Oracle® Communications Policy Management

Platform Configuration User's Guide

Release 9.7.4

E70985 Revision 01

April 2016

ORACLE®

Table of Contents

List of Tables

Chapter

1

About This Guide

Topics:

This chapter describes the organization of the document and provides other information that could be useful to the reader.

How This Guide is Organized

The information in this guide is presented in the following order:

- *About This Guide* contains general information about this guide, the organization of this guide, and how to get technical assistance.
- *Introduction* describes how to access the Platcfg utility, how to use the utility interface in a Policy Management environment, and troubleshooting.
- *Performing Initial Server Configuration* describes how to access the Platcfg utility and configure your application's initial configuration, and then how to verify the configuration.
- *Managing Certificates* describes how to access the Platcfg utility to manage SSL security certificates, which allow two systems to interact with a high level of security.
- *Synchronizing Files* describes how and when to synchronize files in clusters.
- *Custom Ethtool Options* describes how to manually configure Ethtool options.
- *Performing System and Server Backups and Restores* describes how to perform system and server backups and restores.
- Glossary

Intended Audience

This guide is intended for service personnel who are responsible for operating Policy Management systems.

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1: Admonishments

Icon	Description
DANGER	Danger: (This icon and text indicate the possibility of *personal injury*.)
WARNING	Warning: (This icon and text indicate the possibility of *equipment damage*.)

Icon	Description
	Caution: (This icon and text indicate the possibility of *service interruption*.)
	Topple: (This icon and text indicate the possibility of *personal injury* and *equipment damage*.)

Related Publications

For information about additional publications that are related to this document, refer to the *Related Publications Reference* document, which is published as a separate document on the Oracle Help Center site. See *Locate Product Documentation on the Oracle Help Center Site* for more information.

Locate Product Documentation on the Oracle Help Center Site

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

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

Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

http://education.oracle.com/communication

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

www.oracle.com/education/contacts

My Oracle Support (MOS)

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

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

1. Select **2** for New Service Request
2. Select **3** for Hardware, Networking and Solaris Operating System Support
3. Select one of the following options:

   - For Technical issues such as creating a new Service Request (SR), Select **1**
   - For Non-technical issues such as registration or assistance with MOS, Select **2**

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

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

Emergency Response

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

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

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

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

Chapter

2

Introduction

Topics:

This chapter describes how to use the Oracle Communications Policy Management Platform Configuration utility (Platcfg) to configure Oracle Communications Policy Management (Policy Management) on Oracle Communications Policy Management Configuration Management Platform (CMP) servers and Policy Management servers. The reference to Policy Management servers will be used throughout this document to mean the Oracle Communications Policy Management Multimedia Policy Engine (MPE), Oracle Communications Policy Management Multi-Protocol Routing Agent (MRA), Oracle Communications Policy Management Bandwidth on Demand (BoD), Oracle Communications Policy Management Message Distribution Function (MDF), and Oracle Communications Policy Management Management Agent (MA), collectively. Each server is described individually in detail in their respective manuals.

The pages, tabs, fields, menu items, and functions that you see in the utility depend on your configuration, application, or mode.

Platcfg Overview

The Platcfg utility is a Command Line Interface (CLI) tool that simplifies the execution of tasks that cannot be included in the application software. These tasks include those that affect operating system operations or platform services that are invisible to an application or that are not accessible from the application management controls. Platcfg simplifies task execution and reduces the chance of user errors through the use of wizard-like menu options and forms.

You access Platcfg menus by logging in from a console or logging in remotely. Platcfg security actions are centralized at the active CMP server, with all functions propagated automatically to all connected servers.

Accessing Platcfg

- To access Platcfg from the system console:
  - Log on as **root**.
  - Then enter su - platcfg.

- To access Platcfg through an SSH remote session:
  - Log on as **admusr**.
  - Then enter sudo su - platcfg.

Using the Platcfg Utility

Use the following actions to move and enter information within the Platcfg utility:

- Up and down arrows--Moves the action up or down.
- Left and right arrows--Moves the action sideways.
- Enter key--Enters the selected item and moves to the next menu or feature screen.
- First letter--Select the first letter of a menu item to move to that item.

Using the Save Platform Debug Logs Menu to Troubleshoot

If a system failure occurs, use the **Save Platform Debug Logs** menu option on the **Policy Configuration Menu** to help troubleshoot the issue.

Saving Platform Debug Logs

The **Save Platform Debug Logs** menu is used to help troubleshoot a system failure. This action provides two settings that allow you to limit the size of the saved log files.

Information saved in the logs includes the current state of all logs, all the configuration files, all the system proc entries, and several miscellaneous files. Output from this process is a single tar/gzip file.

To access this utility:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.
2. If at the **root** prompt, enter:
   `su - platcfg`
3. If at the **camiant** prompt, to access a limited set of actions, enter:
   `su - platcfg`
4. Or if at the **camiant** prompt, to access a full set of actions, enter:
   a) `su - root`

   Note: The **root** password is not requested.

   b) `su - platcfg`
5. If at the **admusr** prompt, enter:
   `sudo su - platcfg`

   Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
7. Select **Save Platform Debug Logs** from the **Policy Configuration Menu** and press **Enter**.
8. In the screen that opens, enter values, where:

   - **Record limit for qptrace**--Specifies the maximum number of qptrace messages to save. Do not change this setting when generating a save log to debug a problem; only reduce the default number messages when instructed to do so by Customer Support.
   - **Record limit for AppEventLog**--Specifies the maximum number of AppEventLog records to save. Do not change this setting when generating a save log to debug a problem; only reduce the default number records when instructed to do so by Customer Support.
   - **Remember count limit settings**--Specifies whether or not to retain limit setting from previous log.
   - **Include trace/subact/sync log**--Indicates whether to include the extra trace/subact/sync debug records.
   - **Save as**--Lists the path and filename of the file being saved.

   Note: Include trace/subact/sync log should be left set to **No** unless directed to be set to **Yes** by *My Oracle Support (MOS)*.

9. Select **OK** and press **Enter** to save variable changes and generate the tar/gzip file.
   The file is generated and saved in the specified location.

Chapter

3

Performing Initial Server Configuration

Topics:

This chapter describes how to access the Platcfg utility, set the Policy Management configuration mode, configure the initial configuration, and then how to verify the configuration.

Setting the Policy Management Mode

To select the Policy Management mode:

1. Access Platcfg. Refer to *Accessing Platcfg* for details.
2. Select **Policy Configuration** from the **Main Menu** screen and press **Enter**.
3. Select **Set Policy Mode** from the **Policy Configuration Menu** screen and press **Enter**.
4. Select the appropriate mode for your system and press **OK**.
5. If the **Select Network Layout** screen opens, you will need to select the appropriate **Network layout profile**. Refer to *Table 2: Server Network Layouts* for information about the network layout choices.

    a) If you have an Ethernet Mezzanine card installed, select a **Network layout profile** from the **Select Network Layout** screen, select **OK**, and press **Enter.**

        Note: To enable traffic segregation in a system, an Ethernet Mezzanine card is required and the selection of a **Network layout profile** other than **common** from the **Select Network Layout** screen is required.

        Note: If the system does not have an Ethernet Mezzanine card, the **Select Network Layout** screen is not displayed, and the **Network layout profile** of **Common** is applied automatically.

    b) If you have an MRA server and you are using Hewlett Packard (HP) c-Class or Sun Netra hardware to provide separate external SCTP multi-homing and internal traffic by using an additional signaling interface, select **common_with_sigc** from the **Select Network Layout** screen, select **OK**, and press **Enter**.

Table 2: Server Network Layouts

Network Layout Profile	Network Layout Detail	Description
common	PMAC=bond0 OAM=bond0.<VLAN> SIGA=bond0.<VLAN> SIGB=bond0.<VLAN>	This is the default layout after policy product is installed. With this layout, the mezzanine cards are not used. The product behaves exactly like an ordinary c-Class server.
segregated	PMAC=bond0 OAM=bond0.<VLAN> SIGA=bond1.<VLAN> SIGB=bond1.<VLAN>	This mode is used by MPE and MRA for traffic segregation. If the server is upgraded from an earlier release with traffic segregation enabled, this layout is automatically selected.
bkup	PMAC=bond0 OAM=bond0.<VLAN> SIGA=bond0.<VLAN> SIGB=bond0.<VLAN>	This mode is used by CMP where an extra BKUP interface is used. If the server is a CMP upgraded from an earlier release with

Network Layout Profile	Network Layout Detail	Description
	BKUP=bond2	segregation turned off, this layout is automatically selected.
segregated_with_bkup	PMAC=bond0

OAM=bond0.<VLAN>

SIGA=bond1.<VLAN>

SIGB=bond1.<VLAN>

BKUP=bond2 | This mode is used by CMP where an extra BKUP interface is used.

