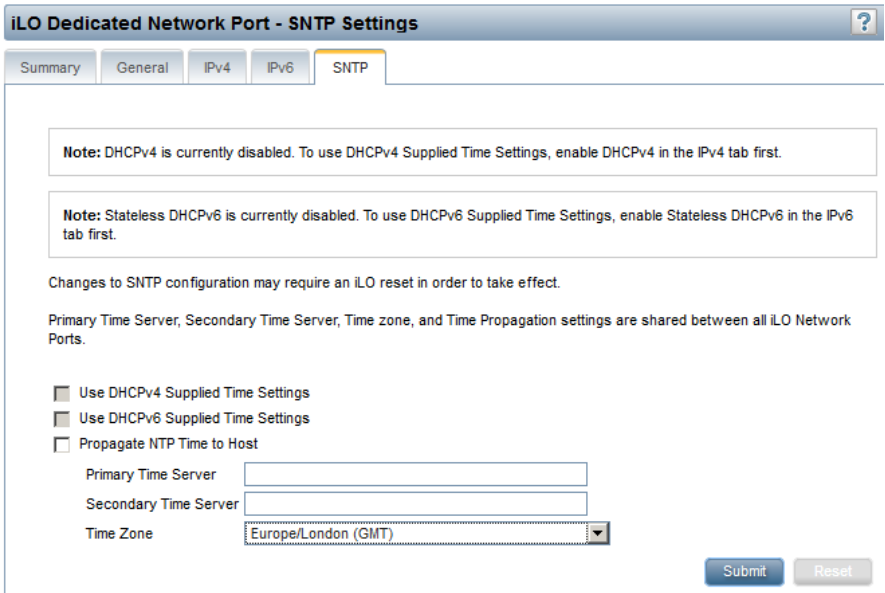
This section must be performed on the management server that hosts the PM&C guest. This procedure may be reused for Application RMS servers to configure the iLO. Since the iLO management is not directly used by, or impacted by, applications, this task may be done with this platform procedure. Only the iLO interface is updated. Application servers are reconfigured here because of the PM&C use of the iLO for managing servers.

Procedure 2 Configure Management Server

S T E P	Use this procedure to configure an IPv6 stack on the management server. Estimated time of completion: 15 minutes <i>Check off (✓) each step as it is completed. Shaded steps indicate: gray = input, white = output, black = Go-No-Go.</i>	
	Task	Description
1 <input type="checkbox"/>	Management Server iLO: Login	Login to the iLO on the management server using a supported browser https://<iLO_IPv4_Address>
2 <input type="checkbox"/>	View current configuration	Navigate to the network configuration: Network -> iLO Dedicated Network Port <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>Expand All</p> <ul style="list-style-type: none"> <input type="checkbox"/> Information <input type="checkbox"/> iLO Federation <input type="checkbox"/> Remote Console <input type="checkbox"/> Virtual Media <input type="checkbox"/> Power Management <input checked="" type="checkbox"/> Network <ul style="list-style-type: none"> iLO Dedicated Network Port Shared Network Port </div>

<p>3</p> <p><input type="checkbox"/></p> <p>Enable IPv6 services</p>	<p>Select the IPv6 tab and update the IPv6 settings. Check the ...use IPv6 first checkbox. Unless applications procedures specify otherwise, disable SLAAC, DHCPv6, and DNS.</p> <p>Scroll down and continue with the next step.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p style="text-align: center; background-color: #4f81bd; color: white; padding: 2px 5px;">iLO Dedicated Network Port - IPv6 Settings</p> <p style="text-align: center;"> Summary General IPv4 IPv6 SNTP </p> <hr/> <p style="text-align: center;">Changes to IPv6 configuration may require an iLO reset in order to take effect.</p> <p><input checked="" type="checkbox"/> iLO Client Applications use IPv6 first</p> <p><input type="checkbox"/> Enable Stateless Address Auto Configuration (SLAAC)</p> <p><input type="checkbox"/> Enable DHCPv6 in Stateful Mode (Address)</p> <p style="padding-left: 20px;"><input type="checkbox"/> Use DHCPv6 Rapid Commit</p> <p><input type="checkbox"/> Enable DHCPv6 in Stateless Mode (Other)</p> <p style="padding-left: 20px;"><input type="checkbox"/> Use DHCPv6 Supplied DNS Servers</p> <p style="padding-left: 20px;"><input type="checkbox"/> Use DHCPv6 Supplied NTP Servers</p> <hr/> <p>Primary DNS Server <input style="width: 150px;" type="text"/></p> <p>Secondary DNS Server <input style="width: 150px;" type="text"/></p> <p>Tertiary DNS Server <input style="width: 150px;" type="text"/></p> <p><input type="checkbox"/> Enable DDNS Server Registration</p> </div>
---	--

<p>4</p> <p><input type="checkbox"/></p>	<p>Configure static IPv6 addresses</p>	<p>Update the Static IPv6 Address and Default gateway. Refer to Section 4.2.3. Then press the Submit button.</p> <p>Note: The gateway may be the customer provided gateway from Section 4.2.1 or the Layer 3 VR optionally created in Procedure 1.</p> 
<p>5</p> <p><input type="checkbox"/></p>	<p>Reset the iLO</p>	<p>Press the Reset button that is enabled after the settings from the previous step are verified. A pop-up will ask to authorize a reset.</p> 
<p>6</p> <p><input type="checkbox"/></p>	<p>Login with IPv6 address</p>	<p>Wait 30 seconds for the iLO to reset, then login with the new IPv6 address to verify.</p> <p>https://[<iLO_IPv6_Address>]</p>

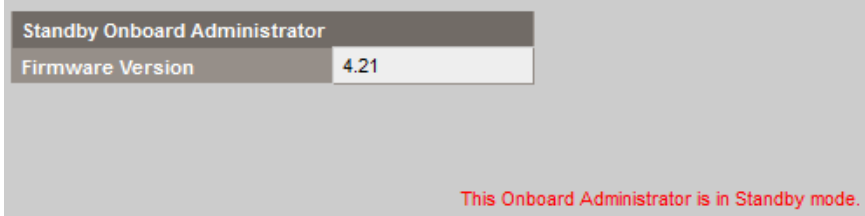
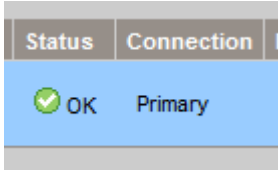
<p>7 <input type="checkbox"/></p>	<p>Change NTP if necessary</p>	<p>Optionally, NTP may be configured with IPv6 addresses. If desired, update the primary and optionally secondary server, then press the Submit and Reset buttons.</p> 
<p>8 <input type="checkbox"/></p>	<p>Logout</p>	<p>Press the Sign out button when complete.</p>
<p>9 <input type="checkbox"/></p>	<p>Application RMSs</p>	<p>If Application RMS servers exist, the iLOs may be updated. Unless directed otherwise, the preceding steps may be used to configure IPv6 addresses on application RMS iLOs.</p>
<p>10 <input type="checkbox"/></p>	<p>Management server: Login</p>	<p>Login to the TVOE host on the management server</p> <pre>\$ ssh admusr@<TVOE_IPv4_Address></pre>
<p>11 <input type="checkbox"/></p>	<p>Add IPv6 address</p>	<p>Add the IPv6 address of the Management Server to the management bridge as recorded in Section 4.2.2.</p> <pre>\$ sudo netAdm set --type=Bridge --name=<management> --address=<ipv6_address> --netmask=<ipv6_prefix></pre>
<p>12 <input type="checkbox"/></p>	<p>Verify dual IP stack</p>	<p>Both the old IPv4 and new IPv6 address should be displayed</p> <pre>\$ sudo netAdm query --type=Bridge --name=<management></pre>

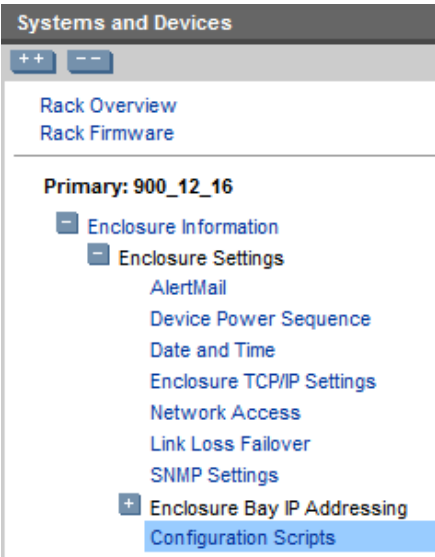
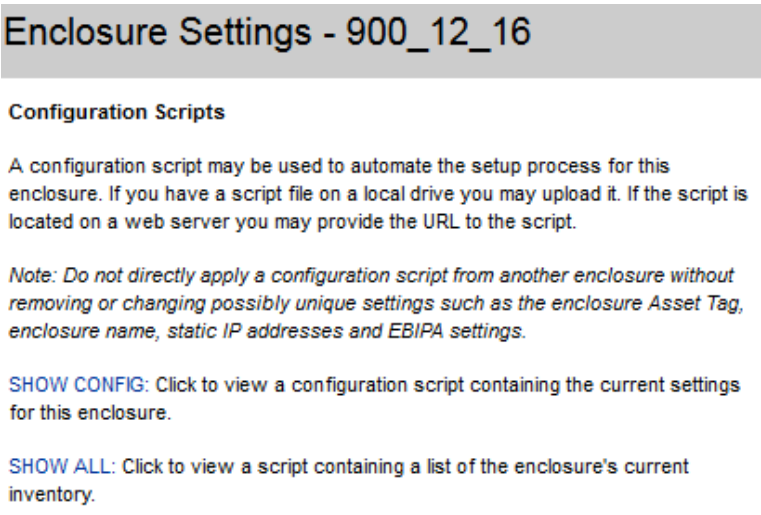
<p>13 <input type="checkbox"/></p>	<p>NetBackup requirements</p>	<p>If the NetBackup feature is implemented, a dedicated bridge may exist and require an IPv6 address as well.</p> <p>List the bridges. Devices other than the management and control likely need an IPv6 address added using commands in the previous steps.</p> <p>\$ sudo netAdm show --type=Bridge</p>															
<p>14 <input type="checkbox"/></p>	<p>Determine routing requirements</p>	<p>If static routes are not required, skip to step 16. Otherwise add routes to the management host from Section 4.2.1.</p> <p>Typically, IPv4 static routes require a similar IPv6 route, but consult network engineers. If netBackup is used, it may require a route.</p>															
<p>15 <input type="checkbox"/></p>	<p>Add routes as required</p>	<p>Use netAdm to add routes. An example to add a default route may look like:</p> <p>\$ sudo netAdm add route --route=default --device=management --gateway=2001::1</p> <p>An example to add a network route is:</p> <p>\$ sudo netAdm add route --route=net --device=netbackup --address=2001:1:: --netmask=96 --gateway=fe80::99</p>															
<p>16 <input type="checkbox"/></p>	<p>Verify IPv6 routes</p>	<p>To verify the routes, the ip command, or preferably ping6 may be used.</p> <p>\$ ip -6 route</p> <p>\$ ping6 -c 3 <IPv6_gateway></p>															
<p>17 <input type="checkbox"/></p>	<p>Check for IPv4 rules</p>	<p>If IPv4 rules for the conserver service exist, they must be added for IPv6.</p> <p>\$ sudo iptablesAdm show --type=rule --protocol=ipv4 --domain=10platnet</p>															
<p>18 <input type="checkbox"/></p>	<p>Verify if IPv6 rules required</p>	<p>If rules were found:</p> <table border="1" data-bbox="576 1308 1284 1409"> <thead> <tr> <th>Persist</th> <th>Domain</th> <th>Table</th> <th>Chain</th> <th>Match</th> </tr> </thead> <tbody> <tr> <td>yes</td> <td>10platnet</td> <td>filter</td> <td>INPUT</td> <td>-s ...</td> </tr> <tr> <td>yes</td> <td>10platnet</td> <td>filter</td> <td>INPUT</td> <td>-s ...</td> </tr> </tbody> </table> <p>Continue with the next step to add the IPv6 rules. Otherwise skip the step.</p>	Persist	Domain	Table	Chain	Match	yes	10platnet	filter	INPUT	-s ...	yes	10platnet	filter	INPUT	-s ...
Persist	Domain	Table	Chain	Match													
yes	10platnet	filter	INPUT	-s ...													
yes	10platnet	filter	INPUT	-s ...													
<p>19 <input type="checkbox"/></p>	<p>Verify they do not exist</p>	<p>If IPv6 rules for the conserver service already exist, skip the next step.</p> <p>\$ sudo iptablesAdm show --type=rule --protocol=ipv6 --domain=10platnet</p> <p>Output from the proceeding command implies the rules exist and the next step is skipped.</p>															

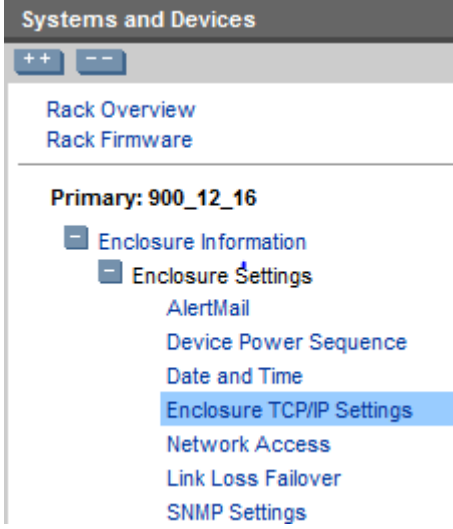
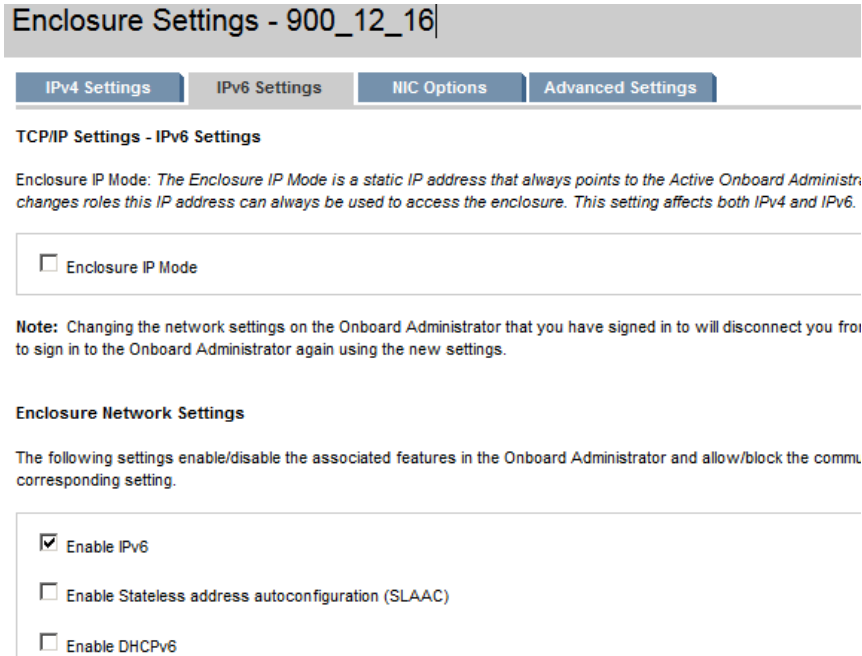
<p>20 <input type="checkbox"/></p>	<p>Add IPv6 firewall rules</p>	<p>Add the two rules show in the previous step to the IPv6 firewall. Replace “<pmacIPv6>” with the PM&C IPv6 management address.</p> <pre>\$ sudo iptablesAdm append --type=rule --protocol=ipv6 --domain=10platnet --table=filter --chain=INPUT --match="-s <pmacIPv6>/128 -p tcp --dport 782 -j ACCEPT" --persist=yes \$ sudo iptablesAdm append --type=rule --protocol=ipv6 --domain=10platnet --table=filter --chain=INPUT --match="-s <pmacIPv6>/128 -p tcp --dport 1024:65535 -j ACCEPT" --persist=yes</pre>
<p>21 <input type="checkbox"/></p>	<p>Verify the new rules exist</p>	<pre>\$ sudo iptablesAdm show --type=rule --protocol=ipv6 --domain=10platnet</pre>
<p>22 <input type="checkbox"/></p>	<p>Verify management server requirements</p>	<p>The management server may provide or require IPv6 services. If client services, such as NTP services or SNMP targets, are defined by IPv4 addresses rather than names, they must be updated.</p> <p>Refer to Reference [1].</p>
<p>23 <input type="checkbox"/></p>	<p>Logout</p>	<pre>\$ exit</pre>
<p>24 <input type="checkbox"/></p>	<p>Application RMS servers</p>	<p>Application RMS servers are managed by PM&C over the iLO interface. Those RMS server iLOs may be migrated to IPv6 at this time – baring Application requirements. Steps 1 through 8 may be executed on each Application RMS server.</p> <p>Note: If this is executed, you will update the target RMSes in procedure 4 also.</p>
<p>---End of Procedure---</p>		

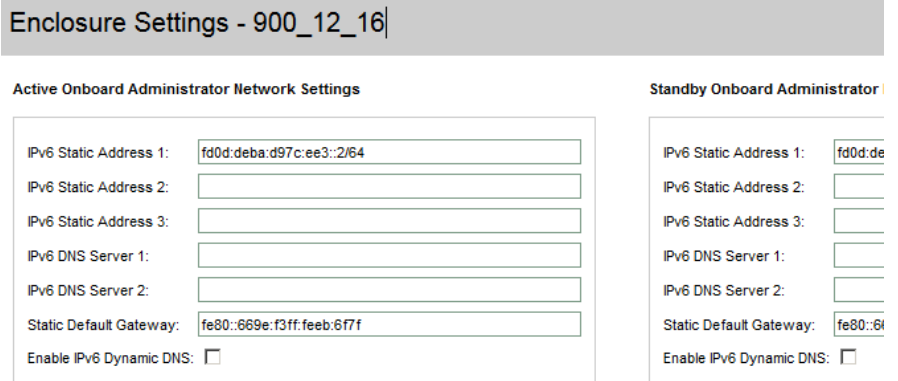
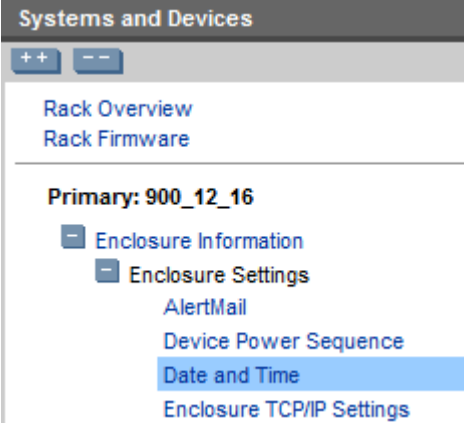
5.3 Configure Enclosure Dual IP Stack

Procedure 3 Configure Enclosures

S T E P	Use this procedure to configure an IPv6 stack on c7000 enclosures Estimated time of completion: 30 minutes <i>Check off (✓) each step as it is completed. Shaded steps indicate: gray = input, white = output, black = Go-No-Go.</i>	
	Task	Description
1 <input type="checkbox"/>	Identify all c7000 enclosures	Each enclosure must be individually configured. The following steps are repeated for each enclosure in Section 4.2.3.
2 <input type="checkbox"/>	OA: Login	Login to the active OA using a supported browser. https://<OA_IPv4_Address> If the OA is in Standby mode, login with the other IPv4 address:  Also ensure the system Status is OK. 

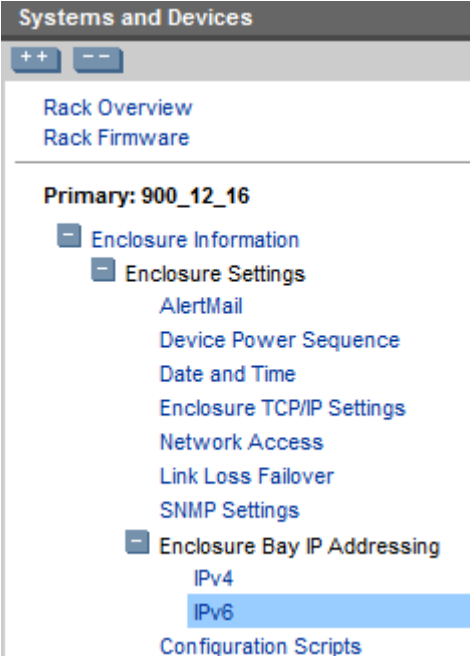
<p>3 <input type="checkbox"/></p>	<p>Backup OA configuration</p>	<p>Navigate to the Configuration Scripts:</p> <p>Enclosure Information -> Enclosure Settings -> Configuration Scripts</p>  <p>The screenshot shows a web interface titled "Systems and Devices" with expand/collapse buttons. Under "Primary: 900_12_16", the "Enclosure Information" menu is expanded to show "Enclosure Settings", which is further expanded to show "Configuration Scripts" as the selected option.</p>
<p>4 <input type="checkbox"/></p>	<p>Display config as a script</p>	<p>View the configuration script. Click on the SHOW CONFIG link. This will open a new tab or window.</p>  <p>The screenshot shows the "Enclosure Settings - 900_12_16" page. The "Configuration Scripts" section explains that a script can be used to automate setup and provides a "SHOW CONFIG" link to view the current settings script.</p>
<p>5 <input type="checkbox"/></p>	<p>Save the script</p>	<p>Save the text in the window to a file, as applicable for the browser (e.g. <code>File->Save</code> or <code><control>-s</code>). A copy should also be placed on the PM&C server using <code>scp</code> in the following directory:</p> <p><code>/var/TKLC/smac/backup</code></p>

<p>6</p> <p><input type="checkbox"/></p>	<p>View the IP settings</p>	<p>Navigate to the TCP/IP configuration:</p> <p>Enclosure Information -> Enclosure Settings -> Enclosure TCP/IP Settings</p>  <p>The screenshot shows a web interface titled "Systems and Devices" with expand/collapse buttons. Under "Primary: 900_12_16", there is a list of settings: Enclosure Information, Enclosure Settings, AlertMail, Device Power Sequence, Date and Time, Enclosure TCP/IP Settings (highlighted), Network Access, Link Loss Failover, and SNMP Settings.</p>
<p>7</p> <p><input type="checkbox"/></p>	<p>Enable IPv6</p>	<p>On the IPv6 Settings tab, check Enable IPv6, but not SLACC or DHCPv6.</p> <p>Scroll down and continue with the next step.</p>  <p>The screenshot shows the "Enclosure Settings - 900_12_16" page with tabs for IPv4 Settings, IPv6 Settings, NIC Options, and Advanced Settings. Under "TCP/IP Settings - IPv6 Settings", there is a checkbox for "Enclosure IP Mode" which is unchecked. A note states: "Changing the network settings on the Onboard Administrator that you have signed in to will disconnect you from to sign in to the Onboard Administrator again using the new settings." Under "Enclosure Network Settings", there are three checkboxes: "Enable IPv6" (checked), "Enable Stateless address autoconfiguration (SLAAC)" (unchecked), and "Enable DHCPv6" (unchecked).</p>

<p>8</p> <p><input type="checkbox"/></p>	<p>Set OA IPv6 addresses</p>	<p>On the same tab, set the IPv6 Static Address 1 and default gateway for both the Active and Standby OA. Then press the Apply button.</p>  <p>The screenshot shows the 'Enclosure Settings - 900_12_16' configuration page. It is divided into two columns: 'Active Onboard Administrator Network Settings' and 'Standby Onboard Administrator Network Settings'. Under 'Active', the 'IPv6 Static Address 1' field contains 'fd0d:deba:d97c:ee3::2/64' and the 'Static Default Gateway' field contains 'fe80::669e:f3ff:feeb:6f7f'. Under 'Standby', the 'IPv6 Static Address 1' field contains 'fd0d:de' and the 'Static Default Gateway' field contains 'fe80::6f'. There are also fields for IPv6 Static Address 2 and 3, IPv6 DNS Server 1 and 2, and checkboxes for 'Enable IPv6 Dynamic DNS'.</p>
<p>9</p> <p><input type="checkbox"/></p>	<p>Verify the time settings</p>	<p>Navigate to the Date and Time configuration:</p>  <p>The screenshot shows the 'Systems and Devices' configuration page. It has a navigation bar with expand/collapse buttons. Below the navigation bar, there are links for 'Rack Overview' and 'Rack Firmware'. Under the 'Primary: 900_12_16' section, there is a tree view of settings: 'Enclosure Information', 'Enclosure Settings', 'AlertMail', 'Device Power Sequence', 'Date and Time' (which is highlighted in blue), and 'Enclosure TCP/IP Settings'.</p>

<p>10 <input type="checkbox"/></p>	<p>Update NTP if necessary</p>	<p>If static IPv4 addresses are used, replace with the appropriate IPv6 address for the NTP server(s). If IPv4 services should be kept, leave the IPv4 and add the IPv6 address. Then press the Apply button.</p> <div data-bbox="581 453 1442 974" style="border: 1px solid #ccc; padding: 10px;"> <p><input checked="" type="radio"/> Set time using an NTP server</p> <p><i>Required Field *</i></p> <p>Primary NTP Server:* <input type="text" value="fd0d:deba:d97c:ee3::10"/> <small>(ex. 61.206.115.3, 2002::1 or host.example.com)</small></p> <p>Secondary NTP Server: <input type="text"/> <small>(ex. 61.206.115.3, 2002::1 or host.example.com)</small></p> <p>Poll Interval:* <input type="text" value="720"/> seconds</p> <p>Time Zone:* <input type="text" value="EST5EDT"/></p> <p style="text-align: right;"><input type="button" value="Apply"/></p> </div>
<p>11 <input type="checkbox"/></p>	<p>Verify the SNMP settings</p>	<p>Navigate to the SNMP Settings and select the Settings tab:</p> <div data-bbox="573 1071 1019 1596" style="border: 1px solid #ccc; padding: 10px;"> <p>Systems and Devices</p> <p>++ --</p> <p>Rack Overview</p> <p>Rack Firmware</p> <hr/> <p>Primary: 900_12_16</p> <ul style="list-style-type: none"> <input type="checkbox"/> Enclosure Information <input checked="" type="checkbox"/> Enclosure Settings <ul style="list-style-type: none"> AlertMail Device Power Sequence Date and Time Enclosure TCP/IP Settings Network Access Link Loss Failover <li style="background-color: #e0f0ff;">SNMP Settings <input type="checkbox"/> Enclosure Bay IP Addressing </div>

<p>12</p> <p><input type="checkbox"/></p>	<p>Update SNMP if necessary</p>	<p>If static IPv4 addresses are used for alert destination, add the IPv6 address for the SNMP server by pressing the New button. The IPv4 addresses may be optionally deleted. Otherwise, skip to step 16.</p> <div data-bbox="574 443 1459 848" style="border: 1px solid #ccc; padding: 10px;"> <p>SNMP Alert Destinations</p> <table border="1" data-bbox="597 506 1450 579"> <thead> <tr> <th><input type="checkbox"/></th> <th>Version</th> <th>Destination</th> <th>Community</th> <th>User - Engine ID</th> <th>Security</th> <th>Inform</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>SNMPv1/2c</td> <td>10.240.72.41</td> <td>public</td> <td>N/A</td> <td>N/A</td> <td>N/A</td> </tr> </tbody> </table> <p style="text-align: right;"> <input type="button" value="New"/> <input type="button" value="Delete"/> </p> <p>Test Alert Destinations</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p style="text-align: center;">Send a test alert to all configured alert destinations.</p> <p style="text-align: right;"><input type="button" value="Send Test Alert"/></p> </div> </div>	<input type="checkbox"/>	Version	Destination	Community	User - Engine ID	Security	Inform	<input type="checkbox"/>	SNMPv1/2c	10.240.72.41	public	N/A	N/A	N/A
<input type="checkbox"/>	Version	Destination	Community	User - Engine ID	Security	Inform										
<input type="checkbox"/>	SNMPv1/2c	10.240.72.41	public	N/A	N/A	N/A										
<p>13</p> <p><input type="checkbox"/></p>	<p>Configure SNMP</p>	<p>Enter the SNMP Alert Destination's IPv6 address, then press the Add Alert button.</p> <div data-bbox="574 978 1446 1482" style="border: 1px solid #ccc; padding: 10px;"> <p style="background-color: #f0f0f0; padding: 5px;">Add SNMP Alert</p> <p><i>Required Field *</i></p> <p>Alert Destination * <input type="text" value="fd0d:deba:d97c:ee3::100"/> (ex. 61.206.115.3, 201)</p> <p>Community String: <input type="text" value="public"/></p> <p><input type="checkbox"/> SNMPv3 SNMPv3 alerts cannot be created until at least one SNMPv3 user exists.</p> <p>User: <input type="text" value="none"/></p> <p>Security: <input type="text" value="authNoPriv"/></p> <p>Inform Message <input type="checkbox"/></p> <p style="text-align: right;"> <input type="button" value="Cancel"/> <input type="button" value="Add Alert"/> </p> </div>														
<p>14</p> <p><input type="checkbox"/></p>	<p>Complete the SNMP settings</p>	<p>Press the Apply button to complete the changes.</p>														
<p>15</p> <p><input type="checkbox"/></p>	<p>Verify SNMP</p>	<p>If you have access to the SNMP manager, test the SNMP configuration by pressing the Send Test Alert button. The SNMP manager should be checked to ensure the alert was received.</p>														

<p>16</p> <p><input type="checkbox"/></p>	<p>Configure bay addressing</p>	<p>Navigate to the EBIPA IPv6 settings and select the Device Bays tab:</p>  <p>The screenshot shows a web interface titled "Systems and Devices" with expand/collapse buttons. Under "Primary: 900_12_16", there is a tree view of settings. "Enclosure Bay IP Addressing" is expanded, and "IPv6" is selected and highlighted in blue.</p>
--	---------------------------------	--

<p>17</p> <p><input type="checkbox"/></p>	<p>Set bay IPv6 addressing</p>	<p>Enter the EBIPA Address and Gateway for Bay 1. If using consecutive IPv6 addresses, press on the Autofill button. Otherwise you must enter each bay individually. Check the Enabled box to enable all bays.</p> <p>When the data is populated, press the Apply button.</p> <p>Enclosure Bay IP Addressing (for IPv6)</p> <p>Device Bays Device Bays Double Dense Side A Device Bays Double Dense Side B Interconnect Bays</p> <p>Device Bay iLO Processor Address Range: <i>The form below provides fixed IPv6 address assignment to the device bay. If there is an IPv6 address in the EBIPA Address field, the device (iLO) has previously been configured or has received a DHCPv6 address.</i></p> <p>Note: <i>All of the selected iLO Processors will be reset if the protocol is enabled. If each iLO has been previously given a static IPv6 address, these EBIPAv6 settings will not change the static IPv6 address. If the iLO IPv6 address has been configured via an external DHCPv6 service, the EBIPAv6 settings will override the existing DHCPv6 address.</i></p> <p>Device List: <i>This list displays the IPv6 addresses that will be assigned to each of the device bays if EBIPAV6 is enabled. Clicking the autofill "down arrow" button will fill in consecutive IPv6 addresses for all of the device bays below the arrow. The domain and DNS servers will also be copied to each of the consecutive bays in the list.</i></p> <table border="1"> <thead> <tr> <th>Bay</th> <th><input checked="" type="checkbox"/> Enabled</th> <th>EBIPA Address</th> <th>Gateway</th> <th>Domain</th> <th>DNS Servers</th> <th>Autofill</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input checked="" type="checkbox"/></td> <td>fd0d:deba:d97c:e</td> <td>69e:f3ff:feeb:6f7f</td> <td></td> <td></td> <td>⌵</td> </tr> <tr> <td>2</td> <td><input checked="" type="checkbox"/></td> <td></td> <td></td> <td></td> <td></td> <td>⌵</td> </tr> </tbody> </table>	Bay	<input checked="" type="checkbox"/> Enabled	EBIPA Address	Gateway	Domain	DNS Servers	Autofill	1	<input checked="" type="checkbox"/>	fd0d:deba:d97c:e	69e:f3ff:feeb:6f7f			⌵	2	<input checked="" type="checkbox"/>					⌵
Bay	<input checked="" type="checkbox"/> Enabled	EBIPA Address	Gateway	Domain	DNS Servers	Autofill																	
1	<input checked="" type="checkbox"/>	fd0d:deba:d97c:e	69e:f3ff:feeb:6f7f			⌵																	
2	<input checked="" type="checkbox"/>					⌵																	
<p>18</p> <p><input type="checkbox"/></p>	<p>Set interconnect IPv6 addresses</p>	<p>Select the Interconnect Bays tab, and perform the above step to set the IPv6 EBIPA Address and Gateway for the device bays, and check Enabled. Then press the Apply button.</p> <p>If all bays are not in use, or will not be assigned addresses, enter and enable the devices as desired.</p> <p>Enclosure Bay IP Addressing (for IPv6)</p> <p>Device Bays Device Bays Double Dense Side A Device Bays Double Dense Side B Interconnect Bays</p> <p>Interconnect Bay Management Port Address Range: <i>The form below provides fixed IPv6 address assignment to the interconnect bays in the enclosure. If there is an IPv6 address in the EBIPA Address field, the interconnect device has previously been configured or has received a DHCPv6 address.</i></p> <p>Note: <i>If each interconnect has been previously given a static IPv6 address, these EBIPAV6 settings will not change the static IPv6 address. If an interconnect management IPv6 address has been configured via an external DHCPv6 service, the EBIPAV6 settings will override the external DHCPv6 address only after lease expiration.</i></p> <p>Interconnect List: <i>This list displays the IPv6 addresses that will be assigned to each of the interconnect bays if EBIPAV6 is enabled. Clicking the autofill "down arrow" button will fill in consecutive IPv6 addresses for all of the interconnect bays below the arrow. The domain and DNS servers will also be copied to each of the consecutive bays in the list.</i></p> <table border="1"> <thead> <tr> <th>Bay</th> <th><input type="checkbox"/> Enabled</th> <th>EBIPA Address</th> <th>Gateway</th> <th>Domain</th> <th>DNS Servers</th> <th>Autofill</th> <th>Current Address</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="checkbox"/></td> <td></td> <td></td> <td></td> <td></td> <td>⌵</td> <td>N/A</td> </tr> </tbody> </table>	Bay	<input type="checkbox"/> Enabled	EBIPA Address	Gateway	Domain	DNS Servers	Autofill	Current Address	1	<input type="checkbox"/>					⌵	N/A					
Bay	<input type="checkbox"/> Enabled	EBIPA Address	Gateway	Domain	DNS Servers	Autofill	Current Address																
1	<input type="checkbox"/>					⌵	N/A																

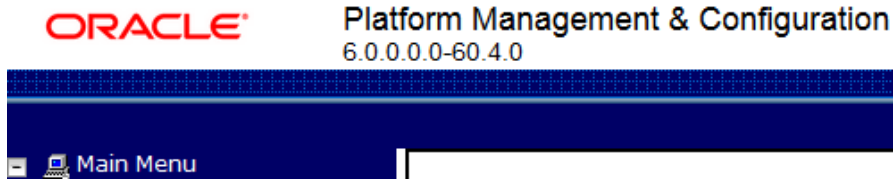
<p>19 <input type="checkbox"/></p>	<p>Logout</p>	<p>Press the Sign Out button when complete.</p>
<p>20 <input type="checkbox"/></p>	<p>Repeat procedure for additional enclosures</p>	<p>If additional enclosures exist, repeat the procedure with the next enclosure.</p>
<p style="text-align: center;">---End of Procedure---</p>		

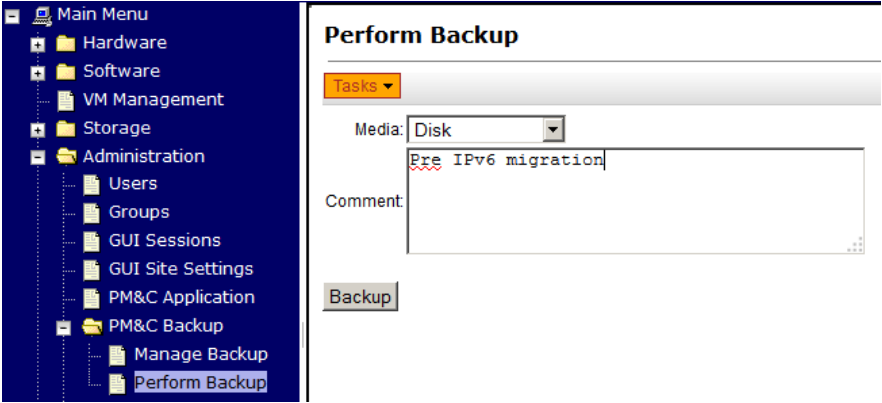
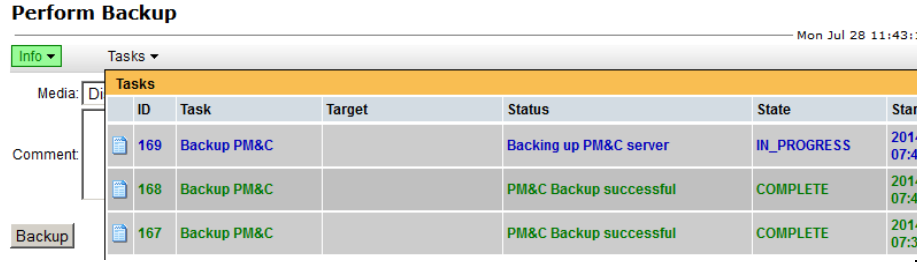
5.4 Migrate PM&C IP addressing

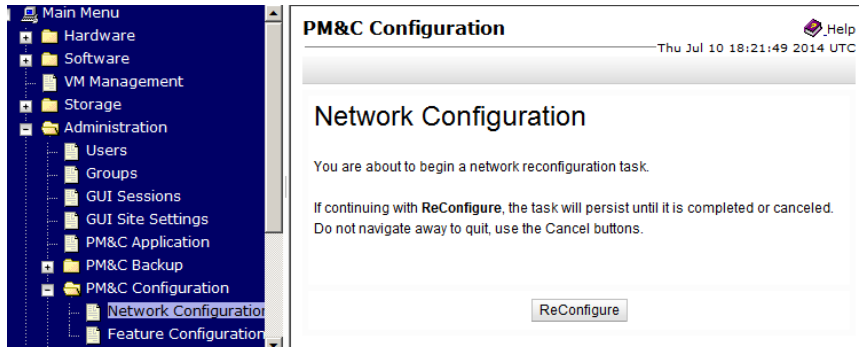
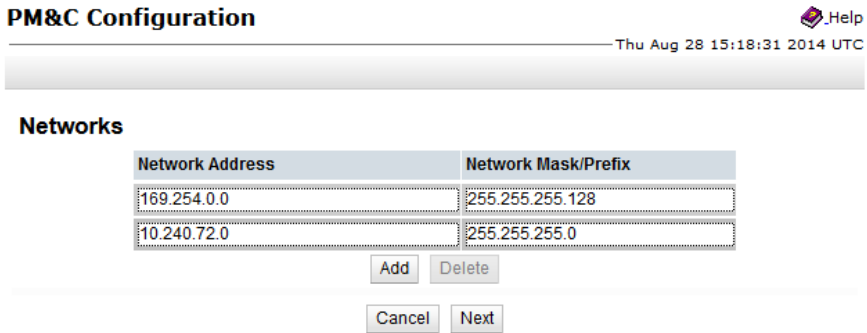
****** WARNING ******


The PM&C application reconfiguration is presented as a wizard. There is no “back” button, and you should not use the browser’s back button; cancel and restart if you make an error. If you navigate away from the wizard, the process is left in progress. Returning to the wizard will ask you to finish or cancel the in-progress task. The safe response is to cancel and restart the reconfiguration. Use the **cancel** button to quit the wizard.