If the server is a CMP upgraded from an earlier release with segregation turned on, this layout is automatically selected |
| common_with_sigc | OAM=bond0.<VLAN>

PMAC=bond0

SIGA=bond0.<VLAN>

SIGB=bond0.<VLAN>

SIGC=bond0.<VLAN> | This mode is used by a customer using an MRA server only in the Wireless mode with c-Class or Netra hardware to provide separate external SCTP multi-homing and internal traffic by using an additional signaling interface. |

Initial Configuration

This section describes how to perform the initial configuration on the CMP devices in your system.

To perform the initial configuration of the system:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.
2. If at the **root** prompt, enter:
    `su – platcfg`
3. If at the **admusr** prompt, enter:
    `sudo su – platcfg`

    Note: The dash (-) is required in the `su – platcfg` or the `sudo su – platcfg` command to ensure proper permissions.

4. If at the **camiant** prompt, to access a limited set of actions, enter:
    `su – platcfg`
5. Or if at the **camiant** prompt, to access a full set of actions, enter:
    a) `su – root`

    Note: The **root** password is not requested.

    b) `su – platcfg`
6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
7. Select **Perform Initial Configuration** from the **Policy Configuration Menu** and press **Enter**.

8. The **Initial Configuration** screen opens.

   Enter the configuration values and then select **OK**, where:

   - **HostName**--The unique name of the host for the device being configured.
   - **OAM Real IP Address**--The IP address that is permanently assigned to this device.
   - **OAM Real IPv4 Address**--The IPv4 address that is permanently assigned to this device.
   - **OAM Default Route**--The default route of the OAM network.
   - **OAM IPv4 Default Route**--The IPv4 default route of the OAM network.
   - **OAM Real IPv6 Address**--The IPv6 address that is permanently assigned to this device.
   - **OAM IPv6 Default Route**--The IPv6 default route of the OAM network.
   - **NTP Server** (required)--A reachable NTP server on the OAM network.
   - **DNS Server A** (optional)--A reachable DNS server on the OAM network.
   - **DNS Server B** (optional)--A second reachable DNS server on the OAM network.
   - **DNS Search**--A directive to a DNS resolver (client) to append the specified domain name (suffix) before sending out a DNS query.
   - **Device**--The bond interface of the OAM device. Note that the default value should be used, as changing this value is not supported.
   - **OAM VLAN**--The OAM network VLAN Id (only applies to c-Class servers or Netra X3-2 RMS; field does not display otherwise).
   - **SIG A VLAN Id**--The Signaling-A network VLAN Id (only applies to c-Class servers or Netra X3-2 RMS; field does not display otherwise).
   - **SIG B VLAN Id**--The Signaling-B network VLAN Id (only applies to c-Class servers or Netra X3-2 RMS; field does not display otherwise).
   - **SIG C VLAN Id**--The Signaling-C network VLAN Id (only applies to c-Class servers or Netra X3-2 RMS; field does not display otherwise).

   - **BackplaneDevice**--The backplane bond interface of the OAM device.
   - **BackplaneIIpPrefix**--The backplane bond interface IP Prefix of the OAM device.

   Note: All of the fields listed above are required, except for fields *DNS Server* and *DNS Search*, which are optional but recommended.

   Note: If traffic segregation is available and is defined, the SIG-A and SIG-B interfaces will be segregated onto the optional second pair of 6120XG/6125XLG enclosure switches. Do not enable traffic segregation if a second pair of 6120XG/6125XLG enclosure switches are not available. Traffic separation information is set in the **Set Policy Mode** activities.

   Note: Every network service and IP flow that is supported by IPv4 is now supported by IPv6. Either interface or a combination of the two can be configured.

9. When finished, select **OK** to save and apply the configuration. At this point the screen pauses for approximately 1 minute. This is normal behavior.

Verifying the Initial Configuration

This section describes how to verity the initial configuration on the CMP devices in your system after you have made the initial configuration settings.

To verify the initial configuration of the system:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) `su - root`

      Note: The **root** password is not requested.

   b) `su - platcfg`

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Verify Initial Configuration** from the **Policy Configuration Menu** and press **Enter**.

7. Your initial configuration settings are displayed.

Verifying the Server Status

After you have made and verified your initial configuration settings, verify the server status by completing the following procedure:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) `su - root`

      Note: The **root** password is not requested.

   b) `su - platcfg`

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Verify Server Status** from the **Policy Configuration Menu** and press **Enter**.

7. Once fully configured, a server will show the server role as **Active** or **Standby**, (or **Spare**, if this is a Policy Management server configured for georedundancy). **Unknown** is a valid state during initial configuration, because the cluster has not been formed. **Policy Process Management Status** should always be **Running**.

Cleaning Up the Cluster Configuration

After removing a server from a cluster and before adding the server to another cluster, clean up the cluster:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
    ```
    su - platcfg
    ```

3. If at the **admusr** prompt, enter:
    ```
    sudo su - platcfg
    ```

    Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

4. Select **Cluster Configuration Removal** from the **Policy Configuration Menu** screen and press **Enter**.

5. Select **Cluster Information Cleanup** from the **Cleanup Configuration Menu** screen and press **Enter**.

6. Select **Yes** or **No** from the **Cleaning up cluster information** screen and press **Enter**.

Configuring Routing on Your Server

This section describes how to configure routes on your server.

When creating routes for an interface that does not have an active IP address, such as the SIG-A interface on the standby server you receive a warning stating that the route cannot be applied at this time but it will be saved. These routes show as **INACT** on the display routes section.

Configuring a Route

To configure a route:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
    ```
    su - platcfg
    ```

3. If at the **camiant** prompt, to access a limited set of actions, enter:
    ```
    su - platcfg
    ```

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

    a) `su - root`

      Note: The **root** password is not requested.

    b) `su - platcfg`

5. If at the **admusr** prompt, enter:

```
sudo su - platcfg
```

Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.

7. Select **Routing Config** from the **Policy Configuration Menu** and press **Enter**.

8. Select **Add Route** from the **Route Configuration Menu** and press **Enter**.

The **Add Route** configuration screen is displayed.

9. Edit the information displayed on the **Add Route** screen, where:

   - **IP Type**--Defines whether this will be an IPv4 or IPv6 route.

   - **Route Type**--Defines whether this route will be for a specific destination (Host), a specific network segment (Net), or a default route. Note that this option is provided to allow the default route to be moved to a different interface; only one default route per address family (IPv4 or IPv6) should exist on a system at one time.

   - **Network**--Indicates whether this route will be created on the OAM, REP (replication), SIGA, or SIGB interface. Note that the BKUP network is available on CMP servers with the optional mezzanine card installed and also on all Oracle RMS including X3-2 NETRA and X5-2 (non-NETRA only) for all products including CMP, MPE, and MRA.

   - **Preferred Source Addr**--Indicates the source address selection for outgoing traffic.

     Options include None, VIP, and STATIC. where:

     - VIP is the virtual IP configured in the CMP GUI.
     - STATIC includes:

       - OAM IP address configured in Policy Initial Configuration
       - Static IP configured in the CMP Topology GUI
       - An IP address assigned by netAdm or ifconfig or `ip addr add`
       - An IP address added by manual editing of the ifcfg file

     - NONE refers to no VIP or STATIC IP assignment.

   Note: See *Table 3: Detailed Behavior of Preferred Source Addr* for details about the behavior of Preferred Source Addr.

   - **Destination**--Indicates the destination IP address.

   - **Gateway Address**--Indicates the gateway address.

Table 3: Detailed Behavior of Preferred Source Addr

Preference/status	Prefer None	Prefer VIP	Prefer STATIC
No VIP, no static IP	Not applied. On Active server, alarm 70015 is raised. On Standby or Spare server, this error is ignored.	Not applied. If VIP is not configured, Alarm 70016 is raised. On Active server, alarm 70015 is also raised.	Not applied. Alarm 70017 is raised.

Preference/status	Prefer None	Prefer VIP	Prefer STATIC
No VIP, one or more static IP	Applied without "src" option specified to kernel. Kernel will use the first static IP as source address automatically.	Not applied. If VIP is not configured, Alarm 70016 is raised. On Active server, alarm 70015 is also raised.	Applied to the first static IP
One VIP, no static IP	Applied without "src" option specified to kernel. Kernel will use the VIP as source address automatically.	Applied to VIP	Not applied. Alarm 70017 is raised.
One VIP, one or more static IP	Applied without "src" option specified to kernel. Kernel will use the VIP as source address automatically.	Applied to VIP	Applied to first static IP
Two or more VIPs, no static IP	Applied without "src" option specified to kernel. Kernel will use the first VIP as source address automatically.	Applied to first VIP	Not applied. Alarm 70017 is raised.
Two or more VIPs, one or more static IP	Applied without "src" option specified to kernel. Kernel will use the first static IP as source address automatically.	Applied to first VIP	Applied to first static IP

10. When finished editing, select **OK** and press **Enter**. Press **Enter** again to save changes.

Deleting a Route

To delete an existing route:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) ```su - root```

   Note: The **root** password is not requested.

   b) ```su - platcfg```

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.