Procedure 4. Reconfigure PM&C

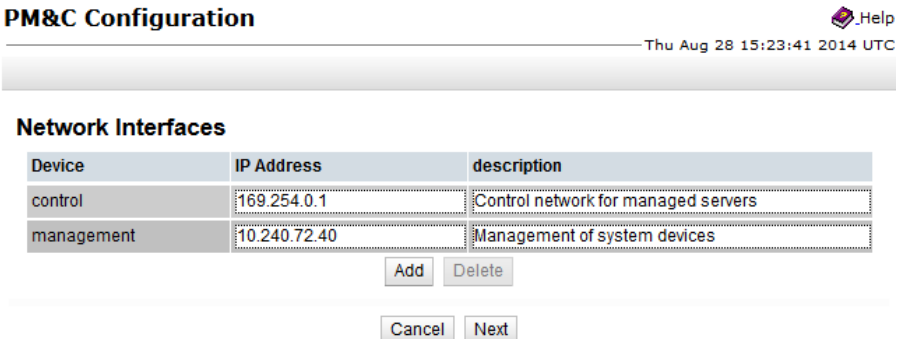
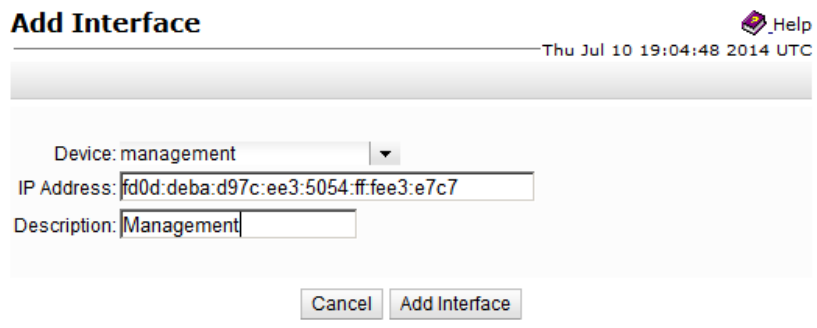
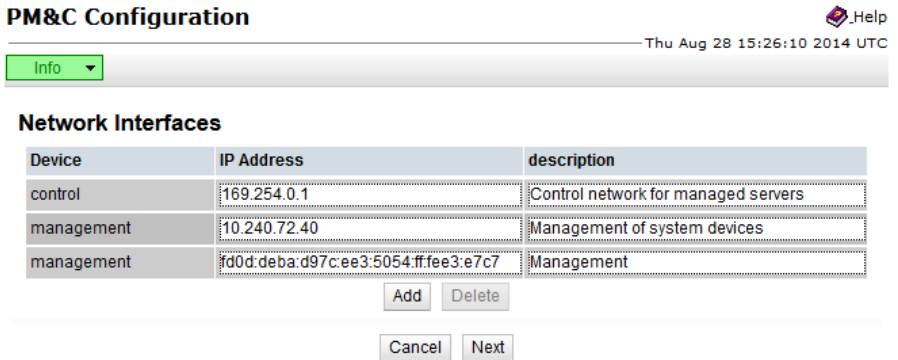
S T E P	Use this procedure to migrate the PM&C application to IPv6 addressing. Estimated time of completion: 15 minutes <i>Check off (✓) each step as it is completed. Shaded steps indicate: gray = input, white = output, black = Go-No-Go.</i>	
	Task	Description
1 <input type="checkbox"/>	PM&C: Login to GUI	Login to the PM&C from a supported browser https://<PM&C_IPv4_address>
2 <input type="checkbox"/>	Verify release	PM&C must be at a current 6.0 release or later: 

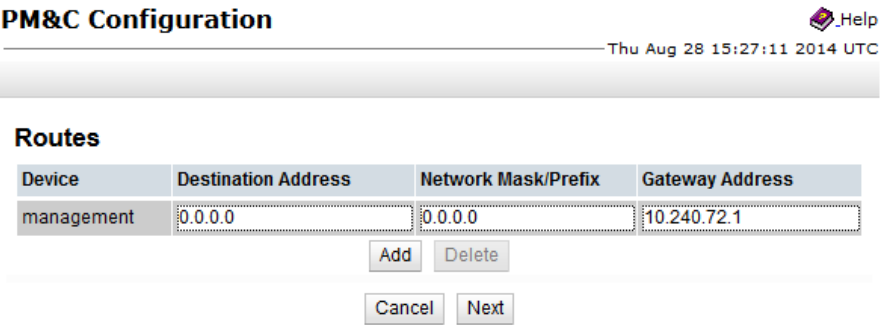
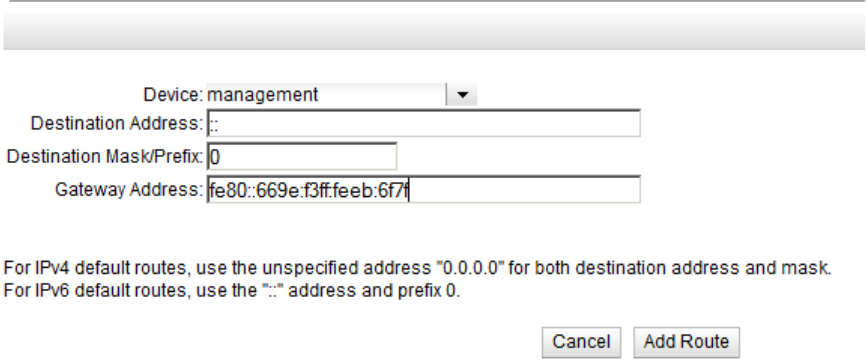
<p>3</p> <p><input type="checkbox"/></p>	<p>Backup PM&C</p>	<p>In the PM&C GUI, navigate to the Backup:</p> <p>Main Menu -> Administration -> PM&C Backup -> Perform Backup</p> <p>Select Disk for the media, enter a Comment, and then press the Backup button.</p>  <p>The screenshot shows the PM&C GUI navigation menu on the left with 'Administration' expanded and 'PM&C Backup' selected. On the right, the 'Perform Backup' form is shown with 'Media' set to 'Disk' and a comment field containing 'IPv6 migration'. A 'Backup' button is visible at the bottom.</p>																								
<p>4</p> <p><input type="checkbox"/></p>	<p>Note timestamp</p>	<p>Press the Tasks drop down to view the task and verify the backup completes successfully.</p> <p>Note the Start Time, it may be needed to identify the correct backup file for recovery: _____</p> <p>The backup file is named using the end time: <code>backupPmac_<yyyymmdd_hhmmss>.pef</code></p>  <p>The screenshot shows the 'Perform Backup' page with the 'Tasks' dropdown menu open. A table lists the backup tasks with columns for ID, Task, Target, Status, State, and Start Time.</p> <table border="1" data-bbox="673 1354 1495 1522"> <thead> <tr> <th>ID</th> <th>Task</th> <th>Target</th> <th>Status</th> <th>State</th> <th>Start Time</th> </tr> </thead> <tbody> <tr> <td>169</td> <td>Backup PM&C</td> <td></td> <td>Backing up PM&C server</td> <td>IN_PROGRESS</td> <td>2014-07-28 07:43:11</td> </tr> <tr> <td>168</td> <td>Backup PM&C</td> <td></td> <td>PM&C Backup successful</td> <td>COMPLETE</td> <td>2014-07-28 07:40:11</td> </tr> <tr> <td>167</td> <td>Backup PM&C</td> <td></td> <td>PM&C Backup successful</td> <td>COMPLETE</td> <td>2014-07-28 07:38:11</td> </tr> </tbody> </table>	ID	Task	Target	Status	State	Start Time	169	Backup PM&C		Backing up PM&C server	IN_PROGRESS	2014-07-28 07:43:11	168	Backup PM&C		PM&C Backup successful	COMPLETE	2014-07-28 07:40:11	167	Backup PM&C		PM&C Backup successful	COMPLETE	2014-07-28 07:38:11
ID	Task	Target	Status	State	Start Time																					
169	Backup PM&C		Backing up PM&C server	IN_PROGRESS	2014-07-28 07:43:11																					
168	Backup PM&C		PM&C Backup successful	COMPLETE	2014-07-28 07:40:11																					
167	Backup PM&C		PM&C Backup successful	COMPLETE	2014-07-28 07:38:11																					

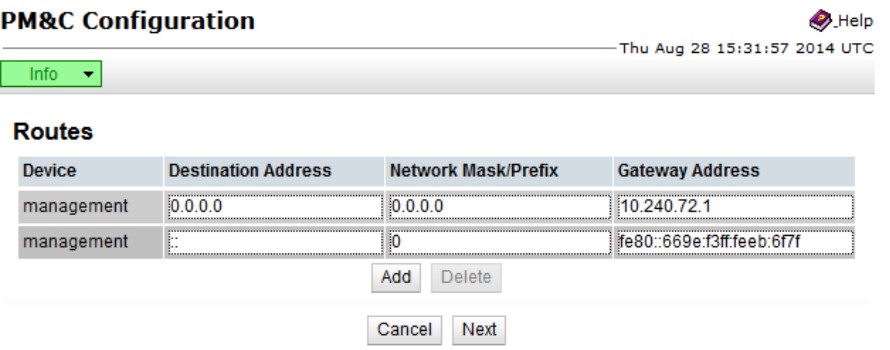
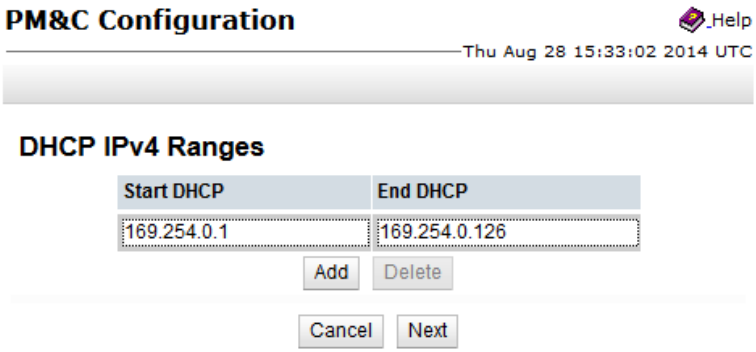
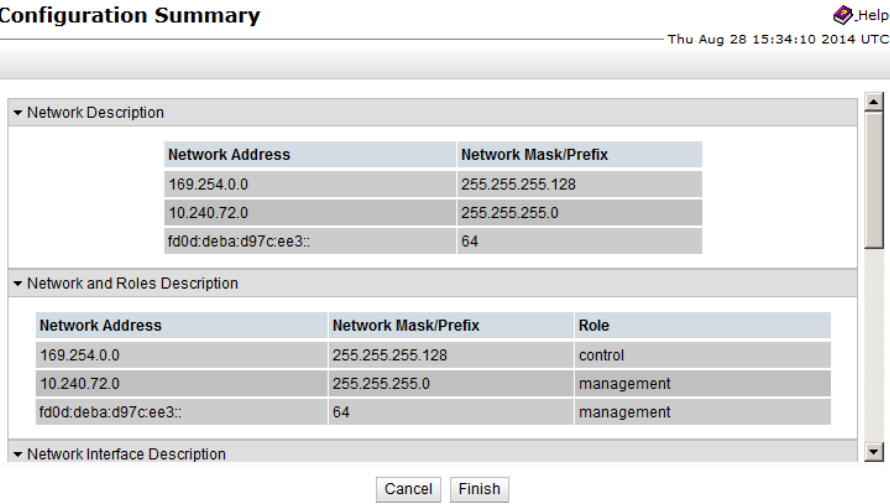
<p>5</p> <p><input type="checkbox"/></p>	<p>Start reconfiguration</p>	<p>Navigate to:</p> <p>Main Menu -> Admin -> PM&C Configuration -> Network Configuration</p> <p>Then press the ReConfigure button.</p> 
<p>6</p> <p><input type="checkbox"/></p>	<p>Use dual stack</p>	<p>Although there are no IPv4 requirements on the management network, do not delete the IPv4 network. Leave it configured as a dual-stack system. Harvesting will be performed later.</p> 
<p>7</p> <p><input type="checkbox"/></p>	<p>Add IPv6 management network</p>	<p>Press the Add button.</p>

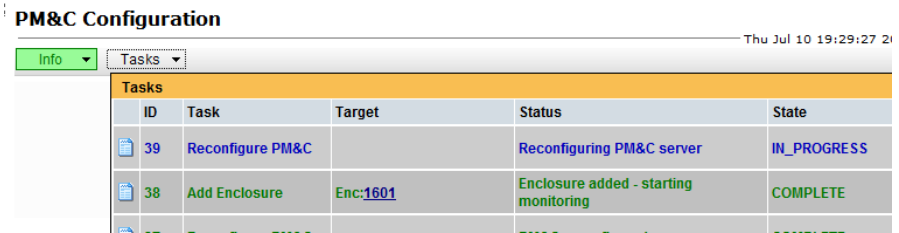
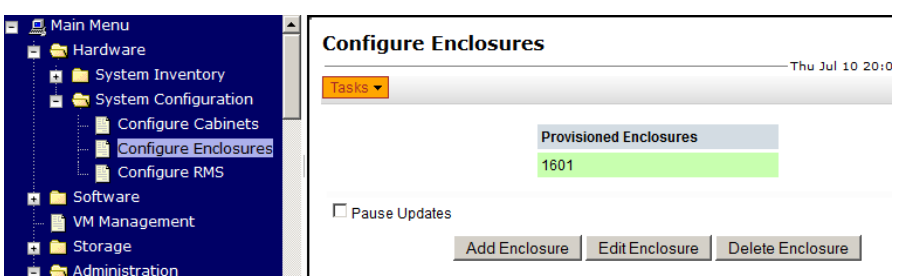
<p>8</p> <input type="checkbox"/>	<p>Add the network</p>	<p>Enter the IPv6 Network Address and Prefix for the management network. Always use 0 for the VLAN ID in a guest environment. Then press the Add Network button.</p> <p>Add Network</p> <hr/> <p>Network Address: <input type="text" value="fd0d:deba:d97c:ee3::"/></p> <p>Network Mask/Prefix: <input type="text" value="64"/></p> <p>VLAN ID: <input type="text" value="0"/></p> <p><input type="button" value="Cancel"/> <input type="button" value="Add Network"/></p>								
<p>9</p> <input type="checkbox"/>	<p>Continue</p>	<p>Verify the address is correct, then press the Next button.</p> <p>PM&C Configuration  Help</p> <p style="text-align: right;">Thu Aug 28 15:21:33 2014 UTC</p> <p><input type="button" value="Info"/> ▾</p> <p>Networks</p> <table border="1" data-bbox="646 1087 1365 1247"> <thead> <tr> <th>Network Address</th> <th>Network Mask/Prefix</th> </tr> </thead> <tbody> <tr> <td>169.254.0.0</td> <td>255.255.255.128</td> </tr> <tr> <td>10.240.72.0</td> <td>255.255.255.0</td> </tr> <tr> <td>fd0d:deba:d97c:ee3::</td> <td>64</td> </tr> </tbody> </table> <p><input type="button" value="Add"/> <input type="button" value="Delete"/></p> <p><input type="button" value="Cancel"/> <input type="button" value="Next"/></p>	Network Address	Network Mask/Prefix	169.254.0.0	255.255.255.128	10.240.72.0	255.255.255.0	fd0d:deba:d97c:ee3::	64
Network Address	Network Mask/Prefix									
169.254.0.0	255.255.255.128									
10.240.72.0	255.255.255.0									
fd0d:deba:d97c:ee3::	64									

<p>10</p> <p><input type="checkbox"/></p>	<p>Configure the network</p>	<p>Press the Add button to configure the newly added management network.</p> <p>PM&C Configuration _Help Thu Aug 28 15:09:02 2014 UTC</p> <hr/> <p>Network Roles</p> <table border="1"> <thead> <tr> <th>Network Address</th> <th>Network Mask/Prefix</th> <th>Role</th> </tr> </thead> <tbody> <tr> <td>169.254.0.0</td> <td>255.255.255.128</td> <td>control</td> </tr> <tr> <td>10.240.72.0</td> <td>255.255.255.0</td> <td>management</td> </tr> </tbody> </table> <p style="text-align: center;"> <input type="button" value="Add"/> <input type="button" value="Delete"/> </p> <p style="text-align: center;"> <input type="button" value="Cancel"/> <input type="button" value="Next"/> </p>	Network Address	Network Mask/Prefix	Role	169.254.0.0	255.255.255.128	control	10.240.72.0	255.255.255.0	management			
Network Address	Network Mask/Prefix	Role												
169.254.0.0	255.255.255.128	control												
10.240.72.0	255.255.255.0	management												
<p>11</p> <p><input type="checkbox"/></p>	<p>Apply the role</p>	<p>Use the drop down for the Network Address and the Role Name to associate the new management network with the management role, and then press the Add Network Role button.</p> <p>Add Network Role _Help Thu Jul 10 18:51:13 2014 UTC</p> <hr/> <p>Network Address: <input type="text" value="fd0d:deba:d97c:ee3::"/></p> <p>Role Name: <input type="text" value="management"/></p> <p style="text-align: center;"> <input type="button" value="Cancel"/> <input type="button" value="Add Network Role"/> </p>												
<p>12</p> <p><input type="checkbox"/></p>	<p>Continue</p>	<p>Verify the information is correct, then press the Next button.</p> <p>PM&C Configuration _Help Thu Aug 28 15:12:57 2014 UTC</p> <p><input type="button" value="Info"/></p> <hr/> <p>Network Roles</p> <table border="1"> <thead> <tr> <th>Network Address</th> <th>Network Mask/Prefix</th> <th>Role</th> </tr> </thead> <tbody> <tr> <td>169.254.0.0</td> <td>255.255.255.128</td> <td>control</td> </tr> <tr> <td>10.240.72.0</td> <td>255.255.255.0</td> <td>management</td> </tr> <tr> <td>fd0d:deba:d97c:ee3::</td> <td>64</td> <td>management</td> </tr> </tbody> </table> <p style="text-align: center;"> <input type="button" value="Add"/> <input type="button" value="Delete"/> </p> <p style="text-align: center;"> <input type="button" value="Cancel"/> <input type="button" value="Next"/> </p>	Network Address	Network Mask/Prefix	Role	169.254.0.0	255.255.255.128	control	10.240.72.0	255.255.255.0	management	fd0d:deba:d97c:ee3::	64	management
Network Address	Network Mask/Prefix	Role												
169.254.0.0	255.255.255.128	control												
10.240.72.0	255.255.255.0	management												
fd0d:deba:d97c:ee3::	64	management												

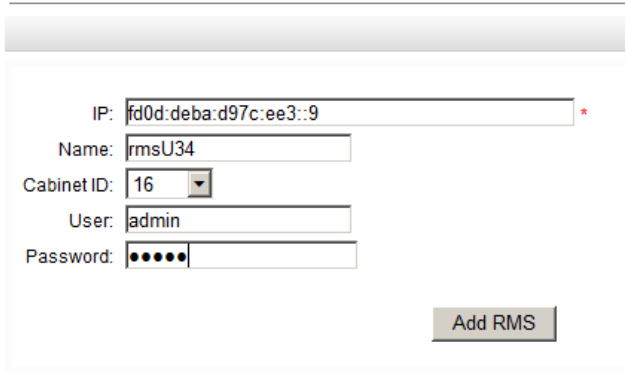
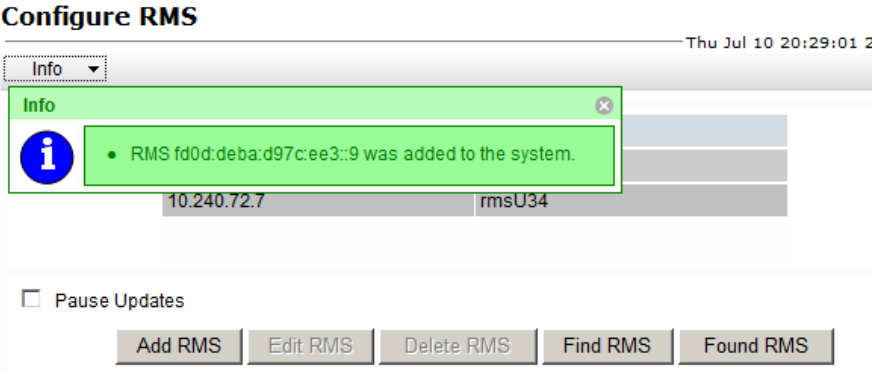
<p>13</p> <p><input type="checkbox"/></p>	<p>Add a new management interface</p>	<p>Press the Add button to define the new interface.</p>  <p>PM&C Configuration .Help Thu Aug 28 15:23:41 2014 UTC</p> <p>Network Interfaces</p> <table border="1"> <thead> <tr> <th>Device</th> <th>IP Address</th> <th>description</th> </tr> </thead> <tbody> <tr> <td>control</td> <td>169.254.0.1</td> <td>Control network for managed servers</td> </tr> <tr> <td>management</td> <td>10.240.72.40</td> <td>Management of system devices</td> </tr> </tbody> </table> <p style="text-align: center;">Add Delete Cancel Next</p>	Device	IP Address	description	control	169.254.0.1	Control network for managed servers	management	10.240.72.40	Management of system devices			
Device	IP Address	description												
control	169.254.0.1	Control network for managed servers												
management	10.240.72.40	Management of system devices												
<p>14</p> <p><input type="checkbox"/></p>	<p>Configure the IPv6 address</p>	<p>Select the management device from the drop down Device list, enter the PM&C IPv6 management IP address, and a Description. Then press the Add Interface button.</p>  <p>Add Interface .Help Thu Jul 10 19:04:48 2014 UTC</p> <p>Device: management</p> <p>IP Address: fd0d:deba:d97c:ee3:5054:ff:fee3:e7c7</p> <p>Description: Management</p> <p style="text-align: center;">Cancel Add Interface</p>												
<p>15</p> <p><input type="checkbox"/></p>	<p>Continue</p>	<p>Verify the information is correct, then press the Next button.</p>  <p>PM&C Configuration .Help Thu Aug 28 15:26:10 2014 UTC</p> <p>Info</p> <p>Network Interfaces</p> <table border="1"> <thead> <tr> <th>Device</th> <th>IP Address</th> <th>description</th> </tr> </thead> <tbody> <tr> <td>control</td> <td>169.254.0.1</td> <td>Control network for managed servers</td> </tr> <tr> <td>management</td> <td>10.240.72.40</td> <td>Management of system devices</td> </tr> <tr> <td>management</td> <td>fd0d:deba:d97c:ee3:5054:ff:fee3:e7c7</td> <td>Management</td> </tr> </tbody> </table> <p style="text-align: center;">Add Delete Cancel Next</p>	Device	IP Address	description	control	169.254.0.1	Control network for managed servers	management	10.240.72.40	Management of system devices	management	fd0d:deba:d97c:ee3:5054:ff:fee3:e7c7	Management
Device	IP Address	description												
control	169.254.0.1	Control network for managed servers												
management	10.240.72.40	Management of system devices												
management	fd0d:deba:d97c:ee3:5054:ff:fee3:e7c7	Management												
<p>16</p> <p><input type="checkbox"/></p>	<p>Add routes?</p>	<p>In absence of application requirements, the IPv6 routing is provisioned statically, not auto-configured. If routes are not necessary, skip to step 21.</p> <p>A default route is typical. A route for NetBackup may also be required.</p>												

<p>17</p> <p><input type="checkbox"/></p>	<p>Add static routes</p>	<p>Press the Add button to add a route.</p>  <p>The screenshot shows the 'PM&C Configuration' interface. At the top right, there is a date and time: 'Thu Aug 28 15:27:11 2014 UTC' and a 'Help' icon. Below this is a 'Routes' section with a table. The table has four columns: 'Device', 'Destination Address', 'Network Mask/Prefix', and 'Gateway Address'. The first row shows 'management' in the Device column, '0.0.0.0' in Destination Address, '0.0.0.0' in Network Mask/Prefix, and '10.240.72.1' in Gateway Address. Below the table are buttons for 'Add', 'Delete', 'Cancel', and 'Next'.</p>
<p>18</p> <p><input type="checkbox"/></p>	<p>Define a default route</p>	<p>Define the default route on the management network. Select the management Device in the drop-down list, enter the default route IPv6 Destination for <code>::/0</code> by using “::” and 0 for the address and prefix respectively. Then enter the next hop Gateway. When done, press the Add Route button.</p>  <p>The screenshot shows the 'Add Route' dialog box. It has a 'Device' dropdown menu set to 'management'. Below it are three input fields: 'Destination Address' with '::', 'Destination Mask/Prefix' with '0', and 'Gateway Address' with 'fe80::669e:f3ff:eeb:6f71'. At the bottom, there is a note: 'For IPv4 default routes, use the unspecified address "0.0.0.0" for both destination address and mask. For IPv6 default routes, use the "::" address and prefix 0.' and buttons for 'Cancel' and 'Add Route'.</p>
<p>19</p> <p><input type="checkbox"/></p>	<p>NetBackup requirements</p>	<p>If the NetBackup feature is implemented, a dedicated route may exist, and require an IPv6 network or host route as well.</p> <p>If necessary, add the route as done in the previous steps.</p>

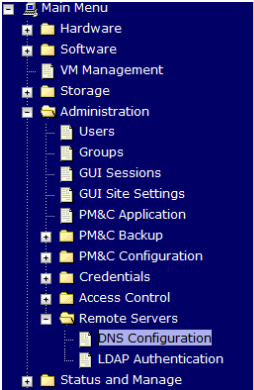
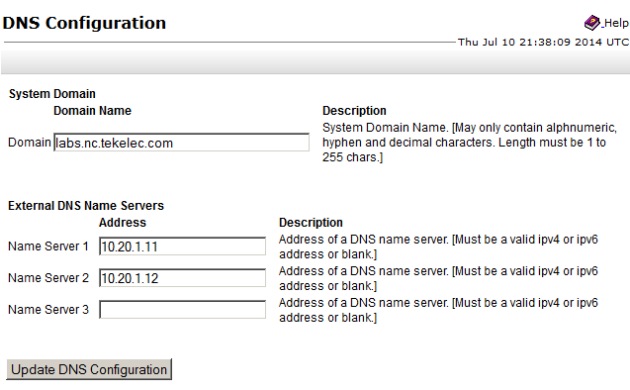
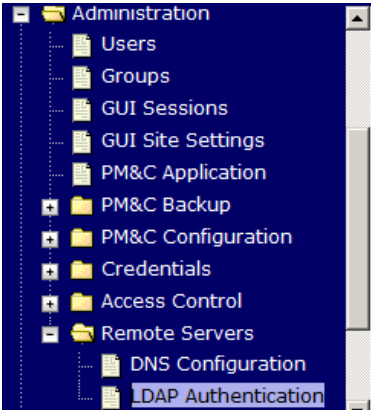
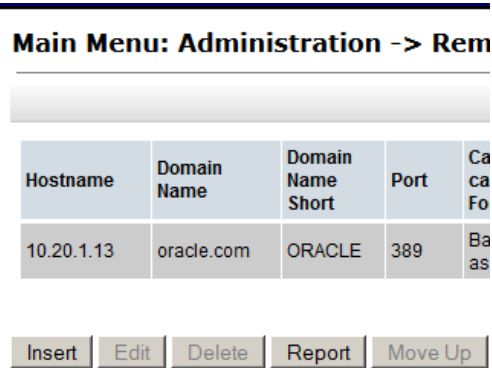
<p>20</p> <p><input type="checkbox"/></p>	<p>Continue</p>	<p>Verify the information is correct, then press the Next button.</p>  <p>PM&C Configuration .Help Thu Aug 28 15:31:57 2014 UTC</p> <p>Info ▾</p> <p>Routes</p> <table border="1"> <thead> <tr> <th>Device</th> <th>Destination Address</th> <th>Network Mask/Prefix</th> <th>Gateway Address</th> </tr> </thead> <tbody> <tr> <td>management</td> <td>0.0.0.0</td> <td>0.0.0.0</td> <td>10.240.72.1</td> </tr> <tr> <td>management</td> <td>::</td> <td>0</td> <td>fe80::669e:f3ff:feeb:67f</td> </tr> </tbody> </table> <p style="text-align: center;">Add Delete</p> <p style="text-align: center;">Cancel Next</p>	Device	Destination Address	Network Mask/Prefix	Gateway Address	management	0.0.0.0	0.0.0.0	10.240.72.1	management	::	0	fe80::669e:f3ff:feeb:67f								
Device	Destination Address	Network Mask/Prefix	Gateway Address																			
management	0.0.0.0	0.0.0.0	10.240.72.1																			
management	::	0	fe80::669e:f3ff:feeb:67f																			
<p>21</p> <p><input type="checkbox"/></p>	<p>Continue</p>	<p>The IPv4 DHCP service on the control network is not modified. Press the Next button.</p>  <p>PM&C Configuration .Help Thu Aug 28 15:33:02 2014 UTC</p> <p>DHCP IPv4 Ranges</p> <table border="1"> <thead> <tr> <th>Start DHCP</th> <th>End DHCP</th> </tr> </thead> <tbody> <tr> <td>169.254.0.1</td> <td>169.254.0.126</td> </tr> </tbody> </table> <p style="text-align: center;">Add Delete</p> <p style="text-align: center;">Cancel Next</p>	Start DHCP	End DHCP	169.254.0.1	169.254.0.126																
Start DHCP	End DHCP																					
169.254.0.1	169.254.0.126																					
<p>22</p> <p><input type="checkbox"/></p>	<p>Verify, and reconfigure</p>	<p>Verify the information, and then press the Finish button.</p>  <p>Configuration Summary .Help Thu Aug 28 15:34:10 2014 UTC</p> <p>▾ Network Description</p> <table border="1"> <thead> <tr> <th>Network Address</th> <th>Network Mask/Prefix</th> </tr> </thead> <tbody> <tr> <td>169.254.0.0</td> <td>255.255.255.128</td> </tr> <tr> <td>10.240.72.0</td> <td>255.255.255.0</td> </tr> <tr> <td>fd0d:deba:d97c:ee3::</td> <td>64</td> </tr> </tbody> </table> <p>▾ Network and Roles Description</p> <table border="1"> <thead> <tr> <th>Network Address</th> <th>Network Mask/Prefix</th> <th>Role</th> </tr> </thead> <tbody> <tr> <td>169.254.0.0</td> <td>255.255.255.128</td> <td>control</td> </tr> <tr> <td>10.240.72.0</td> <td>255.255.255.0</td> <td>management</td> </tr> <tr> <td>fd0d:deba:d97c:ee3::</td> <td>64</td> <td>management</td> </tr> </tbody> </table> <p>▾ Network Interface Description</p> <p style="text-align: center;">Cancel Finish</p>	Network Address	Network Mask/Prefix	169.254.0.0	255.255.255.128	10.240.72.0	255.255.255.0	fd0d:deba:d97c:ee3::	64	Network Address	Network Mask/Prefix	Role	169.254.0.0	255.255.255.128	control	10.240.72.0	255.255.255.0	management	fd0d:deba:d97c:ee3::	64	management
Network Address	Network Mask/Prefix																					
169.254.0.0	255.255.255.128																					
10.240.72.0	255.255.255.0																					
fd0d:deba:d97c:ee3::	64																					
Network Address	Network Mask/Prefix	Role																				
169.254.0.0	255.255.255.128	control																				
10.240.72.0	255.255.255.0	management																				
fd0d:deba:d97c:ee3::	64	management																				

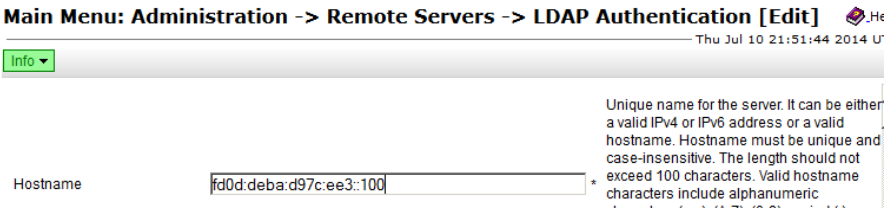
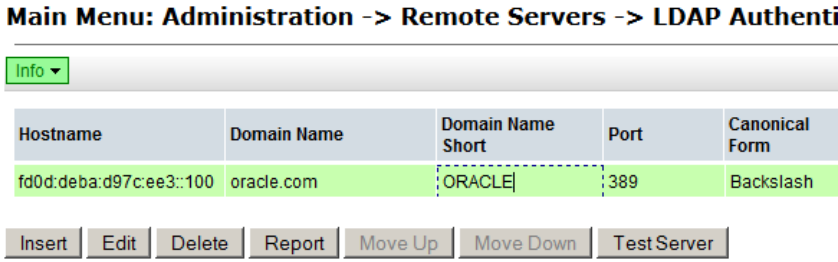
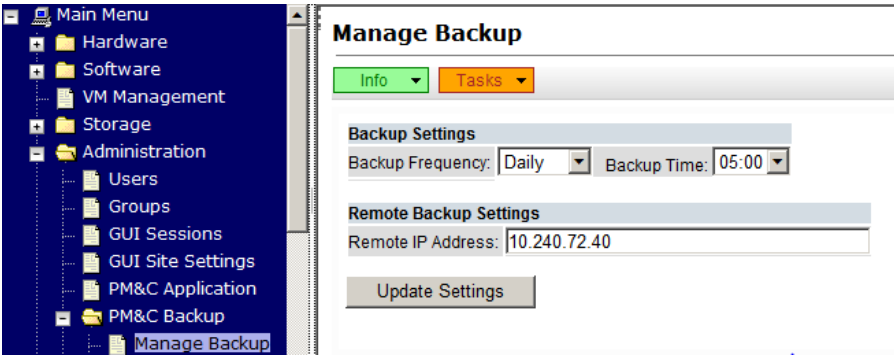
<p>23</p> <p><input type="checkbox"/></p>	<p>Wait for the task to complete</p>	<p>The reconfiguration background task is started. The example below is displayed by pressing the Tasks button. It should show as COMPLETE within a few minutes.</p>  <p>PM&C Configuration Thu Jul 10 19:29:27 21</p> <p>Info Tasks</p> <table border="1"> <thead> <tr> <th>ID</th> <th>Task</th> <th>Target</th> <th>Status</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>39</td> <td>Reconfigure PM&C</td> <td></td> <td>Reconfiguring PM&C server</td> <td>IN_PROGRESS</td> </tr> <tr> <td>38</td> <td>Add Enclosure</td> <td>Enc:1601</td> <td>Enclosure added - starting monitoring</td> <td>COMPLETE</td> </tr> </tbody> </table>	ID	Task	Target	Status	State	39	Reconfigure PM&C		Reconfiguring PM&C server	IN_PROGRESS	38	Add Enclosure	Enc:1601	Enclosure added - starting monitoring	COMPLETE
ID	Task	Target	Status	State													
39	Reconfigure PM&C		Reconfiguring PM&C server	IN_PROGRESS													
38	Add Enclosure	Enc:1601	Enclosure added - starting monitoring	COMPLETE													
<p>24</p> <p><input type="checkbox"/></p>	<p>Update the Enclosures</p>	<p>Navigate to the c7000 enclosure configuration:</p> <p>Main Menu -> Hardware -> System Configuration -> Configure Enclosures</p>  <p>Configure Enclosures Thu Jul 10 20:0</p> <p>Tasks</p> <p>Provisioned Enclosures</p> <p>1601</p> <p><input type="checkbox"/> Pause Updates</p> <p>Add Enclosure Edit Enclosure Delete Enclosure</p>															
<p>25</p> <p><input type="checkbox"/></p>	<p>Choose the enclosure</p>	<p>Select each c7000 enclosure, then press the Edit Enclosure button.</p>															
<p>26</p> <p><input type="checkbox"/></p>	<p>Update the OA addresses</p>	<p>Replace both IPv4 OA addresses with the new IPv6 addresses, and then press the Edit Enclosure button.</p> <p>Edit Enclosure 1601</p> <hr/> <p>Bay 1 OA IP: <input type="text" value="fd0d:deba:d97c:ee3::2"/></p> <p>Bay 2 OA IP: <input type="text" value="fd0d:deba:d97c:ee3::3"/></p> <p style="text-align: right;">Edit Enclosure</p>															

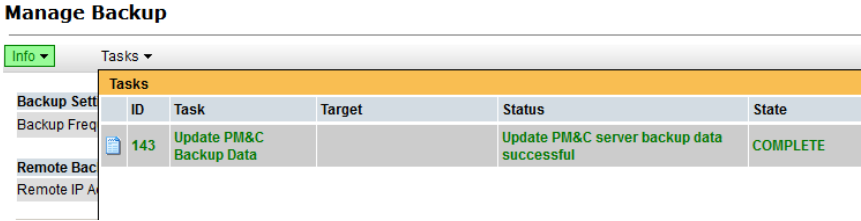
<p>27 <input type="checkbox"/></p>	<p>Wait for the task to complete</p>	<p>A new background task is started to rediscover the enclosure using the IPv6 addresses. You may use the Tasks button to monitor.</p> <p>NOTE: Enclosure discovery takes several minutes.</p> <p>Configure Enclosures .Help Thu Jul 10 20:15:38 2014 UTC</p> <p>Error ▾ Tasks ▾</p> <p><input type="checkbox"/> Pause Up</p> <table border="1"> <thead> <tr> <th colspan="6">Tasks</th> </tr> <tr> <th>ID</th> <th>Task</th> <th>Target</th> <th>Status</th> <th colspan="2">State</th> </tr> </thead> <tbody> <tr> <td>142</td> <td>Add Enclosure</td> <td>Enc:1601</td> <td>Enclosure added - starting monitoring</td> <td colspan="2">COMPLETE</td> </tr> </tbody> </table>	Tasks						ID	Task	Target	Status	State		142	Add Enclosure	Enc:1601	Enclosure added - starting monitoring	COMPLETE	
Tasks																				
ID	Task	Target	Status	State																
142	Add Enclosure	Enc:1601	Enclosure added - starting monitoring	COMPLETE																
<p>28 <input type="checkbox"/></p>	<p>Provision the management server</p>	<p>Navigate to the RMS configuration:</p> <p>Main Menu -> Hardware -> System Configuration -> Configure RMS</p>																		
<p>29 <input type="checkbox"/></p>	<p>Note current settings</p>	<p>RMS iLO addresses cannot be edited. To use IPv6 for PM&C discovery services, the entry must be deleted and then added with the new IPv6 address.</p> <p>The name, cabinet ID and user and password will need to be known. This should be recorded in Section 4.2.2. You may use the Edit RMS button to view this information. The name and Cabinet ID also show in the System Invention navigation.</p>																		
<p>30 <input type="checkbox"/></p>	<p>Delete the management server information</p>	<p>To delete a RMS, select the server, then press the Delete RMS button.</p> <p>Configure RMS</p> <p>Info ▾</p> <table border="1"> <thead> <tr> <th>RMS IP</th> <th>RMS Name</th> </tr> </thead> <tbody> <tr> <td>10.240.72.7</td> <td>rmsU34</td> </tr> </tbody> </table> <p><input type="checkbox"/> Pause Updates</p> <p>Add RMS Edit RMS Delete RMS Find RMS Found RMS</p>	RMS IP	RMS Name	10.240.72.7	rmsU34														
RMS IP	RMS Name																			
10.240.72.7	rmsU34																			

<p>31 <input type="checkbox"/></p>	<p>Provision the management server information</p>	<p>Provision the management server with the new IPv6 address, and the previous data. Press the Add RMS button when complete.</p> <p>NOTE: Alternatively, you may use the find RMS feature.</p> <p>Add RMS</p> 
<p>32 <input type="checkbox"/></p>	<p>Check task</p>	<p>Click on the Info button to verify the action.</p> <p>Configure RMS</p> 

<p>33</p> <p><input type="checkbox"/></p>	<p>Verify discovery</p>	<p>Navigate to the RMS in the System Inventory:</p> <p>Main Menu -> Hardware -> System Inventory -> ...</p> <p>After a few minutes, the RMS Discovery State should show Discovered.</p> <p>RMS rms-u15 with IP fd0d:deba:d97c:ee3::9 Thu Jul 10 21:2</p> <hr/> <p>Hardware Software Firmware Network</p> <p>Hardware Information ↻</p> <table border="1"> <tr> <td>Entity Type</td> <td>Rack Mount Server</td> </tr> <tr> <td>Discovery State</td> <td>Discovered</td> </tr> </table> <p>LED State: OFF Turn On LED</p> <p style="text-align: center;"> Update Firmware Install OS Upgrade Accept Upgrade Reject Upgrade Reset </p>	Entity Type	Rack Mount Server	Discovery State	Discovered
Entity Type	Rack Mount Server					
Discovery State	Discovered					
<p>34</p> <p><input type="checkbox"/></p>	<p>Application RMSses</p>	<p>Application RMSses that are displayed in this view may be updated at this time – but <i>only</i> the iLO interfaces. The OS on Application servers must be migrated with an application specific procedure.</p> <p>If applicable, execute the preceding steps to update Application RMS iLO addresses.</p>				

<p>35</p> <p><input type="checkbox"/></p>	<p>View DNS configuration</p>	<p>Navigate to the DNS Configuration:</p> <p>Main Menu -> Administration -> Remote Servers -> DNS Configuration</p>  
<p>36</p> <p><input type="checkbox"/></p>	<p>Update DNS</p>	<p>If DNS servers are configured, replace the IPv4 addresses with IPv6 addresses for each Name Server, then press the Update DNS Configuration button.</p>
<p>37</p> <p><input type="checkbox"/></p>	<p>View LDAP configuration</p>	<p>Navigate to the LDAP Configuration:</p> <p>Main Menu -> Administration -> Remote Servers -> LDAP Authentication</p>  
<p>38</p> <p><input type="checkbox"/></p>	<p>Update LDAP servers?</p>	<p>If LDAP servers are configured using IPv4 addresses as Hostname, replace the IPv4 addresses with IPv6 addresses or hostnames. For each server, select the row then press the Edit button.</p> <p>If no IPv4 addresses are used, skip to step 41.</p>