7. Select **Routing Config** from the **Policy Configuration Menu** and press **Enter**.

8. Select **Delete Route** from the **Route Configuration Menu** and press **Enter**.

9. Select the route to delete by pressing the space bar, then select **OK** and press **Enter**. Use the **Top**, **Bottom**, **Prev,** and **Next** buttons to scroll through the list. More than one route can be deleted at a time.

   Note: The route is deleted without confirmation.

Displaying Configure Routes

To display configured routes:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```

4. Or if at the **camiant** prompt, to access a full set of actions, enter:
   a) `su - root`

      Note: The **root** password is not requested.

   b) `su - platcfg`

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.

7. Select **Routing Config** from the **Policy Configuration Menu** and press **Enter**.

8. Select **Display Routes** from the **Route Configuration Menu** and press **Enter**.

The status of each route displays as either **ACT** or **INACT**. **ACT** means the route is active and currently running. **INACT** means that the route is saved in configuration, but cannot be activated at this time. An inactive route may mean that an interface for which the route is configured does not currently have an IP address; for example, a standby server on an interface that only has a VIP. An inactive route may also mean that a route has been configured incorrectly, with the gateway IP address not on the same subnet as the interface IP address.

Exporting a Route

Routes can be exported from one server and imported into another or exported and modified with a text editor before importing. To export all existing routes in a route list:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) ```su - root```

      Note: The **root** password is not requested.

   b) ```su - platcfg```

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.

7. Select **Routing Config** from the **Policy Configuration Menu** and press **Enter**.

8. Select **Export Route** from the **Route Configuration Menu** and press**Enter**.

9. Specify the location and filename of the routes in a route list that are to be exported, then select **OK** and press **Enter**. Routes in a route list are exported to the specified directory and filename.

Importing a Route

To import all existing routes within a route list into the routing configuration:

Note: Exported routes can be modified with a text editor before importing.

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) ```su - root```

      Note: The **root** password is not requested.

   b) ```su - platcfg```

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

> **Note:** The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
7. Select **Routing Config** from the **Policy Configuration Menu** and press **Enter**.
8. Select **Import Routes** from the **Routing Configuration Menu** and press **Enter**.
9. Specify the location and filename of the routes in a route list that are to be imported, then select **OK** and press **Enter**.
   Routes in a route list are imported into the routing configuration from the specified directory and filename.

Restarting the Application

To restart the application:

> **Note:** Restarting the application will interrupt service on a server if it is in an active role. However, restarting the application does not log out users.

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.
2. If at the **root** prompt, enter:
   `su - platcfg`
3. If at the **camiant** prompt, to access a limited set of actions, enter:
   `su - platcfg`
4. Or if at the **camiant** prompt, to access a full set of actions, enter:
   a) `su - root`

      > **Note:** The **root** password is not requested.

   b) `su - platcfg`
5. If at the **admusr** prompt, enter:
   `sudo su - platcfg`

   > **Note:** The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**
7. Select **Restart Application** from the **Policy Configuration Menu** and press **Enter**.

Configuring Firewall Settings

> **Note:** During the editing of firewall configuration settings, if an attempt is made to leave the **Firewall Configuration Menu** with unsaved changes, you are presented with the options to save changes and exit, exit without saving changes, and to return to the **Firewall Configuration Menu** to continue.

Note: When all firewall configuration setting changes are completed, be sure to use menu item **Save and Apply Configuration** from the **Firewall Configuration Menu** to commit the changes made to the firewall configuration files and restart the firewall.

Note: In the preceding process, the term **All** indicates open access to any interface, for example: PMAC, REP, OAM, SIG-A, and SIG-B.

To configure firewall settings on the server in order to restrict access to non-standard ports:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   `su - platcfg`

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   `su - platcfg`

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) `su - root`

      Note: The **root** password is not requested.

   b) `su - platcfg`

5. If at the **admusr** prompt, enter:
   `sudo su - platcfg`

   Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.

7. Select **Firewall** from the **Policy Configuration Menu**, and press **Enter**.

8. To enable the firewall, select **Enable/Disable Firewall** from the **Firewall Configuration Menu** and press **Enter**.

9. Select **Edit** from the **Firewall Status** screen and press **Enter**.

10. To define which IPv4 and IPv6 firewall to enable or disable, select from the list of interfaces on the **Enable/Disable Firewall Features Menu** and press **Enter**.

11. When prompted to continue, select **Yes** from the **Enable iptables?** or other appropriate dialog screen that appears and press **Enter**.

12. The Factory Firewall Rule Set cannot typically be changed, but you may wish to open additional ports in the firewall by enabling custom rules. To open additional ports, select **Enable Custom Rules** from the **Enable/Disable Firewall Features Menu**.

13. Select **Yes** from the **Enable custom rules?** screen to confirm that custom rules are to be enabled or select **No** to cancel.

14. If a custom rule conflicts with a default rule, the default rule is used, but the default rule can be overridden if the custom prefer option is enabled. Rules conflict if they have matching protocols (TCP, UDP) and ports (80, 443, etc.). To set custom rules to be used instead of default firewall rules, select **Enable custom prefer** from the **Enable/Disable Firewall Features Menu**.

15. Select **Yes** from the **Enable custom prefer feature?** screen to confirm custom rules are to be preferred over default rules or select **No** to cancel.

16. To add, edit or delete custom firewall rules, select **Customize Firewall** from the **Firewall Configuration Menu**, and press **Enter**.

17. Select **Edit** from the **Firewall Custom Rules** screen and press **Enter**.

18. To add a new rule of edit an existing rule, select **Add Rule** or **Edit Rule** from the **Connection Action Menu** and press **Enter**.

19. Enter information to customize the firewall rule, then select **OK** and press **Enter**.

    Enter field values. When completed, select **OK** and press **Enter**.

    Note: If configuring a CMP with the optional Ethernet mezzanine card or any product on any mode on the Sun Netra X3-2, an additional interface appears called **BKUP**. This interface is dedicated to perform remote archive activities for CMP backup operations. **BKUP** is included if **ALL** is selected for **Interface** on the **Customize Firewall** screen.

    Note: The **REP** network selection will appear in the **Interface** screen only for c-Class MPE and MRA servers if a static IP is set in the topology for MPE and MRA. The **REP** selection will not appear for a CMP server or any other Policy Management server.

20. To delete an existing custom rule, select **Delete Rule** from the **Connection Action Menu** and press **Enter**. Then, select the rule to be deleted from the **Select Rule Menu** and press **Enter**.

21. When all editing is complete, save and apply the changes to the system:

    a) If not at the **Firewall Configuration Menu**, select **Exit** to return to the **Firewall Configuration Menu**. Then, select **Save and Apply Configuration** from the **Firewall Configuration Menu** and press **Enter** to save all changes. A dialog box will appear to confirm that the request to apply the changes is successful.

       Note: During the editing of firewall configuration settings, if an attempt is made to leave the **Firewall Configuration Menu** with unsaved changes, you are presented with the options to save changes and exit, exit without saving changes, and to return to the **Firewall Configuration Menu** to continue.

       Note: When all firewall configuration setting changes are completed, be sure to use menu item **Save and Apply Configuration** from the **Firewall Configuration Menu** to commit the changes made to the firewall configuration files and restart the firewall.

       Note: In the preceding process, the term **All** indicates open access to any interface, for example: PMAC, REP, OAM, SIG-A, and SIG-B.