<p>39</p> <p><input type="checkbox"/></p>	<p>Update service</p>	<p>Update the Hostname then press the Apply button.</p>  <p>Main Menu: Administration -> Remote Servers -> LDAP Authentication [Edit]</p> <p>Info</p> <p>Unique name for the server. It can be either a valid IPv4 or IPv6 address or a valid hostname. Hostname must be unique and case-insensitive. The length should not exceed 100 characters. Valid hostname characters include alphanumeric</p> <p>Hostname: <input type="text" value="fd0d:deba:d97c:ee3::100"/></p>										
<p>40</p> <p><input type="checkbox"/></p>	<p>Verify service</p>	<p>Verify each updated server. Select the row, then press the Test Server button.</p>  <p>Main Menu: Administration -> Remote Servers -> LDAP Authentication</p> <p>Info</p> <table border="1"> <thead> <tr> <th>Hostname</th> <th>Domain Name</th> <th>Domain Name Short</th> <th>Port</th> <th>Canonical Form</th> </tr> </thead> <tbody> <tr> <td>fd0d:deba:d97c:ee3::100</td> <td>oracle.com</td> <td>ORACLE </td> <td>389</td> <td>Backslash</td> </tr> </tbody> </table> <p>Insert Edit Delete Report Move Up Move Down Test Server</p>	Hostname	Domain Name	Domain Name Short	Port	Canonical Form	fd0d:deba:d97c:ee3::100	oracle.com	ORACLE	389	Backslash
Hostname	Domain Name	Domain Name Short	Port	Canonical Form								
fd0d:deba:d97c:ee3::100	oracle.com	ORACLE	389	Backslash								
<p>41</p> <p><input type="checkbox"/></p>	<p>View backup configuration</p>	<p>Navigate to the Backup Configuration:</p> <p>Main Menu -> Administration -> PM&C Backup -> Manage Backup</p>  <p>Main Menu</p> <ul style="list-style-type: none"> Hardware Software VM Management Storage Administration <ul style="list-style-type: none"> Users Groups GUI Sessions GUI Site Settings PM&C Application PM&C Backup <ul style="list-style-type: none"> Manage Backup <p>Manage Backup</p> <p>Info Tasks</p> <p>Backup Settings</p> <p>Backup Frequency: Daily Backup Time: 05:00</p> <p>Remote Backup Settings</p> <p>Remote IP Address: 10.240.72.40</p> <p>Update Settings</p>										
<p>42</p> <p><input type="checkbox"/></p>	<p>Update backup configuration</p>	<p>If a remote Backup server is configured, replace the Remote IP Address with an IPv6 address, then press the Update Settings button.</p>										

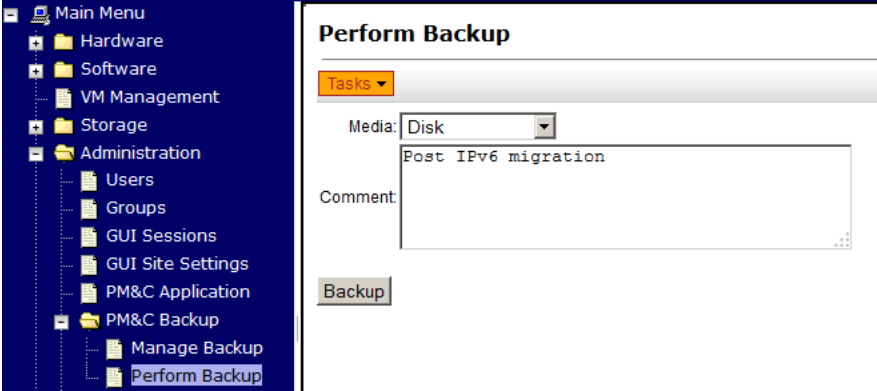
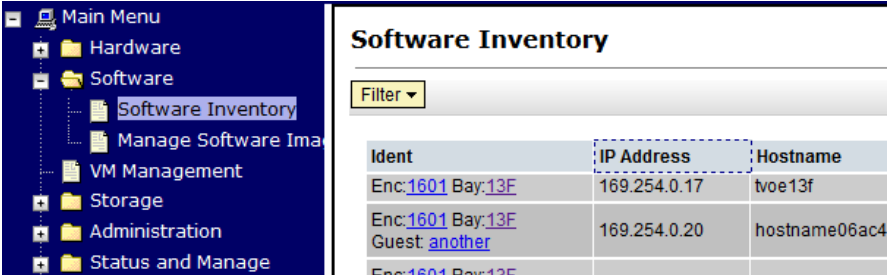
43 <input type="checkbox"/>	Verify backup configuration	<p>Click on the Tasks button to verify the update.</p> 
44 <input type="checkbox"/>	Re login to verify	<p>Logout of the PM&C GUI and re-login with the IPv6 address to verify https://[<PM&C_IPv6_Address>]</p>
45 <input type="checkbox"/>	Continue	<p>You may leave this open for reuse later, and continue to the next procedure.</p>
---End of Procedure---		

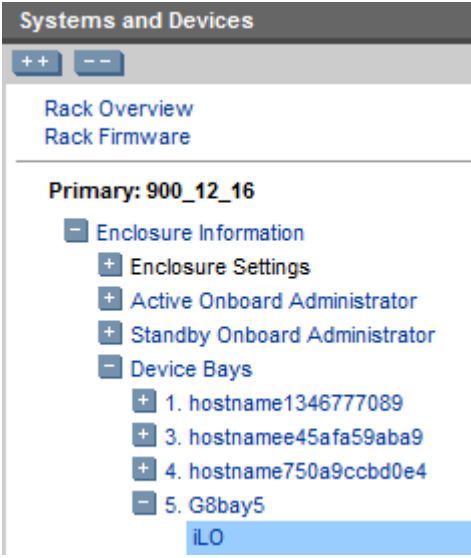
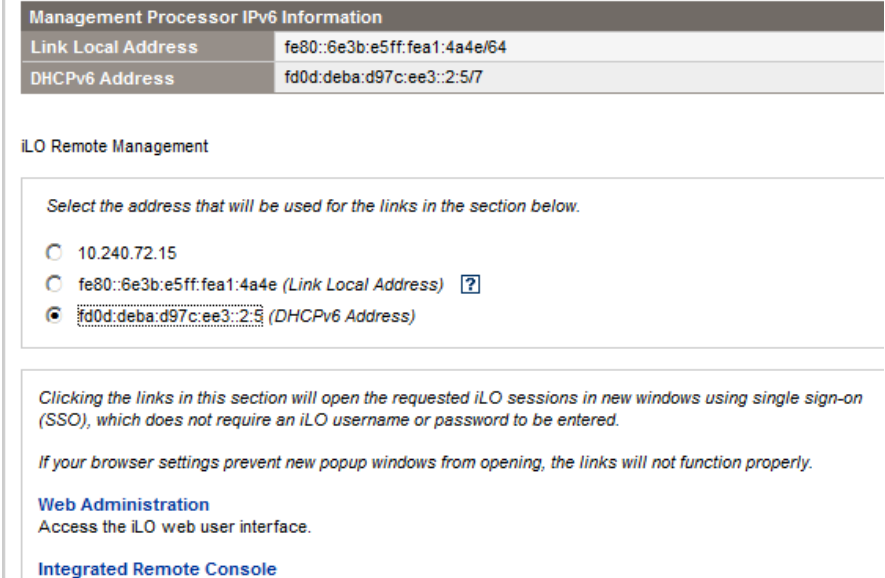
5.5 Migration Completion

Procedure 5 Finish Migration

S T E P	Use this procedure to complete the migration procedure. Estimated time of completion: 20 minutes <i>Check off (✓) each step as it is completed. Shaded steps indicate: gray = input, white = output, black = Go-No-Go.</i>	
	Task	Description
1 <input type="checkbox"/>	Health check	Execute the health check procedure in Procedure 15.
2 <input type="checkbox"/>	Update netConfig repository	All devices identified in Procedure 1 Step 10 must replace the IPv4 management address with the new IPv6 addresses in the netConfig repository. Devices shown in the following command should have IPv6 address listed in Section 4.3.2 \$ netConfig --repo listDevices grep Device: Run the following command for each device: \$ sudo netConfig --repo editDevice name=<name>

<p>3 <input type="checkbox"/></p>	<p>Update addresses</p>	<p>In the example interactive session below, press enter for any data that does not need to be changed, but enter new IPv6 addresses with appropriate. The prompting is device specific, and subject to change:</p> <pre> Access network address [10.240.72.27]: fd0d:deba::1:1/64 Firmware service [pmaCSCP]: Firmware filename [Z_14_37.swi]: Initialization Management Options What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management? [10.240.72.27/24]: fd0d:deba::1:1/64 Live Network Credentials Platform access username [tklc]: Platform user password [***...]: Device privileged mode password [***...]: Device named en9001216bay1R successfully edited. </pre>
<p>4 <input type="checkbox"/></p>	<p>List netConfig services</p>	<p>Services with IPv4 management addresses must be replaced with the new IPv6 addresses in the netConfig repository. Display the services with:</p> <pre> \$ sudo netConfig --repo listServices grep "Service Name:" </pre>
<p>5 <input type="checkbox"/></p>	<p>Update netConfig repository</p>	<p>Run the following command for each service:</p> <pre> \$ sudo netConfig --repo editService name=<name> </pre> <p>Note: this is changing the services used by netConfig; it does not remove the actual service.</p>
<p>6 <input type="checkbox"/></p>	<p>Update addresses</p>	<p>In the example interactive session below, press enter for any data that does not need to be changed, but enter new IPv6 addresses with appropriate:</p> <pre> Note: Edit may only modify existing options. To add or delete options, delete the service. Service Host? [10.240.72.40]: fd0d:deba::1/64 Enter a new password [***...]: Enter the value for user [pmaCuser]: Service named pmaCSCP successfully edited. </pre>
<p>7 <input type="checkbox"/></p>	<p>Sanity test</p>	<p>As a final netConfig validation, run the validate command to login to each device in the repository.</p> <pre> \$ sudo netConfig --repo validate </pre>
<p>8 <input type="checkbox"/></p>	<p>Backup network</p>	<p>Perform a backup of <i>all</i> aggregation and enclosure switches recorded in Procedure 1 step 10 using the service name found in step 5. The filename option should specify a unique name for each of the backups:</p> <pre> \$ sudo netConfig --device=<name> backupConfiguration service=<service> filename=<device>-postmigrate </pre>

<p>9 <input type="checkbox"/></p>	<p>Save backups</p>	<p>Move netConfig backup files to the backup directory to preserve files with PM&C backups. Replace <user> with the userid noted in Procedure 1 Step 4:</p> <pre>\$ sudo mv ~<user>/*migrate* /usr/TKLC/smac/etc/switch/backup</pre> <p>Note: If the backup directory does not exist, create it with:</p> <pre>\$ sudo mkdir /usr/TKLC/smac/etc/switch/backup</pre>												
<p>10 <input type="checkbox"/></p>	<p>Backup the PM&C</p>	<p>In the PM&C GUI, navigate to the Backup:</p> <p>Main Menu -> Administration -> PM&C Backup -> Perform Backup</p> <p>Select the appropriate Media for the site, enter a Comment, and then press the Backup button.</p> 												
<p>11 <input type="checkbox"/></p>	<p>Verify PM&C discovery</p>	<p>In the PM&C GUI, navigate to the Software Inventory, and verify c7000 and RMS systems are discovered. The IP Addresses will show the control network IPv4 address by default.</p> <p>Main Menu -> Software -> Software Inventory</p>  <table border="1"> <thead> <tr> <th>Ident</th> <th>IP Address</th> <th>Hostname</th> </tr> </thead> <tbody> <tr> <td>Enc:1601 Bay:13F</td> <td>169.254.0.17</td> <td>tw0e13f</td> </tr> <tr> <td>Enc:1601 Bay:13F Guest: another</td> <td>169.254.0.20</td> <td>hostname06ac4</td> </tr> <tr> <td>Enc:1601 Bay:13F</td> <td></td> <td></td> </tr> </tbody> </table>	Ident	IP Address	Hostname	Enc:1601 Bay:13F	169.254.0.17	tw0e13f	Enc:1601 Bay:13F Guest: another	169.254.0.20	hostname06ac4	Enc:1601 Bay:13F		
Ident	IP Address	Hostname												
Enc:1601 Bay:13F	169.254.0.17	tw0e13f												
Enc:1601 Bay:13F Guest: another	169.254.0.20	hostname06ac4												
Enc:1601 Bay:13F														

<p>12</p> <p><input type="checkbox"/></p>	<p>Verify c7000 remote management</p>	<p>Test iLO access for a sample of c7000 blades using IPv6. At least one per c7000 enclosure. Login to the OA GUI and navigate to</p> <p>Enclosure Info -> Device Bays -> [bay] -> iLO</p>  <p>The screenshot shows the 'Systems and Devices' section of the OA GUI. It includes a 'Rack Overview' and 'Rack Firmware' section. Under 'Primary: 900_12_16', there is a tree view with 'Enclosure Information' expanded to show 'Enclosure Settings', 'Active Onboard Administrator', and 'Standby Onboard Administrator'. 'Device Bays' is also expanded, listing five bays: '1. hostname1346777089', '3. hostnameee45afa59aba9', '4. hostname750a9ccbd0e4', and '5. G8bay5'. The 'iLO' link under bay 5 is highlighted in blue.</p>
<p>13</p> <p><input type="checkbox"/></p>	<p>Open iLO session</p>	<p>Select the global IPv6 address from the iLO Remote Management radio button then click on a link to open the iLO session. Once the console window displays, it may be closed; the test passed. Logout of the OA GUI when complete.</p>  <p>The screenshot shows the 'Management Processor IPv6 Information' table with 'Link Local Address' as fe80::6e3b:e5ff:fea1:4a4e/64 and 'DHCPv6 Address' as fd0d:deba:d97c:ee3::2:5/7. Below is the 'iLO Remote Management' section with radio buttons for '10.240.72.15', 'fe80::6e3b:e5ff:fea1:4a4e (Link Local Address)', and 'fd0d:deba:d97c:ee3::2:5 (DHCPv6 Address)'. The DHCPv6 address is selected. A note states: 'Clicking the links in this section will open the requested iLO sessions in new windows using single sign-on (SSO), which does not require an iLO username or password to be entered. If your browser settings prevent new popup windows from opening, the links will not function properly.' There are links for 'Web Administration' and 'Integrated Remote Console'.</p>

14 <input type="checkbox"/>	netBackup?	If netBackup is used, verify netBackup is using IPv6 for the backup. Since this is a customer provided service, this must be performed by the customer.
---End of Procedure---		

6 Harvest IPv4

To contact Oracle Support by phone, refer to the [Oracle Support Contacts Global Directory](#).

Before beginning the address harvesting, users must perform a system health check. Refer to section 8. This check only ensures that the system does not have any know issues. Performing the system health check determines alarms present in the system, however the procedure may proceed with alarms raised; Contact Oracle support.

**** WARNING ****

Some of the procedural steps must be executed on multiple devices. In particular, the network configuration typically must be performed on pairs of switches, or over a variable number of enclosures.

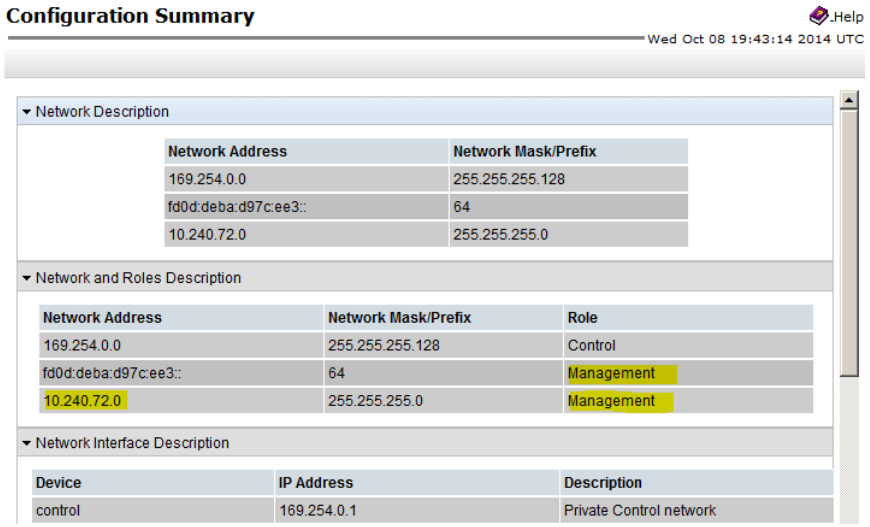
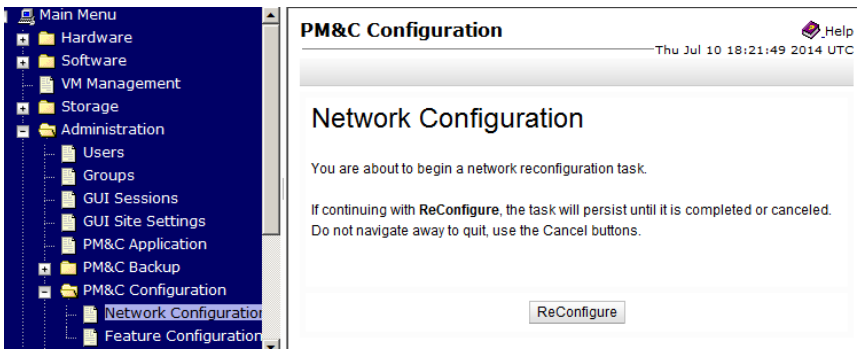
6.1 Harvest PM&C addresses

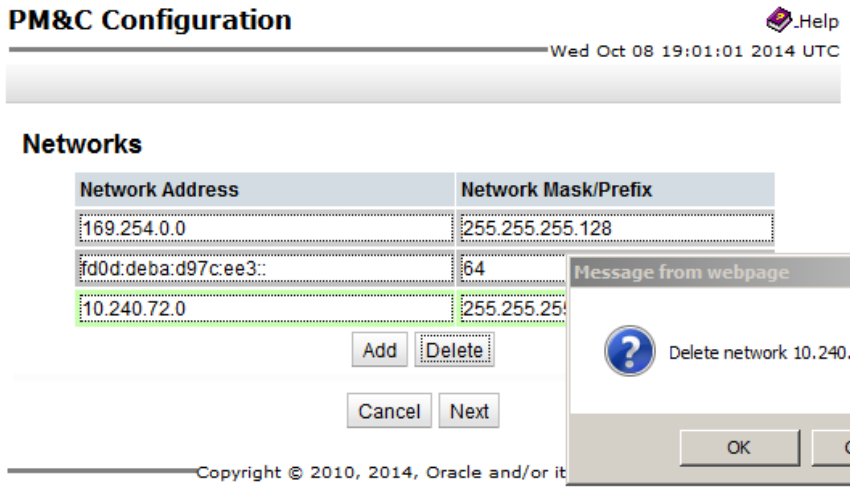
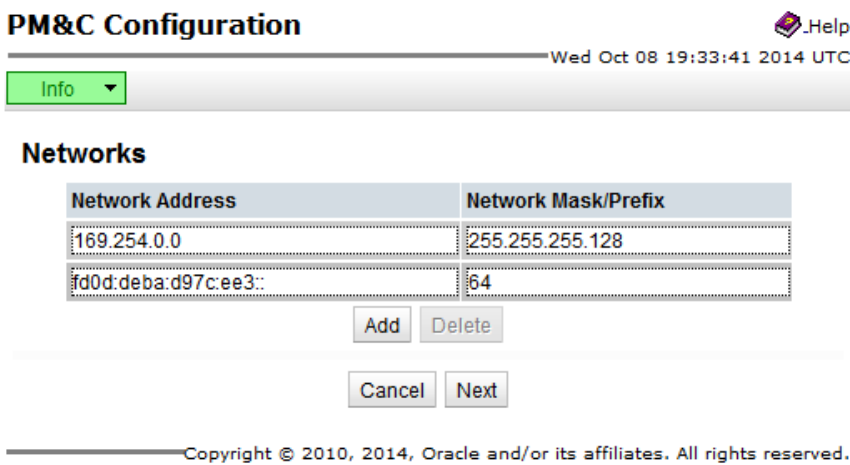
**** WARNING ****

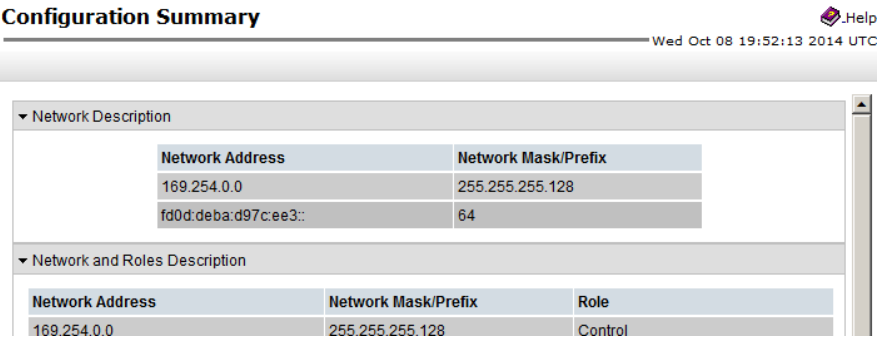
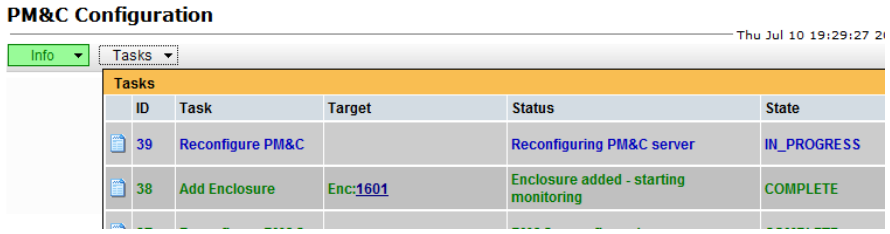
The PM&C application reconfiguration is presented as a wizard. There is no “back” button, and you should not use the browser’s back button; cancel and restart if you make an error. If you navigate away from the wizard, the process is left in progress. Returning to the wizard will ask you to finish or cancel the in-progress task. The safe response is to cancel and restart the reconfiguration. Use the **cancel** button to quit the wizard.