Displaying Firewall Settings

To display current firewall settings, complete the following procedures:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su – platcfg
   ```

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su – platcfg
   ```

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) ```
   su – root
   ```

      **Note:** The **root** password is not requested.

    b) `su - platcfg`

5. If at the **admusr** prompt, enter:
`sudo su - platcfg`

   **Note:** The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
7. Select **Firewall** from the **Policy Configuration Menu**, and press **Enter**.
8. Select **Display Firewall** from the **Firewall Configuration Menu** and press **Enter**.
9. Select the firewall action from the **Display Firewall Menu** and press **Enter**.

   The following is an example of the **Display Firewall Status** screen:

   The following is an example of the **Display Factory Rules** screen:

   The following is an example of the **Display Custom Rules** screen:

# Configuring DSCP

Use the options on the DSCP (Differentiated Services Code Point) Configuration menu to manage DSCP configurations. These configurations allow you to operate DSCP on network interfaces (SIG A, SIG B) for a Policy Management device. The configurations are persistent during system power off, reboot, and upgrade. Configurations can also sync to other servers within a cluster.

Menu options include:

- Add a DSCP configuration
- View existing DSCP configurations
- Edit a DSCP configuration
- Delete a DSCP configuration
- Sync a configuration to other servers in cluster

## Adding a DSCP Configuration

Use **Add New DSCP Configuration** to add a new DSCP configuration on the network interface and begin DSCP marking of specified packets. Each DSCP configuration is saved to the configuration file in the order in which it is added.

To add a new DSCP configuration:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.
2. If at the **root** prompt, enter:
`su - platcfg`
3. If at the **admusr** prompt, enter:
`sudo su - platcfg`

   **Note:** The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

4. Select **DSCP Config** from the **Policy Configuration Menu** and press **Enter**.

5. Select **Add New DSCP Configuration** from the **DSCP Configuration Menu** and press **Enter**.

6. Select the desired interface for the new configuration from the **Select Interface** screen, then select **OK** and press **Enter**.

   **Note:** In the Policy Management architecture, network interfaces are segregated into SIGA, SIGB, SIGC, and OAM. The interface SIGA is used to connect to the customer signaling A network; SIGB is used to connect to the customer signaling B network; SIGC is used to connect to the customer signaling C network SIGC is used on MRA only to internally connect to MPE when both SIGA and SIGB were used for SCTP multi-homing; and OAM is used to connect to the customer management network and for internal connection between the cluster and site. The Configuration includes interface SIGA, SIGB, and SIGC but does not include OAM. Select either SIGA or SIGB for the current DSCP configuration.

   **Note:** If more than one DSCP configuration is added on the same network interface (for example, SIGA), the output packets sent from this interface are from the latest DSCP configuration added. The new DSCP configuration (with the same or greater scope in output packets of this network interface) takes precedence over any previous DSCP configurations.

   **Note:** If one interface has both VIP and IP and associates DSCP only with VIP, the packets sent from this interface may not be marked with DSCP as expected because the application may send packets from the server IP instead of the VIP.

7. Specify the **IP Protocol Version**, **Source IP Address**, and **Destination IP Address** to associate with the new configuration from the **Input Source IP and Destination IP** screen. If settings are not specified, default settings are used.
   Select **OK** and press **Enter** to save setting selections and continue to **Code Point selection**.

8. Select the **Code Point** to use with this configuration from the **Code Point selection** window, then select **OK**, and press **Enter**. When the configuration has been saved, DSCP marking begins on the specified packets.

## Viewing a DSCP Configuration

To view a DSCP configuration:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```

3. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   **Note:** The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

4. Select **DSCP Config** from the **Policy Configuration Menu** and press **Enter**.

5. Select **View DSCP Configuration** from the **DSCP Configuration Menu** and press **Enter**.

6. All existing DSCP configurations are displayed.

## Editing a DSCP Configuration

To edit an existing DSCP configuration:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```

3. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   **Note:** The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

4. Select **DSCP Config** from the **Policy Configuration Menu** and press **Enter**.

5. Select **Edit DSCP Configuration** from the **DSCP Configuration Menu** and press **Enter**.

6. All existing DSCP configurations are displayed. Select the configuration to change from the **Edit DSCP Configuraton Menu**  and press **Enter**.

7. Select the interface to use for the configuration from the **Select Interface** screen, then select **OK**, and press **Enter**.

8. Specify the **IP Protocol Version**, **Source IP Address**, and **Destination IP Address** from the **Input Source IP and Destination IP** screen to associate with the configuration. If settings are not specified, the previous settings are used. Select **OK** and press **Enter** to save setting selections and continue to **Code Point selection**.

9. Select the **Code Point** to use with this configuration from the **Code Point selection** screen, then select **OK**, and press **Enter**.

## Deleting a DSCP Configuration

To delete an existing DSCP configuration:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```

3. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   **Note:** The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

4. Select **DSCP Config** from the **Policy Configuration Menu** and press **Enter**.

5. Select **Edit DSCP Configuration** from the **DSCP Configuration Menu** and press **Enter**.

   All existing DSCP configurations are displayed.

6. Select the configuration you want to delete by pressing the space bar; more than one configuration can be deleted at a time. Select **OK**and press **Enter**. The selected configuration(s) are deleted.

**Note:** When a configuration is deleted for a network interface that has more than one configuration defined, priority is given to the most current remaining DSCP configuration regarding output packet processing.

## Syncing a DSCP Configuration

DSCP configurations on one server can be synced with other servers in the same cluster. It is recommended the sync be performed from the active server to all other servers (standby or standby and spare) in a one site or two site cluster.

To sync a DSCP configuration:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su – platcfg
   ```

3. If at the **admusr** prompt, enter:
   ```
   sudo su – platcfg
   ```

   **Note:** The dash (-) is required in the `su – platcfg` or the `sudo su – platcfg` command to ensure proper permissions.

4. Select **DSCP Config** from the **Policy Configuration Menu** and press **Enter**.

5. Select **Sync DSCP Configuration** from the **DSCP Configuration Menu** and press **Enter**.

   All existing DSCP configurations are displayed.

6. If the sync is performed from a server that is not the Active server, a warning message appears, giving you the option to abort the sync process. If you select **Yes** to continue, the sync process begins. Once the process is complete, a confirmation message screen is displayed.

   The configurations are copied to the other servers and take effect. The sync status is displayed for each remote server.

# Chapter

# 4

## Managing Certificates

**Topics:**

This chapter describes how to access the Platcfg utility to manage SSL security certificates, which allow two systems to interact with a high level of security.

# Description of Security Certificates

There are two types of security certificates used in a system: self-signed or signed by a 3$^{rd}$ party.

- Self-signed certificates are created locally on each server in platcfg, then synchronized throughout the system to allow encrypted communications between servers. Self-signed certificates are inherently less secure than 3$^{rd}$ party signed certificates, so they are not recommended for use in a production environment. Additionally, some external systems may not allow the use of self-signed certificates, which may necessitate the use of 3$^{rd}$ party certificates.

- A Certificate Signature Request (CSR) is created locally in the platcfg utility, then is sent to a 3$^{rd}$ party signing authority who generates a signed certificate based on your request. You then synchronize this certificate throughout the system.

The following terminology is related to the management of certificate.

**Table 4: Certificate Management Terminology**

| Term | Definition |
| --- | --- |
| Certificate | Used by SSL to verify a trusted server, also known as a Key. |
| CN (Common Name) | CN is the primary ID inside of a certificate. The Keytool allows you to set this. Keytool refers to the CN as First and Last Name. |
| First and Last Name | First and Last Name is the primary ID inside of a certificate, also know as the CN. First and Last Name is the way the Keytool refers to this ID. |
| Key | Used by SSL to verify a trusted server, also known as a Certificate. |

# Managing SSL Security Certificates

## Creating a Self-Signed Certificate

A Certificate, commonly known as a Key, is used by SSL to verify a trusted server. Certificate creation is performed on the local server, and depending on your implementation, on the remote server. This local certificate acts as a Private key for the local server.

Common Name (CN) is the primary ID inside of a certificate. The Keytool allows you to set this; however, the Keytool refers to the CN as First and Last Name.

To create a self-signed key:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```
3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```
4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) `su - root`

      **Note:** The **root** password is not requested.

   b) `su - platcfg`

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   **Note:** The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
7. Select **SSL Key Configuration** from the **Policy Configuration Menu** and press **Enter**.
8. Select **Configure keystore** from the **Configure SSL keys Menu** and press **Enter**.
9. Select **Create Self-Signed Key** from the**Operate keystore Menu** and press **Enter**.
10. Enter information on the **Keystore Parameters** screen.

    **Note:** `tomcat` must be used for the **Alias** field.

    **Note:** A unique cluster ID name should be used in the **First and Last Name** field (the CN value).

11. When finished, select **OK** and press **Enter**.

## Verifying a Self-Signed Certificate

Once an SSL certificate has been created, verify a certificate's attributes before attempting to import or export the certificate in order to create your secure connection. If the certificate on the host is not the same after it is imported into its peer, the secure connection will not be allowed.

To verify a Self-Signed certificate:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.
2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```
3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```
4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) `su - root`

      **Note:** The **root** password is not requested.

   b) `su - platcfg`

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

> **Note:** The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
7. Select **SSL Key Configuration** from the **Policy Configuration Menu** and press **Enter**.
8. Select **Configure keystore** from the **Configure SSL keys Menu** and press **Enter**.
9. Select **View key** and press **Enter**.
10. Enter the password (`changeit`), select **OK** and press **Enter**.
11. Select the certificate and press **Enter**.
12. Verify the certificate information in the **Verify Self-Signed Certificate** confirmation screen.

   The key portions of the certificate are the **Alias name**, **Owner**, and **Issuer**. These attributes are exported and imported to the other server to establish the secure HTTP session.

13. Select **Exit** and press **Enter**.


# Using a Local Certificate to Establish a Secure HTTP (https) Web-Browser Session

To ensure a safe and secure TCP connection between an end-user (PC Web-browser) and the CMP system, an https session can be created between the two by passing a predefined certificate to the end-user. Once the end-user accepts the certificate, the https session is created.



Web browsers function differently based on their configuration. Review your browser settings before using SSL certificates.

To force end-users to establish an HTTPS session with the CMP system:

1. Exchange and import SSL keys between the CMP and the workstation as described in
2. Enable the firewall on the CMP,
3. Enable prefer custom,
4. Create two customized firewall rules (one for port 80 and one for port 8080) where the allowed host is 0.0.0.0/32.

**Note:** Because the ports 80 and 8080 conflict with the factory rule that allows anyone access to these ports, using the prefer custom option will discard this rule, and instead use the custom rule which will allow only 0.0.0.0 to connect via 80 or 8080, which locks down the unencrypted http ports.

**Note:** For more information, refer to *Creating a Self-Signed Certificate* and *Configuring Firewall Settings*.

# Establishing a Secure Connection Between a CMP System and an MPE Device

To establish a secure connection between a CMP system and an MPE device, both the CMP system and the MPE device must exchange certificates. Refer to the example figure:



Within this figure, the SSL Certificate is shared within the cluster, and the following certificate exchange is done:

1. The CMP system creates a local certificate and exports the certificate to the MPE device.
2. The MPE device imports the peer certificate (local certificate created by the CMP system) into its trust store.
3. The MPE device creates a local certificate and exports the certificate to the CMP system.
4. The CMP system imports the peer certificate (local certificate created by the MPE device) into its trust store.

**Note:** Procedures used in this chapter may require the rebooting of one or more servers. Subsequently, for HA to operate correctly in a clustered system, the active server of the cluster must not be rebooted unless the cluster is in the **online** state. Before rebooting any server, check cluster status using the CMP GUI. If a cluster is labeled Degraded, but the server detail does not show any failed or disconnected equipment, the server is performing a database synchronization operation and until the synchronization process has completed, the standby server cannot perform as the active server.

When a new certificate is configured, the synchronization will cause HA on the standby server to restart.

SSL certificates are created on a per-cluster basis, and to ensure that the cluster has the same certificate installed, you should force a system synchronization.

## Exporting a Certificate Signed Request to the Policy Management Servers

Ensure that the local certificate signed request has been created on each server or cluster, as described in *Creating a Self-Signed Certificate*. Then, to export a certificate signed request, establish a secure connection between the CMP system and a Policy Management server:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.
2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```
3. If at the **camiant** prompt, to access a limited set of actions, enter:

```
su - platcfg
```

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

    a) `su - root`

        Note: The **root** password is not requested.

    b) `su - platcfg`

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

    Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
7. Select **SSL Key Configuration** from the **Policy Configuration Menu** and press **Enter**.
8. Select **Configure Keystore** from the **Configure SSL keys Menu** and press **Enter**.
9. Select **Export key** from the **Operate keystore Menu** and press **Enter**.
10. Enter the **Keystore Password** (`changeit`), select **OK** and press **Enter**.
11. Press **Enter** to accept the alias `tomcat` or enter the alias previously created for the certificate.
12. Select a certificate type of binary or ascii from the **Export Certificate** screen, then select **OK** and press **Enter**.
13.

Importing a Peer Certificate

Once you have exported the local certificate, import the peer certificate (this is the certificate that was exported from the other system):

Note: This procedure is used to import a certificate to the peer machine. This includes certificates generated by other servers including certificates signed by a third party or similar.

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.
2. If at the **root** prompt, enter:
   ```
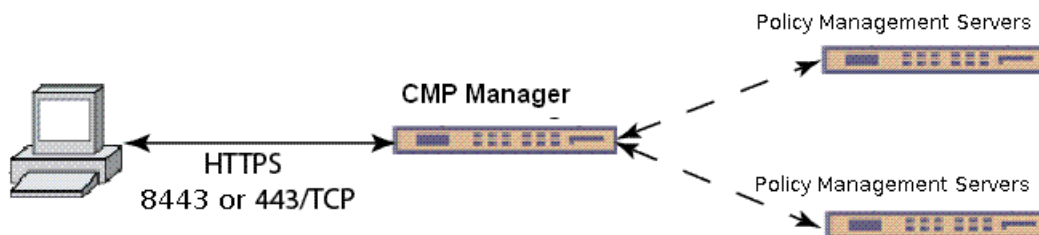   su - platcfg
   ```
3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```
4. Or if at the **camiant** prompt, to access a full set of actions, enter:

    a) `su - root`

        Note: The **root** password is not requested.

    b) `su - platcfg`

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

    Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.

7. Select **SSL Key Configuration** from the **Policy Configuration Menu** and press **Enter**.

8. Select **Configure cacerts** from the **Configure SSL keys Menu** and press **Enter**.

9. Select **Import trusted key** from the **Operate keystore Menu** and press **Enter**.

10. Enter the **Keystore Password** (`changeit`), select **OK** and press **Enter**.

11. You are prompted for the import location and alias for the certificate.

12. Enter the **Alias** for the certificate, as set previously for the **CN** name, select **OK** and press **Enter**. You are then presented with the certificate data for verification. Ensure that the **CN** name, **Owner**, and **Issuer** names of the input file name match that of the previous export file.

13. If the certificate data is correct, select **OK** and press **Enter**.

14. Log in to the CMP system, select the Policy Management server, and click the **Secure Connections** checkbox, located on the **Policy Server** tab. Refer to the CMP user's guide that corresponds to the mode of the system for more information.

Creating a CA Third-party Signed Certificate

Note: This section assumes that no SSL certificates have previously been generated on or imported into the servers. If there are pre-existing certificates on the system (besides the default `tomcat` certificate), please contact *My Oracle Support (MOS)* to determine their purpose and importance. Read this method in its entirety before starting the operations.

To create third-party certificates:

1. *Deleting an SSL Certificate*
2. *Generate a Certificate Signature Request*, *Export the Certificate Signature Request from the System*, *Import the Third-party Peer Certificates*
3. *Re-import the Third-party Signed Certificates*
4. *Synchronize and Reboot the Cluster*

Deleting an SSL Certificate

On most Policy Management servers, there is a pre-existing certificate in the store that has the alias `tomcat`. Before continuing with any of the other required certificate generation or import/export functions, delete this certificate:

Note: Also use these steps to delete an expired SSL certificate.

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) ```
   su - root
   ```

   Note: The **root** password is not requested.

b) `su - platcfg`

5. If at the **admusr** prompt, enter:
   `sudo su - platcfg`

   Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
7. Select **SSL Key Configuration** from the **Policy Configuration Menu**, and press **Enter**.
8. Select **Configure Keystore** from the **Configure SSL keys Menu** and press **Enter**.
9. Select **Delete key** from the **Operate keystore Menu** and press **Enter**.
10. Enter the Keystore Password (`changeit`), select **OK** and press **Enter.**
11. Select the certificate to be deleted (**tomcat** in this example) and press **Enter**.

Generating a Certificate Signature Request, Exporting for Signing, Re-importing, and Verifying

To generate the third-party signed local certificate:

1. *Generate a Certificate Signature Request*
2. *Export the Certificate Signature Request from the System*
3. *Re-import the Third-party Signed Certificates*
4. *Verifying a Self-Signed Certificate*

Generate a Certificate Signature Request

To generate a certificate signature request:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.
2. If at the **root** prompt, enter:
   `su - platcfg`
3. If at the **camiant** prompt, to access a limited set of actions, enter:
   `su - platcfg`
4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) `su - root`

      Note: The **root** password is not requested.

   b) `su - platcfg`

5. If at the **admusr** prompt, enter:
   `sudo su - platcfg`

   Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
7. Select **SSL Key Configuration** from the **Policy Configuration Menu** and press **Enter**.
8. Select **Configure keystore** from the **Configure SSL keys Menu** and press **Enter**.

9. Select **Create Certificate Signature Request (CSR)** from the **Operate keystore Menu** and press **Enter**.

10. Enter the **Keystore Password** (`changeit`), select **OK** and press **Enter**.

11. Select the desired certificate (`tomcat`, in this example) from the **Create CSR** screen to export for signature and press **Enter**.

    Note: The alias of the certificate is used later for re-importing the certificate after signing by a third party. Use an alias that allows the certificate to be identified with a specific system. Also of importance is the **Expiration** attribute, which should be set to a sufficiently large value so that the certificate does not expire before any peer certificates. A value preventing expiration before 2019 is recommended.

12. Select **OK** to accept the keystore destination, and press **Enter**. A confirmation screen is displayed.

Export the Certificate Signature Request from the System

To export a locally generated certificate signature request:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su – platcfg
   ```