Procedure 6 Harvest PM&C IPv4 addresses

S T E P	Use this procedure to reconfigure PM&C to remove unused IPv4 addresses. Procedure 4 is a prerequisite. Estimated time of completion: 15 minutes <i>Check off (✓) each step as it is completed. Shaded steps indicate: gray = input, white = output, black = Go-No-Go.</i>	
	Task	Description
1 <input type="checkbox"/>	PM&C: Login to GUI	Login to the PM&C from a supported browser https://[<PM&C_IPv6_address>]

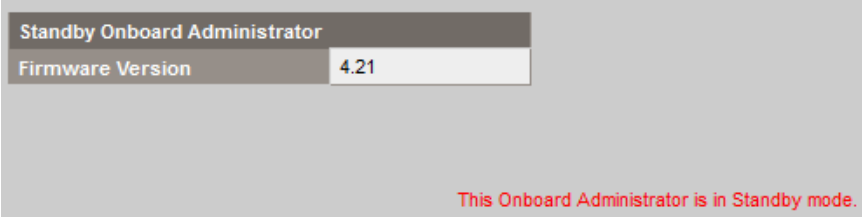
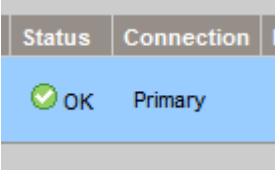
<p>2</p> <p><input type="checkbox"/></p>	<p>Identify IPv4 networks in the current configuration to delete</p>	<p>Navigate to the current configuration and identify all IPv4 networks are that <i>not</i> associated with the “control” role. All IPv4 addresses except for the PM&C control network may be harvested.</p> <p>Main Menu -> Admin -> PM&C Configuration</p>  <p>Configuration Summary .Help</p> <p style="text-align: right;">Wed Oct 08 19:43:14 2014 UTC</p> <p>▼ Network Description</p> <table border="1"> <thead> <tr> <th>Network Address</th> <th>Network Mask/Prefix</th> </tr> </thead> <tbody> <tr> <td>169.254.0.0</td> <td>255.255.255.128</td> </tr> <tr> <td>fd0d:deba:d97c:ee3::</td> <td>64</td> </tr> <tr> <td>10.240.72.0</td> <td>255.255.255.0</td> </tr> </tbody> </table> <p>▼ Network and Roles Description</p> <table border="1"> <thead> <tr> <th>Network Address</th> <th>Network Mask/Prefix</th> <th>Role</th> </tr> </thead> <tbody> <tr> <td>169.254.0.0</td> <td>255.255.255.128</td> <td>Control</td> </tr> <tr> <td>fd0d:deba:d97c:ee3::</td> <td>64</td> <td>Management</td> </tr> <tr> <td>10.240.72.0</td> <td>255.255.255.0</td> <td>Management</td> </tr> </tbody> </table> <p>▼ Network Interface Description</p> <table border="1"> <thead> <tr> <th>Device</th> <th>IP Address</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>control</td> <td>169.254.0.1</td> <td>Private Control network</td> </tr> </tbody> </table>	Network Address	Network Mask/Prefix	169.254.0.0	255.255.255.128	fd0d:deba:d97c:ee3::	64	10.240.72.0	255.255.255.0	Network Address	Network Mask/Prefix	Role	169.254.0.0	255.255.255.128	Control	fd0d:deba:d97c:ee3::	64	Management	10.240.72.0	255.255.255.0	Management	Device	IP Address	Description	control	169.254.0.1	Private Control network
Network Address	Network Mask/Prefix																											
169.254.0.0	255.255.255.128																											
fd0d:deba:d97c:ee3::	64																											
10.240.72.0	255.255.255.0																											
Network Address	Network Mask/Prefix	Role																										
169.254.0.0	255.255.255.128	Control																										
fd0d:deba:d97c:ee3::	64	Management																										
10.240.72.0	255.255.255.0	Management																										
Device	IP Address	Description																										
control	169.254.0.1	Private Control network																										
<p>3</p> <p><input type="checkbox"/></p>	<p>Start reconfiguration</p>	<p>Navigate to:</p> <p>Main Menu -> Admin -> PM&C Configuration -> Network Configuration</p> <p>Then press the ReConfigure button.</p>  <p>Main Menu</p> <ul style="list-style-type: none"> Hardware Software VM Management Storage Administration <ul style="list-style-type: none"> Users Groups GUI Sessions GUI Site Settings PM&C Application PM&C Backup PM&C Configuration <ul style="list-style-type: none"> Network Configuration Feature Configuration <p>PM&C Configuration .Help</p> <p style="text-align: right;">Thu Jul 10 18:21:49 2014 UTC</p> <p>Network Configuration</p> <p>You are about to begin a network reconfiguration task.</p> <p>If continuing with ReConfigure, the task will persist until it is completed or canceled. Do not navigate away to quit, use the Cancel buttons.</p> <p style="text-align: center;"><input type="button" value="ReConfigure"/></p>																										

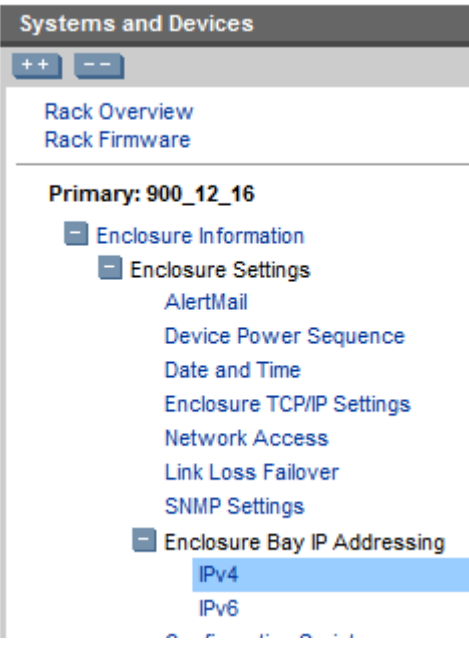
<p>4</p> <p><input type="checkbox"/></p>	<p>Delete IPv4 networks</p>	<p>For each IPv4 networks identified in step 2, select the network then press the delete button.</p> <p>A pop-up window to confirm will display; Click OK to continue.</p> 
<p>5</p> <p><input type="checkbox"/></p>	<p>Verify</p>	<p>Verify the information and press the Next button.</p> 
<p>6</p> <p><input type="checkbox"/></p>	<p>Continue with wizard</p>	<p>Continue to press Next through the Network Roles, Network Interfaces, Routes, and DHCP IPv4 Ranges windows; the IPv4 addresses for the deleted network(s) should be removed already, leaving just the control network IPv4 addresses.</p>

<p>7</p> <p><input type="checkbox"/></p>	<p>Verify IPv4 networks are removed</p>	<p>Verify the new configuration, then press the Finish button:</p>  <p>Configuration Summary .Help Wed Oct 08 19:52:13 2014 UTC</p> <p>▼ Network Description</p> <table border="1"> <thead> <tr> <th>Network Address</th> <th>Network Mask/Prefix</th> </tr> </thead> <tbody> <tr> <td>169.254.0.0</td> <td>255.255.255.128</td> </tr> <tr> <td>fd0d:deba:d97c:ee3::</td> <td>64</td> </tr> </tbody> </table> <p>▼ Network and Roles Description</p> <table border="1"> <thead> <tr> <th>Network Address</th> <th>Network Mask/Prefix</th> <th>Role</th> </tr> </thead> <tbody> <tr> <td>169.254.0.0</td> <td>255.255.255.128</td> <td>Control</td> </tr> </tbody> </table>	Network Address	Network Mask/Prefix	169.254.0.0	255.255.255.128	fd0d:deba:d97c:ee3::	64	Network Address	Network Mask/Prefix	Role	169.254.0.0	255.255.255.128	Control			
Network Address	Network Mask/Prefix																
169.254.0.0	255.255.255.128																
fd0d:deba:d97c:ee3::	64																
Network Address	Network Mask/Prefix	Role															
169.254.0.0	255.255.255.128	Control															
<p>8</p> <p><input type="checkbox"/></p>	<p>Wait for the task to complete</p>	<p>The reconfiguration background task is started. The example below is displayed by pressing the Tasks button. It should show as COMPLETE within a few minutes.</p>  <p>PM&C Configuration Thu Jul 10 19:29:27 21</p> <p>Info Tasks</p> <table border="1"> <thead> <tr> <th>ID</th> <th>Task</th> <th>Target</th> <th>Status</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>39</td> <td>Reconfigure PM&C</td> <td></td> <td>Reconfiguring PM&C server</td> <td>IN_PROGRESS</td> </tr> <tr> <td>38</td> <td>Add Enclosure</td> <td>Enc:1601</td> <td>Enclosure added - starting monitoring</td> <td>COMPLETE</td> </tr> </tbody> </table>	ID	Task	Target	Status	State	39	Reconfigure PM&C		Reconfiguring PM&C server	IN_PROGRESS	38	Add Enclosure	Enc:1601	Enclosure added - starting monitoring	COMPLETE
ID	Task	Target	Status	State													
39	Reconfigure PM&C		Reconfiguring PM&C server	IN_PROGRESS													
38	Add Enclosure	Enc:1601	Enclosure added - starting monitoring	COMPLETE													
<p>9</p> <p><input type="checkbox"/></p>	<p>Backup PM&C configuration</p>	<p>In the PM&C GUI, navigate to the Backup:</p> <p>Main Menu -> Administration -> PM&C Backup -> Perform Backup</p> <p>Select the appropriate Media for the site, enter a Comment that includes a phrase similar to “IPv4 harvested”, and then press the Backup button.</p> <p style="text-align: center;">---End of Procedure---</p>															


6.2 Harvest Enclosure addresses

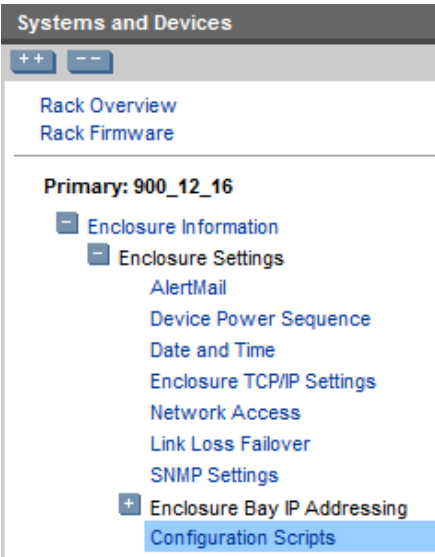
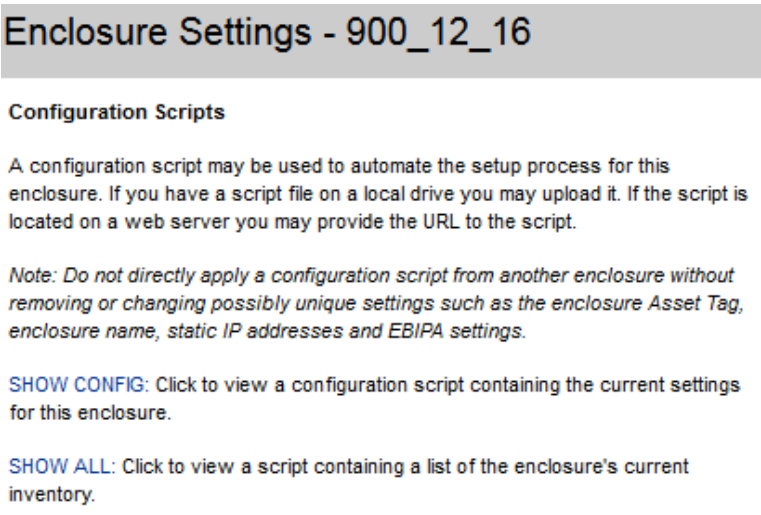
Procedure 7 Harvest Enclosure IPv4 addresses

S T E P	Use this procedure to reconfigure OA to remove IPv4 addresses. Procedure 3 is a prerequisite. Estimated time of completion: 20 minutes <i>Check off (✓) each step as it is completed. Shaded steps indicate: gray = input, white = output, black = Go-No-Go.</i>	
	Task	Description
1 <input type="checkbox"/>	Identify all e7000 enclosures	Each enclosure must be individually configured. The following steps are repeated for each enclosure from Section 4.2.3
2 <input type="checkbox"/>	OA: Login to GUI	Login to the active OA. https://[<OA_IPv6_Address>] If the OA is in Standby mode, login with the secondary IPv6 address:  Also ensure the system Status is OK. 

<p>3 <input type="checkbox"/></p>	<p>Configure bay addressing</p>	<p>Navigate to the EBIPA IPv4 settings and select the Device Bays tab:</p>  <p>The screenshot shows a web interface titled "Systems and Devices" with expand/collapse buttons. Under "Rack Overview" and "Rack Firmware", there is a section for "Primary: 900_12_16". A tree view shows "Enclosure Information" expanded, with "Enclosure Settings" expanded. Under "Enclosure Settings", "Enclosure Bay IP Addressing" is expanded, and "IPv4" is selected and highlighted in blue.</p>
--	---------------------------------	--

<p>4</p> <p><input type="checkbox"/></p>	<p>Delete IPv4 EBIPA addresses</p>	<p>On the table header, uncheck the Enabled box. This will uncheck all Enabled boxes in the table. Unless directed by application procedures, delete the IPv4 addresses. Then press the Apply button. Next, respond to the pop-up warning by pressing OK.</p> <p>Enclosure Bay IP Addressing</p> <p>Device Bays Device Bays Double Dense Side A Device Bays Double Dense Side B</p> <p>Device Bay iLO Processor Address Range: The form below provides fixed IP address assignment address in</p> <p>Note: All settings will be lost if you change any settings. Existing IP addresses will be deleted.</p> <p>Device List: The table below shows the current IP address settings for each device. You can click the "arrow" button to copy the IP address to the clipboard.</p> <div data-bbox="690 619 1445 877"> </div> <table border="1"> <thead> <tr> <th>Bay</th> <th><input type="checkbox"/> Enabled</th> <th>EBIPA Address</th> <th>Subnet Mask</th> <th>Gateway</th> <th>Domain</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="checkbox"/></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>2</td> <td><input type="checkbox"/></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Bay	<input type="checkbox"/> Enabled	EBIPA Address	Subnet Mask	Gateway	Domain	1	<input type="checkbox"/>					2	<input type="checkbox"/>				
Bay	<input type="checkbox"/> Enabled	EBIPA Address	Subnet Mask	Gateway	Domain															
1	<input type="checkbox"/>																			
2	<input type="checkbox"/>																			
<p>5</p> <p><input type="checkbox"/></p>	<p>Delete IPv4 EBIPA addresses</p>	<p>Select the Interconnect Bays tab and perform the action in the previous step for the network devices.</p>																		
<p>6</p> <p><input type="checkbox"/></p>	<p>Configure OA addressing</p>	<p>Navigate to the Enclosure IP Settings and select the IPv4 Settings tab:</p> <div data-bbox="581 1329 1024 1776"> </div>																		

<p>7</p> <p><input type="checkbox"/></p>	<p>Delete OA addresses</p>	<p>Click on DHCP radio button, then click Apply:</p> <p>TCP/IP Settings - IPv4 Settings</p> <p>Enclosure IP Mode: <i>The Enclosure IP Mode is a static IP address that always points to the Active Onboard Administrator.</i></p> <div data-bbox="706 472 1396 724" style="border: 1px solid gray; padding: 5px;"> <p>Message from webpage</p> <p> Warning: changing your network settings could disconnect you from the Onboard Administrator. If you are disconnected you must close your browser and sign in again.</p> <p>OK Cancel</p> </div> <p>Note: Changing the Onboard Administrator's DNS Name could cause a hostname mismatch on the SSL certificate. Update the certificate information on any Onboard Administrator whose DNS Name is changed.</p> <p>Active Onboard Administrator Network Settings Standby Onboard Administrator Network Settings</p> <div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid gray; padding: 5px;"> <p><input checked="" type="radio"/> DHCP</p> <p><input type="checkbox"/> Enable Dynamic DNS</p> </div> <div style="border: 1px solid gray; padding: 5px;"> <p><input checked="" type="radio"/> DHCP</p> <p><input type="checkbox"/> Enable Dynamic DNS</p> </div> </div>
<p>8</p> <p><input type="checkbox"/></p>	<p>Verify</p>	<p>After a few minutes, the old static IPv4 address will be replaced with the IPv4 unspecified address "0.0.0.0".</p> <p>TCP/IP Settings</p> <p>Information: <i>The Onboard Administrator's current TCP/IP settings.</i></p> <p>IPv4 Information</p> <div style="border: 1px solid gray; padding: 5px;"> <p>IP Address: 0.0.0.0 (DHCP)</p> <p>Dynamic DNS: Disabled</p> <p>Subnet Mask:</p> <p>Gateway:</p> </div> <p>IPv6 Information</p> <div style="border: 1px solid gray; padding: 5px;"> <p>IPv6: Enabled</p> <p>IPv6 Link Local Address: fe80::7ae7:d1ff:fe57:5a45/64</p> <p>IPv6 Static Address 1: fd0d:deba:d97c:ee3::2/64</p> </div>

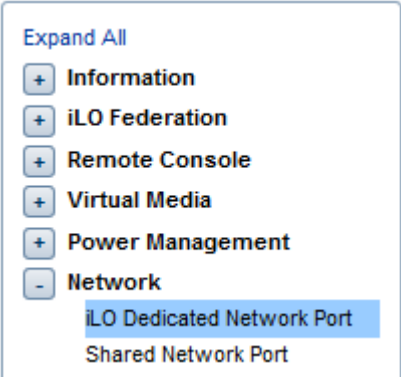
<p>9</p> <input type="checkbox"/>	<p>Backup OA configuration</p>	<p>Navigate to the Configuration Scripts:</p> <p>Enclosure Information -> Enclosure Settings -> Configuration Scripts</p> 
<p>10</p> <input type="checkbox"/>	<p>Display the configuration</p>	<p>View the configuration script. Click on the SHOW CONFIG link. This will open a new tab or window.</p> 
<p>11</p> <input type="checkbox"/>	<p>Save the script</p>	<p>Save the text in the window to a file, as applicable for the browser (e.g. <code>File->Save</code> or <code><control>-s</code>). A copy should also be placed on the PM&C server using <code>scp</code> in the following directory:</p> <p><code>/var/TKLC/smac/backup</code></p>