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su – platcfg
   ```

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) `su – root`

      Note: The **root** password is not requested.

   b) `su – platcfg`

5. If at the **admusr** prompt, enter:
   ```
   sudo su – platcfg
   ```

   Note: The dash (-) is required in the `su – platcfg` or the `sudo su – platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.

7. Select **SSL Key Configuration** from the **Policy Configuration Menu** and press **Enter**.

8. Select **Configure keystore** from the **Configure SSL keys Menu** and press **Enter**.

9. From the **Policy Configuration Menu**, select **SSL Key Configuration** and press **Enter**.

10. Select **Export key** and from the **Operate keystore Menu** and press **Enter**.

11. Enter the **Keystore Password** (`changeit`), select **OK** and press **Enter**.

12. Select the desired certificate (`tomcat`, in this example) to export for signature and press **Enter**. You are prompted to export a **binary** or **ascii** certificate.

13. Select **OK** and press **Enter** to accept the default value of **binary**. The certificate is exported.

    After the certificate file is exported, provide it to the third party who signs and returns the certificate request.

Re-import the Third-party Signed Certificates

After the certificate has been signed by the third party, two certificate files are returned by them for importing into the Policy Management servers. One of these files is a signed local client certificate and the other is a certificate authority (CA), peer certificate. Both certificates must be imported into the system for proper SSL communication.

Note: It may necessary to edit the returned files to remove extraneous debugging information in the certificate. This must be accomplished using a Linux-based editor to preserve line termination style. The only contents that should be in the files are the blocks of data headlined by:

`----BEGIN CERTIFICATE-----`

and concluded by:

`-----END CERTIFICATE-----`

All other text above or below these blocks should be removed.

To remove extra text in the certificate files, a further modification needs to be made to the signed local client certificate. In order for the Policy Management servers to be able to import the local certificate successfully, the CA certificate must be merged into this file as well. To do this, copy the `BEGIN/END` certificate text block from the CA certificate and then paste the blocks into the local client certificate below the `BEGIN/END` certificate text block. The final result is the original local client certificate text block immediately followed by the certificate text block of the CA cert that was provided by the third-party signer. An example of what this should look like is as follows:

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAligAwIBAgIBBTANBgkqhkiG9w0BAQUFADCBjDELMAkGA1UEBhMCVVMx
<text removed>
gJeTRnZwMJEXv7lV85NGobVGqbluR94kIQazFP5HC2b2C0Q=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDjTCCAvagAwIBAgIJAJCKgXrXbhQ/MA0GCSqGSIb3DQEBBQUAMIGMMQswCQYD
<text removed>
YVPOATiFnrt1B9Qb1P8kW8lwPmG88Gg6nqttolhAnIi/lWBcp+QZfJMxPBcMkH2k7A==
-----END CERTIFICATE-----
```

Either copy these certificate files to the Policy Management server in advance, or store them somewhere on the network accessible via SCP. They can be imported back into the system to secure the communication channel with the third-party system. To import the certificates:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   `su – platcfg`

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   `su – platcfg`

4. Or if at the **camiant** prompt, to access a full set of actions, enter:
   a) `su – root`

   Note: The **root** password is not requested.

   b) `su – platcfg`

5. If at the **admusr** prompt, enter:
   `sudo su – platcfg`

Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.

7. Select **SSL Key Configuration** from the **Policy Configuration Menu** and press **Enter**.

8. Select **Configure keystore** from the **Configure SSL keys Menu** and press **Enter**.

9. First, import the local signed certificate. Select **Import trusted key** from the **Operate keystore Menu** and press **Enter**

10. Enter the **Keystore Password** (`changeit`), select OK and press Enter. You are prompted for the location of the certificate to be imported.

11. Select or enter the location where the certificate is located and the certificate alias name, then select **OK** and press **Enter**.

    The certificate data displays for verification. To avoid confusion, though they may be different, ensure that the **Owner** and **Issuer** names used for the certificate match the hostname of the server the certificate is being created on. If all certificate information is correct, the next operation is to import the CA certificate as a peer certificate.

    Note: The alias entered MUST match the alias originally used to Create the Certificate Request.

12. Next, import the CA signed certificate. Select **Import trusted key** from the **Operate cacerts Menu** and press **Enter**.

13. Enter the **Keystore Password** (`changeit`), select OK and press Enter. You are prompted for the location of the certificate to be imported.

14. Select or enter the location where the certificate is located and the certificate alias name, then select **OK** and press **Enter**.

    The certificate data displays for verification. To avoid confusion, though they may be different, ensure that the **Owner** and **Issuer** names used for the certificate match the hostname of the server the certificate is being created on. If all certificate information is correct, the next operation is to import the CA certificate as a peer certificate.

    Note: The alias entered MUST match the alias originally used to Create the Certificate Request.

Import the Third-party Peer Certificates

In addition to the certificates that were imported in section *Re-import the Third-party Signed Certificates*, you must also import a pair of peer certificates from the third party to connect to and communicate with their server (versus their client communicating with the Policy Management servers).

The third party will provide a set of new client and CA certificate files, both of which will be imported to the Policy Management servers as peer certificates.

Note: It may be necessary to edit the returned files to remove extraneous debugging-type information in the certificate. The only contents that should be in the files, are the blocks of data headlined by:

- `-----BEGIN CERTIFICATE-----`

and concluded by:

- `-----END CERTIFICATE-----`

All other text above or below these blocks should be removed.

To import the peer certificates, either copy these certificate files to the Policy Management servers in advance, or store them somewhere on the network accessible via SCP. To import the certificate:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) `su - root`

      Note: The **root** password is not requested.

   b) `su - platcfg`

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.

7. Select **SSL Key Configuration** from the **Policy Configuration Menu** and press **Enter**.

8. Select **Configure keystore** from the **Configure SSL keys Menu** and press **Enter**.

9. Select **Import trusted key** from the **Operate keystore Menu** and press **Enter**.

10. Enter the **Keystore Password** (`changeit`), select **OK** and press **Enter**. You are prompted for the location of the certificate to be imported.

11. Select or enter the location where the certificate is located and the certificate alias name, select **OK** and press **Enter**.

    Note: The alias entered here MUST match the alias originally used to Create the Certificate Request.

Synchronize and Reboot the Cluster

In order for the new certificates to take effect, all cluster servers must be synchronized and then rebooted for the certificates to take effect on the CMP system.

• To synchronize, refer to *Performing File Synchronization*.

• To reboot, refer to the CMP user's guide corresponding to the system mode.

Chapter

5

Synchronizing Files

Topics:

This chapter describes how and when to synchronize files in clusters.

Files should be synchronized after either of the following are configured:

- Routes (Routing Config)
- Firewall (Firewall)

Managing Cluster Sync Configurations

Use the **Cluster Sync Config** menu to manage cluster sync configurations:

- *Reading Destination from COMCOL*
- *Adding a Sync File*
- *Deleting a Sync File*

Reading Destination from COMCOL

To read the cluster sync destination from COMCOL:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) `su - root`

      Note: The **root** password is not requested.

   b) `su - platcfg`

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.

7. Select **Cluster File Sync** from the **Policy Configuration Menu** and press **Enter**.

8. Select **Cluster Sync Config** from the **Cluster Configuration Sync Menu** and press **Enter**.

9. Select **Read Destination from Comcol** from the **Config the Destination of Cluster Sync Menu** and press **Enter**.

Adding a Sync File

To add a new cluster sync configuration file:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

     a) `su - root`

       Note: The **root** password is not requested.

     b) `su - platcfg`

5. If at the **admusr** prompt, enter:
   `sudo su - platcfg`

   Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
7. Select **Cluster File Sync** from the **Policy Configuration Menu** and press **Enter**.
8. Select **Cluster Sync Config** from the **Cluster Configuration Sync Menu** and press **Enter**.
9. Select **Add Sync File** from the **Config the Destination of Cluster Sync Menu** and press **Enter**.
10. The Add a Sync File screen is displayed.
11. Enter data into the fields, where:

    1. **filename**--The name of the sync file.
    2. **remote file**--The name of the sync file if different at the remote site.
    3. **scope (cluster/site/clusterGroup)**--Lists where each file is to be synced:

       - **cluster**--Indicates access to all servers at all sites. Files that need to be in sync at all sites (such as certificates) should be listed as Cluster.
       - **site**--Indicates access to servers at the local site. IP-related files that may not be valid at other sites (such as firewall and static routes) should be listed as Site.
       - **clusterGroup**--Indicates access to all servers only in multiple CMP, MPE, or MRA clusters.

    4. **post script**--

12. Select **OK** and press **Enter**
    The new cluster sync configuration is saved.

Deleting a Sync File

To delete an existing cluster sync configuration file:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.
2. If at the **root** prompt, enter:
   `su - platcfg`
3. If at the **camiant** prompt, to access a limited set of actions, enter:
   `su - platcfg`
4. Or if at the **camiant** prompt, to access a full set of actions, enter:

        a) `su - root`

          Note: The **root** password is not requested.

        b) `su - platcfg`

5. If at the **admusr** prompt, enter:
   `sudo su - platcfg`

Note: The dash (-) is required in the `su – platcfg` or the `sudo su – platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
7. Select **Cluster File Sync** from the **Policy Configuration Menu** and press **Enter**.
8. Select **Cluster Sync Config** from the **Cluster Configuration Sync Menu** and press **Enter**.
9. Select **Delete Sync File** from the **Config the Destination of Cluster Sync Menu** and press **Enter**.
10. The **Main Routing Table** screen is displayed.

Displaying a Sync Configuration

Use this option to display the location of a sync configuration; this is useful when georedundancy is implemented. The Scope column lists where each file is being synced: Site indicates that the file is synced to servers at the local site, Cluster indicates that the file is synced to all servers at all sites. Files that must be in sync at all sites (like certificates) are listed as Cluster; IP-related files that may are not valid at other sites (like firewall and static routes) are listed as Site.

To display a sync configuration:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.
2. If at the **root** prompt, enter:
   `su – platcfg`
3. If at the **camiant** prompt, to access a limited set of actions, enter:
   `su – platcfg`
4. Or if at the **camiant** prompt, to access a full set of actions, enter:
   a) `su – root`

   Note: The **root** password is not requested.

   b) `su – platcfg`
5. If at the **admusr** prompt, enter:
   `sudo su – platcfg`

   Note: The dash (-) is required in the `su – platcfg` or the `sudo su – platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
7. Select **Cluster File Sync** from the **Policy Configuration Menu** and press **Enter**.
8. Select **Show Sync Config** from the **Cluster Configuration Sync Menu** and press **Enter**.
9. The Sync File screen is displayed.

Displaying a Sync Destination

To display a sync destination (hostname, IP address, and location):

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) ```su - root```

      Note: The **root** password is not requested.

   b) ```su - platcfg```

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   Note: The dash (-) is required in the ```su - platcfg``` or the ```sudo su - platcfg``` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
7. Select **Cluster File Sync** from the **Policy Configuration Menu** and press **Enter**.
8. Select **Show Sync Destination** from the **Cluster Configuration Sync Menu** and press **Enter**.
9. The Sync Destination screen is displayed.

Displaying a Sync Status

To display a cluster sync status:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) ```su - root```

      Note: The **root** password is not requested.

   b) ```su - platcfg```

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   Note: The dash (-) is required in the ```su - platcfg``` or the ```sudo su - platcfg``` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.
7. Select **Cluster File Sync** from the **Policy Configuration Menu** and press **Enter**.
8. Select **Show Sync Status** from the **Cluster Configuration Sync Menu** and press **Enter**.

9. **The Sync Status** screen is displayed.

Performing File Synchronization

Note: File synchronization (or cluster sync) copies configuration files from the target server to the remaining servers in the cluster. Performing a cluster sync restarts qp_procmgr on the target servers, so this action should only be performed from the Active server, otherwise a failover will occur. A warning displays on the screen before continuing with the sync, to help prevent this issue from occurring.

To perform the cluster file synchronization:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   `su - platcfg`

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   `su - platcfg`

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) `su - root`

      Note: The **root** password is not requested.

   b) `su - platcfg`

5. If at the **admusr** prompt, enter:
   `sudo su - platcfg`

   Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.

7. Select **Cluster File Sync** from the **Policy Configuration Menu** and press **Enter**.

8. Select **Start Synchronizing** from the **Cluster Configuration Sync Menu** and press **Enter**.

   Note: A warning message is displayed, indicating that a cluster sync restarts qp_procmgr on the target servers.

    Warning: This action should only be performed from the Active server, otherwise a failover will occur.

9. Select **OK** and press **Enter** to continue. Configuration files are synced to the other servers in the cluster, and qp_procmgr is restarted on the target servers.

Chapter

6

Custom Ethtool Options

Topics:

This chapter describes how to manually customize Ethtool options, including auto-negotiation, speed, and duplex transmission parameters, on the interface controller for a wireline network installation.

Configuration settings are persistent over system upgrades and reboots.

Editing Network Interface Ethernet Parameters (Policy Configuration Method)

This section describes how to edit Network Interface Ethernet parameter settings using the Policy Configuration method.

To edit network interface ethernet parameter settings:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) `su - root`

      Note: The **root** password is not requested.

   b) `su - platcfg`

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.

7. Select **Network Interfaces ETHTOOL_OPTS** from the **Policy Configuration Menu** and press **Enter**.

8. Select a network from the list on the **Network Interfaces List Menu** and press **Enter**.

   Each line in this display represents a physical interface (OAM, SIGA or SIGB) using logical names instead of physical names. If multiple logical interfaces share a physical interface, those interfaces are grouped on a single line.

9. Select **Set EthTool Options of** *linkname* from the **Interface** *linkname* **Menu** and press **Enter**.

10. Select from the options on the **Edit** *linkname* **Link Options** screen, then select **OK** and press **Enter**. Selection changes are made on both devices of a bond interface at the same time.

Notes for setting link options:

1. The **Speed** is configurable only when the device supports **100baseT/Full**. HP ProLiant BL* (C-Class) eth01/eth02 does not support **100baseT/Full**, so the speed is not configurable for C-Class bond0.

2. The physical device might support several **Speed** modes, but **100baseT/Full** is the only candidate in the Platcfg gui.

3. If the interface is a bond device, then the **Speed** and duplex settings for the active secondary device is fetched from kernel and displayed on the Platcfg gui. If any secondary device of the bond interface is not linked, the bond interface is not configurable.

---

4. If the interface is a bond device, then primary_reselect is configurable.

5. If the two secondary devices in a bond device are running in different modes, a warning message is displayed before the window is updated.

6. It is strongly recommended that the auto-negotiation option is set to **autoneg on** at both ends. If it is set to **autoneg off**, a warning message is displayed when **OK** is selected.

7. The link behavior is undefined if one end has**autoneg on** while the other end has **autoneg off**.

8. When **OK** is selected, the setting is applied to the interface immediately. For a bond device, the setting is applied to both of the secondary devices.

9. If the applied mode is not compatible with the switch, it is possible that the link goes down. This utility does not try to detect or correct this case.

Table 5: Ethtool speed compatibility matrix

Speed Setting: server/switch	Default (autoneg on)	100baseT/Full, Autoneg on	100baseT/Full, Autoneg off
Default (autoneg on)	OK (case 1)	OK (case 2)	Undefined
100baseT/Full, Autoneg on	OK (case 2)	OK (case 3)	Undefined
100baseT/Full, Autoneg off	Undefined	Undefined	OK (case 4)

Editing Network Interface Ethernet Parameters (TPD Method)

This section describes how to edit network interface ethernet parameter settings using the TPD platform method. If none of the options are specified, auto-negotiation is assumed.

To edit network interface ethernet parameter settings:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```

3. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

4. Select **Network Configuration** from the **Main Menu - Network Configuration** and press **Enter**.

5. Select **Network Interfaces** from the **Network Configuration Menu** and press **Enter**.

6. Select **Edit an Interface** from the **Network Interfaces Menu** and press **Enter**.

7. Select a Network Interface name from the **Connection to edit Menu** choices.

8. To continue to the network **Interface Options** menu, select **Edit** from the **Options** menu on the screen. Otherwise, select **Exit** to return to the previous menu.

9. Select the required speed and duplex options from the **Interface Options** menu, select **OK** and press **Enter.**

Chapter

7

Performing System and Server Backups and Restores

Topics:

This chapter describes how to perform system and server backups and restores.

Performing a Server Backup

The server backup contains OS-level information that is configured in the platcfg utility such as IP, NTP, and DNS addresses. This type of backup is unique to a server and should be created for every server within a cluster.

To perform a server backup:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) ```su - root```

      Note: The **root** password is not requested.

   b) ```su - platcfg```

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   Note: The dash (-) is required in the ```su - platcfg``` or the ```sudo su - platcfg``` command to ensure proper permissions.

6. Select the **Policy Configuration** from the **Main Menu** and press **Enter**.

7. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**. Note that **System Backup** and **System Restore** are only allowed on a CMP server or MA Server, so these options do not appear on the menu for other types of servers.