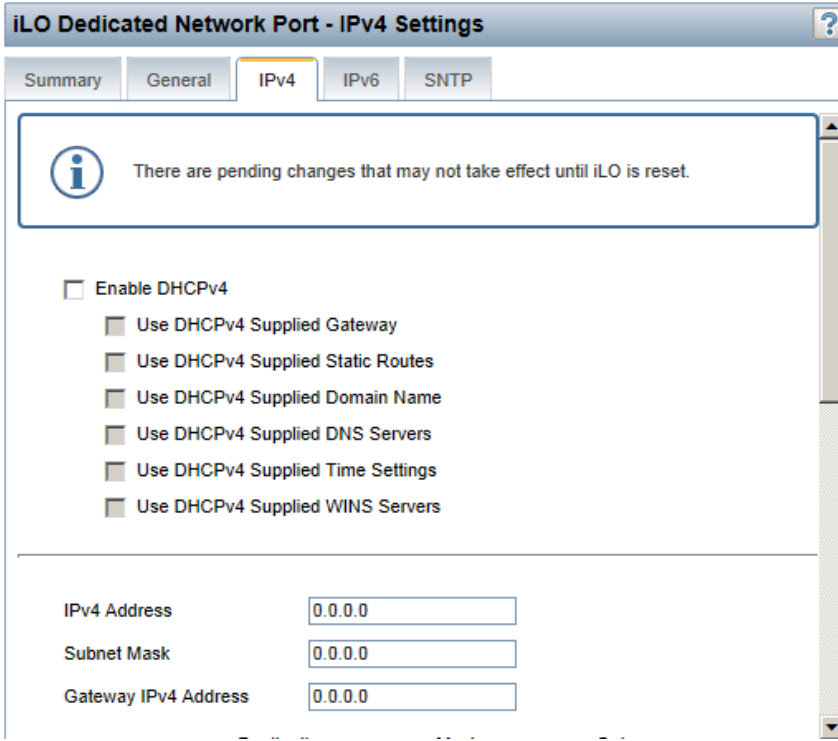
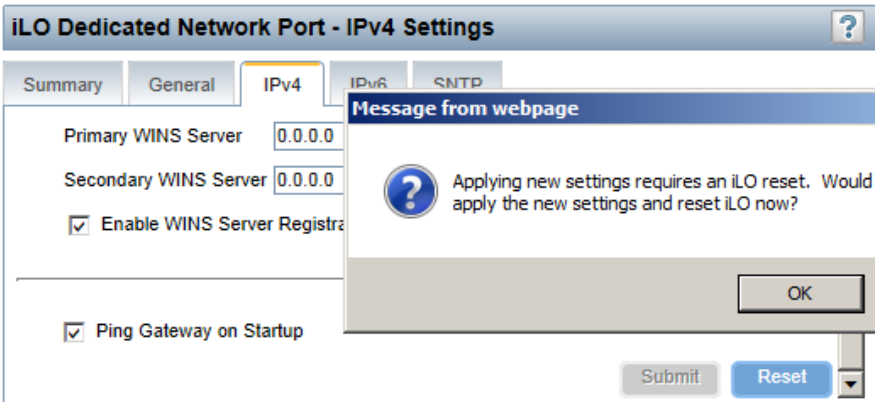
12 <input type="checkbox"/>	Logout	Press the Sign Out button when complete.
---End of Procedure---		

6.3 Harvest Management Server addresses

This section must be performed on the management server that hosts the PM&C guest. This procedure may be reused for Application RMS servers. Since the iLO management is not directly used by, or impacted by, applications, this task may be done with this platform procedure. Only the iLO interface is updated; Application TVOE host addresses should be configured with the application migration.

Procedure 8 Harvest iLO IPv4 addresses

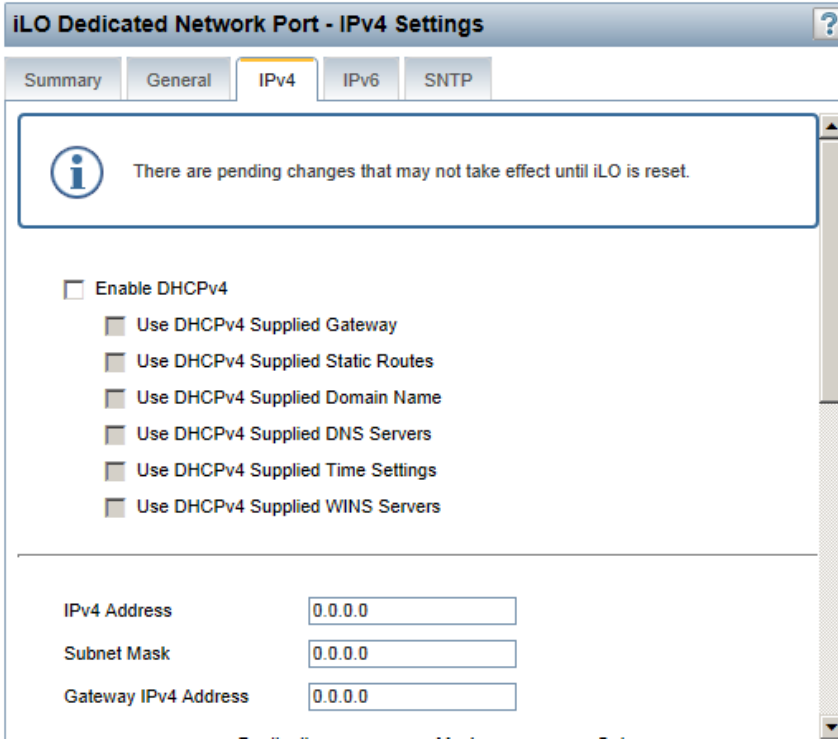
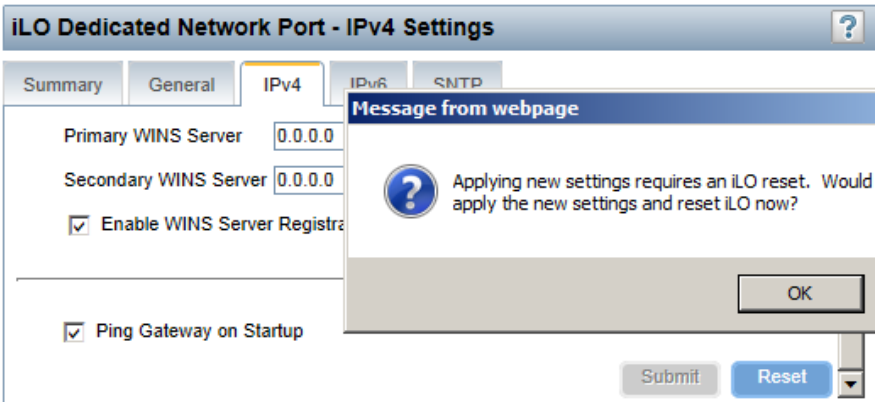
S T E P	Use this procedure to reconfigure the iLO on the management server to remove unused IPv4 addresses. Procedure 2 is a prerequisite. Estimated time of completion: 20 minutes <i>Check off (✓) each step as it is completed. Shaded steps indicate: gray = input, white = output, black = Go-No-Go.</i>	
	Task	Description
1 <input type="checkbox"/>	Management Server iLO: Login	Login to the iLO on the management server https://[<iLO_IPv6_address>]
2 <input type="checkbox"/>	View current configuration	Navigate to the network configuration: Network -> iLO Dedicated Network Port 

<p>3</p> <p><input type="checkbox"/></p>	<p>Delete IPv4 addresses</p>	<p>Select the IPv4 tab and update the IPv4 Address, Mask and Gateway is use 0.0.0.0.</p> <p>Scroll down and press the Submit button. The pending changes notice shown below will be displayed.</p>  <p>The screenshot shows the 'iLO Dedicated Network Port - IPv4 Settings' page with the 'IPv4' tab selected. A message box at the top states: 'There are pending changes that may not take effect until iLO is reset.' Below this, there are several unchecked checkboxes for DHCPv4 settings. At the bottom, the IPv4 Address, Subnet Mask, and Gateway IPv4 Address fields are all set to 0.0.0.0.</p>
<p>4</p> <p><input type="checkbox"/></p>	<p>Reset the iLO</p>	<p>Press the Reset button that is enabled after the settings from the previous step are verified. A pop-up will ask to authorize a reset, press OK.</p>  <p>The screenshot shows the same 'iLO Dedicated Network Port - IPv4 Settings' page. A 'Message from webpage' pop-up is displayed over the settings, asking: 'Applying new settings requires an iLO reset. Would you apply the new settings and reset iLO now?' with an 'OK' button. The 'Submit' button is disabled, and the 'Reset' button is enabled.</p>

5 <input type="checkbox"/>	Verify	Wait 30 seconds for the iLO to reset, then login to verify. https://[<iLO_IPv6_Address>] Press the Sign out button when complete.
6 <input type="checkbox"/>	Application RMSs	If Application RMS servers exist, the iLOs may be updated. Unless directed otherwise, the preceding steps may be used to remove IPv4 addresses on application RMS iLOs.
---End of Procedure---		

Procedure 9 Harvest Management Server IPv4 addresses

S T E P	Use this procedure to reconfigure the TVOE management server host to remove unused IPv4 addresses. Procedure 2 is a prerequisite. Estimated time of completion: 20 minutes <i>Check off (✓) each step as it is completed. Shaded steps indicate: gray = input, white = output, black = Go-No-Go.</i>	
	Task	Description
	1 <input type="checkbox"/>	Management Server iLO: Login
2 <input type="checkbox"/>	View current configuration	Navigate to the network configuration: Network -> iLO Dedicated Network Port <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> Expand All + Information + iLO Federation + Remote Console + Virtual Media + Power Management - Network iLO Dedicated Network Port Shared Network Port </div>

<p>3</p> <p><input type="checkbox"/></p>	<p>Delete IPv4 addresses</p>	<p>Select the IPv4 tab and update the IPv4 Address, Mask and Gateway is use 0.0.0.0.</p> <p>Scroll down and press the Submit button. The pending changes notice shown below will be displayed.</p>  <p>The screenshot shows the 'iLO Dedicated Network Port - IPv4 Settings' page with the 'IPv4' tab selected. A message box states: 'There are pending changes that may not take effect until iLO is reset.' Below this, there are several unchecked checkboxes for DHCPv4 settings: 'Enable DHCPv4', 'Use DHCPv4 Supplied Gateway', 'Use DHCPv4 Supplied Static Routes', 'Use DHCPv4 Supplied Domain Name', 'Use DHCPv4 Supplied DNS Servers', 'Use DHCPv4 Supplied Time Settings', and 'Use DHCPv4 Supplied WINS Servers'. At the bottom, the IPv4 Address, Subnet Mask, and Gateway IPv4 Address fields are all set to 0.0.0.0.</p>
<p>4</p> <p><input type="checkbox"/></p>	<p>Reset the iLO</p>	<p>Press the Reset button that is enabled after the settings from the previous step are verified. A pop-up will ask to authorize a reset, press OK.</p>  <p>The screenshot shows the same 'iLO Dedicated Network Port - IPv4 Settings' page. A 'Message from webpage' pop-up is displayed, asking: 'Applying new settings requires an iLO reset. Would you apply the new settings and reset iLO now?' with an 'OK' button. In the background, the 'Primary WINS Server' and 'Secondary WINS Server' fields are set to 0.0.0.0, and the 'Enable WINS Server Registration' checkbox is checked. At the bottom, the 'Ping Gateway on Startup' checkbox is also checked, and the 'Reset' button is highlighted in blue.</p>

5 <input type="checkbox"/>	Verify	<p>Wait 30 seconds for the iLO to reset, then login to verify.</p> <p>https://[<iLO_IPv6_Address>]</p> <p>Press the Sign out button when complete.</p>
6 <input type="checkbox"/>	Application RMSs	<p>If Application RMS servers exist, the iLOs may be updated. Unless directed otherwise, the preceding steps may be used to remove IPv4 addresses on application RMS iLOs.</p>
7 <input type="checkbox"/>	Management server: Login	<p>Login to the TVOE host on the management server</p> <p>\$ ssh admusr@<TVOE_IPv6_Address></p>
8 <input type="checkbox"/>	Determine devices	<p>Display the bridges. The management and optional netBackup bridges should be updated. Application bridges may be updated using these steps only when directed by application procedures.</p> <p>\$ sudo netAdm show --type=Bridge</p>
9 <input type="checkbox"/>	Determine IPv4 routing	<p>Display the routes for each non-control bridge, noting the NETWORK or HOST and GATEWAY values to use in the next step. There may be multiple routes per device.</p> <p>\$ sudo netAdm query --route --device=<bridge></p>
10 <input type="checkbox"/>	Delete IPv4 routes	<p>For each IPv4 route, delete the route using the type of “default”, “network”, or “host”, and the gateway noted in the previous step.</p> <p>\$ sudo netAdm delete --route=<type> --device=<bridge> --gateway=<IPv4_Address></p>
11 <input type="checkbox"/>	Determine IPv4 addresses	<p>Display the IP addressing for each non-control bridge, noting the IP Address and Netmask to use in the next step.</p> <p>\$ sudo netAdm query --type=Bridge --name=<bridge></p>
12 <input type="checkbox"/>	Delete IPv4 addresses	<p>Remove the IPv4 address of the Management Server on the management bridge and the optional netBackup bridge if it exists.</p> <p>\$ sudo netAdm set --type=Bridge --name=<bridge> --address=<ipv4_address> --netmask=<ipv4_mask> --deleteAddr</p>
13 <input type="checkbox"/>	Backup the TVOE	<p>Backup the TVOE configuration from platcfg using appropriate media.</p> <p>\$ sudo su - platcfg</p>
14 <input type="checkbox"/>	Logout	<p>\$ exit</p>
---End of Procedure---		

6.4 Harvest Switch addresses

This procedure will remove IPv4 addresses on the Aggregation and Enclosure switches, using the netConfig utility.

Procedure 10 Harvest Network IPv4 addresses

S T E P	Use this procedure to reconfigure network switches to remove IPv4 addresses. Procedure 1 is a prerequisite. Estimated time of completion: 15 minutes <i>Check off (✓) each step as it is completed. Shaded steps indicate: gray = input, white = output, black = Go-No-Go.</i>	
	Task	Description
1 <input type="checkbox"/>	PM&C server: Login	Login to the PM&C server \$ ssh admusr@<PM&C_IPv6_Address>
2 <input type="checkbox"/>	Identify all aggregation switches	Each aggregation switch must be individually configured. The following steps are repeated for each device in Section 4.2.3 If there are no aggregation switches, skip to step 17.
3 <input type="checkbox"/>	List interfaces	For aggregation device, display all the interfaces: \$ sudo netConfig --device=<name> listInterfaces
4 <input type="checkbox"/>	Identify interfaces	Each interface is the IPv4 Interfaces section of output: IPv4 Interfaces: = (VLAN20 <interface>) IPv6 Interfaces: = (VLAN20)
5 <input type="checkbox"/>	Display interface addresses	Display the IPv4 addresses \$ sudo netConfig --device=<name> getInterface interface=<if>
6 <input type="checkbox"/>	Identify address	IP Address: = (<IPv4_Address> FD0D:DEBA:D97C:FFF::10/64) Netmask: <IPv4_Netmask> Router Advertisements: On
7 <input type="checkbox"/>	Calculate CIDR	Determine the network prefix to use for the IPv4 address in CIDR format for the next step. \$ ipcalc -p <IPv4_Address> <IPv4_Netmask>

<p>8 <input type="checkbox"/></p>	<p>Delete IPv4 addresses</p>	<p>Delete the IPv4 addresses.</p> <pre>\$ sudo netConfig --device=<name> deleteInterface interface=<interface> ip=<IPv4_Address>/<prefix></pre>
<p>9 <input type="checkbox"/></p>	<p>Verify IPv4 address removed</p>	<p>Verify the address was deleted</p> <pre>\$ sudo netConfig --device=<name> getInterface interface=<if></pre>
<p>10 <input type="checkbox"/></p>	<p>Identify IPv4 routes</p>	<p>Use the following command to identify all IPv4 routes:</p> <pre>sudo netConfig --device=<name> listRoutes Interface: VLAN2 Netmask: = (<IPv4_Netmask> 255.255.255.255) Network: = (<IPv4_network> 0.0.0.0 2001:DB8::/32 ::/0) Next Hop: = (<nexthop> 192.168.2.1 FD0D:DEBA:D97C:FF1:5054:FF:FE3A:FC2B FE80::1 FD0D::1)</pre>
<p>11 <input type="checkbox"/></p>	<p>Delete IPv4 Routes</p>	<p>Use the following command to identify the CIDR netmask to use when deleting the routes identified in the previous step:</p> <pre>\$ ipcalc -p <IPv4_Network> <IPv4_Netmask></pre> <p>PREFIX=<prefix></p> <p>Delete all IPv4 routes:</p> <pre>sudo netConfig --device=<name> deleteRoute network=<IPv4_Network>/<prefix> nexthop=<nexthop></pre>
<p>12 <input type="checkbox"/></p>	<p>Verify all IPv4 addresses and routes are removed</p>	<p>Repeat steps 3 through 11 above for each device.</p> <p>Then, verify no IPv4 addresses still exist:</p> <pre>\$ sudo netConfig --device=<name> listInterfaces</pre> <p>Verify no IPv4 routes still exist:</p> <pre>sudo netConfig --device=<name> listRoutes</pre>

13 <input type="checkbox"/>	Display virtual interfaces	For aggregation device, display any IPv4 virtual interfaces: \$ sudo netConfig --device=<name> listVR protocol=v4
14 <input type="checkbox"/>	Identify interfaces	Each virtual interface is defined by the ID and Interface. If there is more than one virtual interface, they should be paired in the order shown in the output, e.g. ID=3 and VLAN3 as shown below. <pre>ID: = (3 <id>) Interface: = (VLAN3 <interface>) Preempt: =(</pre>
15 <input type="checkbox"/>	Delete the interfaces	Delete the interface. \$ sudo netConfig --device=<name> deleteVR id=<id> interface=<interface> protocol=v4
16 <input type="checkbox"/>	Verify interfaces are removed	Verify the address was deleted \$ sudo netConfig --device=<name> listVR protocol=v4
17 <input type="checkbox"/>	Identify all enclosure switches	Enclosure switches must be individually configured. Enclosure switches dedicated to applications should be configured with application procedures. The following steps are repeated for each device from Section 4.2.3
18 <input type="checkbox"/>	Delete IPv4 addresses	\$ sudo netConfig --device=<name> deleteInterface interface=management addrType=dhcp
19 <input type="checkbox"/>	Verify IPv4 addresses are removed	Verify no IPv4 addresses are shown: \$ sudo netConfig --device=<name> getInterfaces interface=management
20 <input type="checkbox"/>	Repeat for each enclosure switch	Repeat steps 18 through 19 for each enclosure switch.
21 <input type="checkbox"/>	Backup switch configurations	Perform a backup of the aggregation and enclosure switches recorded in step 10 of procedure in section 5.1. The filename option should specify a unique name for each. \$ sudo netConfig --device=<name> backupConfiguration service=<service> filename=<device>-harvested

22 <input type="checkbox"/>		Move <code>netConfig</code> backup files to the backup directory to preserve files with PM&C backups. Replace <code><user></code> with the userid noted in Procedure 1 Step 4: \$ sudo mv ~<user>/*harvested /usr/TKLC/smac/etc/switch/backup
---End of Procedure---		

6.5 Harvest Completion

Procedure 11 Finish Harvest

S T E P	Use this procedure to verify the health of the system Estimated time of completion: 5 minutes <i>Check off (✓) each step as it is completed. Shaded steps indicate: gray = input, white = output, black = Go-No-Go.</i>	
	Task	Description
1 <input type="checkbox"/>	Health check	Execute the health check procedure in Procedure 15.
---End of Procedure---		

7 Recovery Procedures

**** WARNING ****

Execute this section only if there is a problem and it is desired to undo changes introduced with this migration procedure. Do not attempt to perform these backout procedures without first contacting Oracle Support:

Log on to [My Oracle Support](#). To contact Oracle Support by phone, refer to the [Oracle Support Contacts Global Directory](#).

NOTE: These recovery procedures are provided for the reconfiguration of the PM&C application. IPv6 addressing is left intact.

**** WARNING ****

Prior to executing this procedure, log on to [My Oracle Support](#) to ensure that proper recovery planning is performed. To contact Oracle Support by phone, refer to the [Oracle Support Contacts Global Directory](#).

Before disaster recovery, users must properly evaluate the outage scenario. This check ensures that the correct procedures are executed for the recovery.

NOTE: Disaster Recovery is an exercise that requires collaboration of multiple groups and is expected to be coordinated by the TAC prime. Based on TAC's assessment of Disaster, it may be necessary to deviate from the documented process.

7.1 Backout Setup

The decision to execute a backout may be determined at multiple points in the procedure. Since the reason and failure point cannot be known ahead of time, no definitive procedure is provided.

Oracle Support personnel may have to have login access to the affected system, probe for the root cause of the problem, and set up or clean up what is necessary to prepare the recovery.

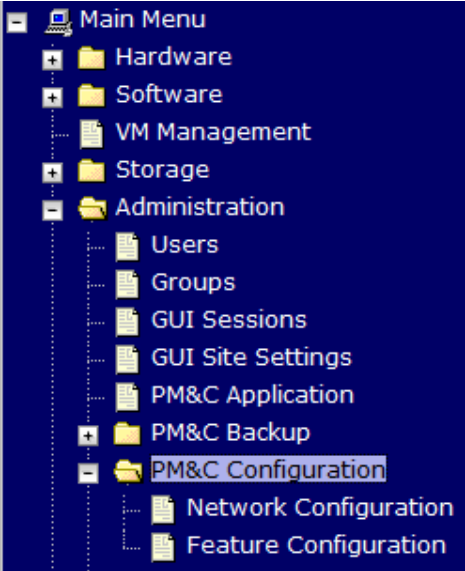
The migration procedure involved configuration a dual IP stack on all components, and configuring the IPv6 resources. If only PM&C is impacted, recovery may leave the IPv6 stack configured. The OA and management platform may require a backout. For networking issues, recovery may require backout of migration modifications.

7.2 Backout Execution

Once the necessity of a backout has been determined and the scope of the backup, the following procedures can be executed. Refer to section 3.5 for the Backout process overview.

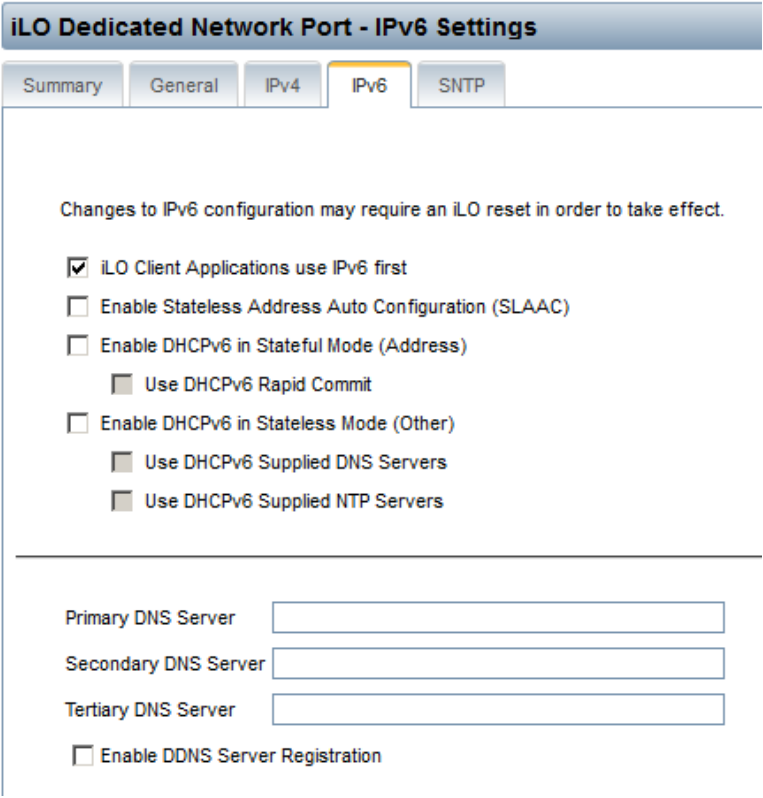
Procedure 12 PM&C Recovery Preparation

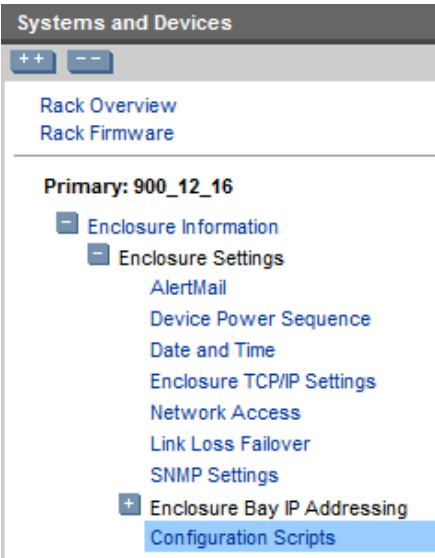
STEP	Use this procedure backout the PM&C migration. Estimated time of completion: 15 minutes <i>Check off (✓) each step as it is completed. Shaded steps indicate: gray = input, white = output, black = Go-No-Go.</i>	
	Task	Description
1 <input type="checkbox"/>	Verify recovery scope	With Oracle Support assistance, determine if the PM&C configuration must be undone.
2 <input type="checkbox"/>	PM&C: Login	Login to the PM&C host on the management server \$ ssh admusr@<PM&C_IPv4_Address> SSH access via IPv4 should still be functional, but the TVOE vi rsh console access may be used.
3 <input type="checkbox"/>	Identify and test backup	Find the backup file from the pre-migration. \$ ls -lrt /var/TKLC/smac/backup/ Verify the file and check the Description matches from your pre-migrate task comment used in step 3 of Procedure 4: \$ sudo pmacadm checkBackup --fileName=<backupFile.pef>
4 <input type="checkbox"/>	Verify backup is valid	PM&C checkBackup was successful Backup Description: Pre IPV6 migration Otherwise, contact Oracle Support for assistance
5 <input type="checkbox"/>	Prepare to restore	Reset the configuration. \$ sudo pmacadm resetProfileConfig
6 <input type="checkbox"/>	Verify reset succeeded	Platform has been successfully reset
7 <input type="checkbox"/>	Restore	Begin the restore task \$ sudo pmacadm restore --fileName=<backupFile.pef>
8 <input type="checkbox"/>	Note the task ID	PM&C Restore been successfully initiated as task ID <taskID>

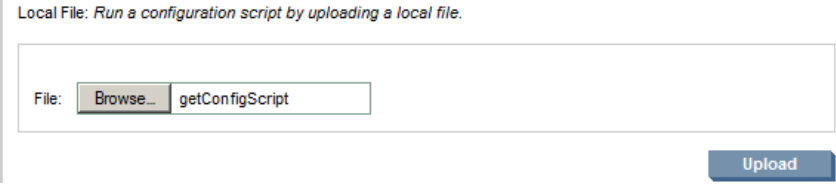

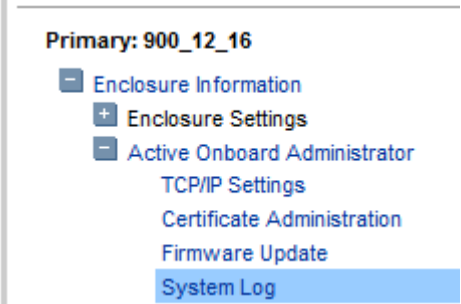
<p>9 <input type="checkbox"/></p>	<p>Verify restore completes</p>	<p>Wait for the task state to reach the COMPLETE state: It will take a few minutes, and network interruptions and an application restart may be noticed.</p> <pre>\$ sudo pmaccli getBgTaskState --id=<taskID> IN_PROGRESS \$ sudo pmaccli getBgTaskState --id=<taskID> Error communicating with the PM&C server. Is the application running? \$ sudo pmaccli getBgTaskState --id=<taskID> COMPLETE</pre>
<p>10 <input type="checkbox"/></p>	<p>Logout of shell</p>	<pre>\$ exit</pre>
<p>11 <input type="checkbox"/></p>	<p>PM&C: Login to PM&C GUI</p>	<p>Navigate to the current network configuration:</p> <p>Main Menu -> Administration -> PM&C Configuration</p>  <p>The screenshot shows a tree view of the PM&C GUI. The 'Main Menu' is expanded to show 'Administration', which is further expanded to show 'PM&C Configuration'. Other items in the tree include Hardware, Software, VM Management, Storage, Users, Groups, GUI Sessions, GUI Site Settings, PM&C Application, PM&C Backup, Network Configuration, and Feature Configuration.</p>
<p>12 <input type="checkbox"/></p>	<p>Verify</p>	<p>The Configuration Summary should show the pre-migration state.</p>
<p>13 <input type="checkbox"/></p>	<p>Logout</p>	<p>Press the Logout button.</p>
<p>14 <input type="checkbox"/></p>	<p>Continue?</p>	<p>If the Management server or IPv6 network changes must be backed out, continue.</p>
<p style="text-align: center;">---End of Procedure---</p>		

Procedure 13 Management recovery

S T E P	Use this procedure to restore the management server and OA components. Estimated time of completion: 20 minutes <i>Check off (✓) each step as it is completed. Shaded steps indicate: gray = input, white = output, black = Go-No-Go.</i>	
	Task	Description
1 <input type="checkbox"/>	Verify scope	With Oracle Support assistance, determine if the OA and management server must be restored to their original configurations.
2 <input type="checkbox"/>	RMS iLO: Login	Login to the iLO on the management server https://<iLO_IPv4_Address>
3 <input type="checkbox"/>	Navigate to configuration	Navigate to the network configuration: Network -> iLO Dedicated Network Port <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Expand All</p> <ul style="list-style-type: none"> <input type="checkbox"/> Information <input type="checkbox"/> iLO Federation <input type="checkbox"/> Remote Console <input type="checkbox"/> Virtual Media <input type="checkbox"/> Power Management <input checked="" type="checkbox"/> Network <ul style="list-style-type: none"> <li style="background-color: #add8e6;">iLO Dedicated Network Port Shared Network Port </div>

<p>4 <input type="checkbox"/></p>	<p>Remove IPv6 addresses</p>	<p>Remove the IPv6 addressing on the IPv6 tab and uncheck the ...use IPv6 first checkbox. Press the Submit button and then the Reset button. A pop-up will ask to authorize a reset.</p> 
<p>5</p>	<p>Change NTP if necessary</p>	<p>If NTP was configured with IPv6 addresses on the OA: On the SNTP tab, update the servers to use IPv4 addresses, then press the Submit and Reset buttons.</p>
<p>6</p>	<p>Logout</p>	<p>Press the Sign out button when complete.</p>
<p>7 <input type="checkbox"/></p>	<p>Application RMS servers</p>	<p>If Application RMS server iLO interfaces were updated in Procedure 2 remove the IPv6 iLO addresses on those servers.</p>
<p>8 <input type="checkbox"/></p>	<p>OA: Login to active OA</p>	<p>For each enclosure (identified in section 4.2.3), display the OA login window</p> <p>https://<OA_IPv4_Address></p> <p>If the login window shows the OA is in Standby mode, login with the other OA IP address.</p>

<p>9</p> <p><input type="checkbox"/></p>	<p>Prepare to restore OA</p>	<p>Navigate to the Configuration Scripts:</p> <p>Enclosure Information -> Enclosure Settings -> Configuration Scripts</p>  <p>The screenshot shows a web interface titled "Systems and Devices" with expand/collapse buttons. Under "Enclosure Information", "Enclosure Settings" is expanded, and "Configuration Scripts" is highlighted in blue.</p>
<p>10</p> <p><input type="checkbox"/></p>	<p>Select file to restore</p>	<p>Upload the file saved in Procedure 3 step 5. Press the Browse button then select the saved file from the pop-up window and then press Open.</p> <p>Configuration Scripts</p> <p>A configuration script may be used to automate the setup process for this enclosure. If you have a script file on a local drive you may upload it. If the script is located on a web server you may provide the URL to the script.</p> <p><i>Note: Do not directly apply a configuration script from another enclosure without removing or changing possibly unique settings such as the enclosure Asset Tag, enclosure name, static IP addresses and EBIPA settings.</i></p> <p>SHOW CONFIG: Click to view a configuration script containing the current settings for this enclosure.</p> <p>SHOW ALL: Click to view a script containing a list of the enclosure's current inventory.</p> <p>Local File: <i>Run a configuration script by uploading a local file.</i></p> <p>File: <input type="button" value="Browse..."/> No file selected.</p> <p><input type="button" value="Upload"/></p> <p>URL: <i>Run a configuration script from a URL accessible file.</i></p> <p>URL: <input type="text"/></p> <p><input type="button" value="Apply"/></p>

<p>11 <input type="checkbox"/></p>	<p>Begin restore</p>	<p>Press the Upload button:</p>  <p>Local File: <i>Run a configuration script by uploading a local file.</i></p> <p>File: <input type="text" value="getConfigScript"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/></p>
<p>12 <input type="checkbox"/></p>	<p>The script is uploaded and run</p>	<p style="text-align: center;">Completing Script Upload and Execution ...</p> 
<p>13 <input type="checkbox"/></p>	<p>Verify logs</p>	<p>Navigate to the logs to review for errors. If in doubt, consult Oracle Support:</p>  <p>Primary: 900_12_16</p> <ul style="list-style-type: none"> <input type="checkbox"/> Enclosure Information <input type="checkbox"/> Enclosure Settings <input type="checkbox"/> Active Onboard Administrator <ul style="list-style-type: none"> TCP/IP Settings Certificate Administration Firmware Update System Log
<p>14 <input type="checkbox"/></p>	<p>Logout</p>	<p>Press the Sign out button when complete.</p>
<p>15 <input type="checkbox"/></p>	<p>Additional OAs?</p>	<p>Restore the OA configuration for each enclosure.</p>
<p>16 <input type="checkbox"/></p>	<p>Management server: Login</p>	<p>Login to the TVOE host on the management server</p> <pre>\$ ssh admusr@<TVOE_IPv4_Address></pre>
<p>17 <input type="checkbox"/></p>	<p>List routes</p>	<p>Check for IPv6 routes on the management and other bridges listed in section 4.2.2.</p> <pre>\$ sudo netAdm query --route --device=management</pre>
<p>18 <input type="checkbox"/></p>	<p>Remove IPv6 routes</p>	<p>Remove the IPv6 routes, for example:</p> <pre>\$ sudo netAdm delete route --route=default --device=management --gateway=<ipv6_address></pre>
<p>19 <input type="checkbox"/></p>	<p>List bridges</p>	<p>Display the the management and other bridges:</p> <pre>\$ sudo netAdm query --type=Bridge --name=management</pre>

20 <input type="checkbox"/>	Remove IPv6 address	Remove the IPv6 address from the management bridge and other bridges. \$ sudo netAdm delete --type=Bridge --name=<management> --address=<ipv6_address> --netmask=<ipv6_prefix>
21 <input type="checkbox"/>	Continue?	If the IPv6 network changes must be backed out, continue.
---End of Procedure---		

Procedure 14 Network Recovery

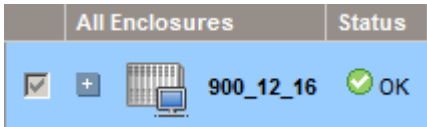
S T E P	Use this procedure to restore the network devices to the original state. Estimated time of completion: 20 minutes <i>Check off (✓) each step as it is completed. Shaded steps indicate: gray = input, white = output, black = Go-No-Go.</i>	
	Task	Description
1 <input type="checkbox"/>	Verify scope	With Oracle Support assistance, determine if the network devices must be restored to their original configurations.
2 <input type="checkbox"/>	PM&C: Login	Login to the PM&C host on the management server using IPv4 addresses. \$ ssh admusr@<PM&C_IPv4_Address>
3 <input type="checkbox"/>	Restore repository	Restore the pre-migration netConfig repository \$ sudo cp -fp /usr/TKLC/plat/etc/TKLCnetwork-config/model.xml-premigrate /var/TKLC/smac/backup/model.xml
4 <input type="checkbox"/>	List service used to backup	List the service used to backup. This will be used to list all the backup files: \$ sudo netConfig -repo showService name=<service>
5 <input type="checkbox"/>	Find backup location	The output include the user: field, to identify the location of backup files: <pre> Service Name: pmacSCP Type: ssh Host: 10.240.72.40 Options: password: FC076474A8F1ECB8 user: pmacuser </pre>
6 <input type="checkbox"/>	List configuration files	List the backup files that need to be used in the next step (e.g. <code>ls ~pmacuser/*pre migrate</code>): \$ sudo ls ~<user>/*pre migrate

7 <input type="checkbox"/>	Restore configurations	<p>Perform a restore of <i>all</i> aggregation and enclosure switches using the filename and service from the backup. Switches will reboot during this step:</p> <pre>\$ sudo netConfig --device=<name> restoreConfiguration service=<service> filename=<device>-premigrate</pre>
8 <input type="checkbox"/>	Verify netConfig	<p>The following command will attempt to login to each switch using the management address. It is only to verify access from netConfig, not the switch configuration.</p> <pre>\$ sudo netConfig --repo validate</pre>
9 <input type="checkbox"/>	Logout	<pre>\$ exit</pre>
10 <input type="checkbox"/>	Health checks	The health check procedure should be executed, but additional verification may be required.
---End of Procedure---		

8 Health Check Procedures

Depending upon the calling procedure, either IPv4 or IPv6 addresses may be used here.

Procedure 15 Health Check

STEP	Use this procedure to verify the system health of platform components. Estimated time of completion: 5 minutes <i>Check off (✓) each step as it is completed. Shaded steps indicate: gray = input, white = output, black = Go-No-Go.</i>	
	Task	Description
1 <input type="checkbox"/>	PM&C: Login	Login to the PM&C on the management server \$ ssh admusr@<PM&C_IP_Address>
12 <input type="checkbox"/>	Check for alarms	\$ sudo alarmMgr --alarmStatus
13 <input type="checkbox"/>	Verify	No (new) alarms should be reported. Otherwise, stop and contact Oracle Support.
14 <input type="checkbox"/>	List OAs	List provisioned enclosures to be used in OA health checks \$ sudo pmacccli getProvEnclosures
15 <input type="checkbox"/>	TVOE: Login	Login to the TVOE host on the management server \$ ssh admusr@<TVOE_IP_Address>
16 <input type="checkbox"/>	Check for alarms	\$ sudo alarmMgr --alarmStatus
17 <input type="checkbox"/>	Verify	No alarms should be reported. Otherwise, stop and contact Oracle Support.
18 <input type="checkbox"/>	OA: Display Login GUI	For each enclosure (from step 4), display the OA login window https://<OA_IP_Address> If the login window does not show OK, continue to login. Otherwise this procedure is complete. 

<p>19</p> <p><input type="checkbox"/></p>	<p>Verify details</p>	<p>Click on the system status link to display the alerts.</p> <p>If any alerts are displayed, contact Oracle Support.</p> <div style="border: 1px solid gray; padding: 5px; background-color: #f0f0f0;"> <p>System Status ☰</p> <hr/> <p>View Legend ...</p> <hr/> <p><i>Updated Tue Jul 15 2014, 10:52:34</i></p> <hr/> <p> ✖ ▼ ⚠ i ? 🔄 </p> <p>System Status 0 0 0 0 0 0</p> </div>
<p>---End of Procedure---</p>		

Appendix A. SWOPS Sign Off

Discrepancy List

Date	Test Case	Description of Failure/Issues. Any CSRs/RMAs issued during Acceptance. Discrepancy	Resolution and SWOPS Engineer Responsible	Resolution Date

Appendix B. Customer Sign-Off

Sign-Off Record

*** Please review this entire document. ***

This is to certify that all steps required for the upgrade completed successfully without failure.

Sign your name to show approval of this procedure. Then fax this page and the Discrepancy List to:

Oracle Support, FAX # 919-460-3669.

Company Name: _____

Date: _____

Site: Location: _____

Customer:(Print) _____

Phone: _____

Fax:: _____

Start Date: _____

Completion Date: _____

This procedure has been approved by the undersigned. Any deviations from this procedure must be approved by both Oracle and customer representatives. A copy of this page was given to the customer representative. The SWOPS supervisor will maintain signed original..

Oracle (Print): _____

Date: _____

Appendix C. Locate Product Documentation on the Oracle Technology Network Site

Oracle customer documentation is available on the web at the Oracle Technology Network (OTN) 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 www.adobe.com.

1. Log into the Oracle Technology Network site at <http://docs.oracle.com>.
2. Select the Applications tile.
The Applications Documentation page appears.
3. Select Apps A-Z.
4. After the page refreshes, select the Communications link to advance to the Oracle Communications Documentation page.
5. Navigate to your Product and then Release Number, and click the View link (note that the Download link will retrieve the entire documentation set).
6. To download a file to your location, right-click the PDF link and select Save Target As.