8. Select **Server Backup** from the **Backup and Restore Menu** and press **Enter**.

9. You are prompted to enter the ISO path to save the backup file.

   Accept the default backup directory or enter a desired directory. The file naming convention used for the backup file is:

   <hostname>-camiant-*<release>*-serverbackup-*<datetime>*.iso

10. When you are done, select **OK** and press **Enter**. The backup is created.

Performing a System Backup

The system backup contains application-level information such as Topology, Network Element, and Policy Management configurations that are configured in the CMP system. This backup saves the information for an entire deployment and should be created on the active server of the Primary CMP cluster.

When the backup file is created, the file contains a specific name and is located in a specific directory. Transfer this backup to the FTP server and the PMAC server.

To perform a system backup:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   `su - platcfg`

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   `su - platcfg`

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) `su - root`

      Note: The **root** password is not requested.

   b) `su - platcfg`

5. If at the **admusr** prompt, enter:
   `sudo su - platcfg`

   Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.

7. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.

8. Select **System Backup** from the **Backup and Restore Menu** and press **Enter**.

9. You are prompted to enter the tar.gz path to save the backup file.

   Accept the default backup directory or enter a desired directory. The file naming convention used for the backup file is:

   <hostname>-camiant-*<release>*-systembackup-*<datetime>*.tar.gz

10. When you are done, select **OK** and press **Enter**. The backup is created.

Displaying Backup Files

To display current local archive and remote archive backup files:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   `su - platcfg`

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   `su - platcfg`

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) `su - root`

      Note: The **root** password is not requested.

b) `su – platcfg`

5. If at the **admusr** prompt, enter:
   `sudo su – platcfg`

   Note: The dash (-) is required in the `su – platcfg` or the `sudo su – platcfg` command to ensure proper permissions.

6. Select the **Policy Configuration** from the **Main Menu** and press **Enter**.

7. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.

8. Select **Display Backup Files** from the **Backup and Restore Menu** and press **Enter**.

9. Make a selection from the **Display Backup Files Menu** to display either the local archive or the remote archive:

   a) Select **Display Local Archive** and press **Enter**.
   b) Select **Display Remote Archive** and press **Enter**.

Configuring Local Archive Settings

You can store up to three archives for both the server and system backup files. To configure local archive settings:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   `su – platcfg`

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   `su – platcfg`

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) `su – root`

      Note: The **root** password is not requested.

   b) `su – platcfg`

5. If at the **admusr** prompt, enter:
   `sudo su – platcfg`

   Note: The dash (-) is required in the `su – platcfg` or the `sudo su – platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.

7. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.

8. Select **Local Archive Settings** from the **Backup and Restore Menu** and press **Enter**.

9. You are prompted to specify the number of archives for the server and system backups. Note that the server backup option will only appear on a CMP system or MA Server.

10. Select the number of backups to keep for each archive. When finished, select **OK** and press **Enter**.

Configuring Remote Archive Settings

You can store system and server archives remotely. These archives have separate directories for each host. This section describes how to cmanage remotely stored systems and server archives.

Configuring a Remote Archive

To configure a remote archive:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) `su - root`

      Note: The **root** password is not requested.

   b) `su - platcfg`

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select **Policy Configuration** from the **Main Menu** and press **Enter**.

7. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.

8. Select **Remote Archive Settings** from the **Backup and Restore Menu** and press **Enter**.

9. You are prompted for the archive type (server or system) to configure. Note that the server backups option only appears on a CMP system or MA Server. Select **Remote Archive for Server Backups** or **Remote Archive for System Backups** from the **Remote Archive Settings Menu** and press **Enter**.

10. Select **Add Remote Archive** or **Remote Archive Settings Menu** from the 2nd **Remote Archive Settings Menu** and press **Enter**.

11. Enter remote access information in the screen that displays:

12. When you are done, select **OK** and press **Enter**.

Editing a Remote Archive Configuration

To edit a remote archive configuration:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```
4. Or if at the **camiant** prompt, to access a full set of actions, enter:
   a) ```su - root```

      Note: The **root** password is not requested.

   b) ```su - platcfg```

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   Note: The dash (-) is required in the ```su - platcfg``` or the ```sudo su - platcfg``` command to ensure proper permissions.

6. Select either **Remote Archive for Server Backups** or **Remote Archive for System Backups** from the **Remote Archive Settings Menu** and press **Enter**.
7. Select **Edit Remote Archive** from the **Remote Archive Settings Menu** and press **Enter**.
8. Select the remote archive to edit from the **Remote Archives Menu** and press **Enter**.
9. Enter all remote archive information and when finished, select **OK** and press **Enter**.

Deleting a Remote Archive Configuration

To delete a remote archive configuration:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.
2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```
3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```
4. Or if at the **camiant** prompt, to access a full set of actions, enter:
   a) ```su - root```

      Note: The **root** password is not requested.

   b) ```su - platcfg```

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   Note: The dash (-) is required in the ```su - platcfg``` or the ```sudo su - platcfg``` command to ensure proper permissions.

6. Select either **Remote Archive for Server Backups** or **Remote Archive for System Backups** from the **Remote Archive Settings Menu** and press **Enter**.
7. Select **Delete Remote Archive** and press **Enter**.
8. Select the remote archive to edit from the **Remote Archives Menu** and press **Enter**.
9. Select **Yes** or **No** from the **Confirm deletion** dialog box and press **Enter**. If **Yes** is selected, the remote archive is deleted; if **No** is selected, the **Remote Archive Settings Menu** is redisplayed.

Displaying a Remote Archive Configuration

To display a remote archive configuration:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) ```su - root```

   > **Note:** The **root** password is not requested.

   b) ```su - platcfg```

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   > **Note:** The dash (-) is required in the ```su - platcfg``` or the ```sudo su - platcfg``` command to ensure proper permissions.

6. Select either **Remote Archive for Server Backups** or **Remote Archive for System Backups** from the **Remote Archive Settings Menu** and press **Enter**.

7. Select **Display Remote Archive** from the 2nd **Remote Archive Settings Menu** and press **Enter**.

8. Either the **Display Remote Archive For Server-Backup** or the **Display Remote Archive For System-Backup** screen is displayed.

Scheduling Backups

You can configure your system or server to conduct backups on a scheduled basis. This section describes how to manage scheduled backups.

Note: When **Weekly** is selected, the **Days of the Month** field is ignored, and when **Monthly** is selected, the **Days of the Week** field is ignored.

Scheduling a Backup

To schedule a backup:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

a) `su - root`

   Note: The **root** password is not requested.

b) `su - platcfg`

5. If at the **admusr** prompt, enter:
   `sudo su - platcfg`

   Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select the **Policy Configuration** from the **Main Menu** and press **Enter**.
7. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.
8. Select **Scheduled Backup Settings** from the **Backup and Restore Menu** and press **Enter**.
9. You are prompted for the backup type (server or system) to be scheduled. Select either **Scheduled Backup for Server Backups** or **Scheduled Backup for System Backups** from the **Scheduled Backup Settings Menu** and press **Enter**.
10. Select **Add Schedule** from the **Scheduled Backup for server backups Menu** and press **Enter**.
11. Enter the following information:

    - **Name**--A unique name identifying the scheduled backup.
    - **Min**--Minute to perform backup. Valid values are 0 to 59, with a default of 0.
    - **Hour**--Hour to perform backup. Valid values are 0 to 23, with a default of 0.
    - **Weekly**--Select to have the backup performed weekly. When **Weekly** is selected, the **Days of the Month** value is ignored. The default backup is performed weekly.
    - **Days of Week**--Specifies that the backup is performed on specific days. Valid values are sun, mon, tue, wed, thu, fri, and sat.
    - **Monthly**--Select to have the backup performed monthly. When **Monthly** is selected, the **Days of the Week** value is ignored.
    - **Days of the Month**--Day to perform backup. Valid values include 1 and 15.

12. When you have finished, select **OK** and press **Enter**.

Editing a Scheduled Backup

To edit a scheduled backup:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.
2. If at the **root** prompt, enter:
   `su - platcfg`
3. If at the **camiant** prompt, to access a limited set of actions, enter:
   `su - platcfg`
4. Or if at the **camiant** prompt, to access a full set of actions, enter:
   a) `su - root`

      Note: The **root** password is not requested.

   b) `su - platcfg`
5. If at the **admusr** prompt, enter:

```
sudo su - platcfg
```

Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select the **Policy Configuration** from the **Main Menu** and press **Enter**.
7. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.
8. Select **Scheduled Backup Settings** from the **Backup and Restore Menu** and press **Enter**.
9. Select either **Scheduled Backup for Server Backups** or **Scheduled Backup for System Backups** from the **Scheduled Backup Settings Menu** and press **Enter**.
10. Select **Edit Schedule** from the **Scheduled Backup for server backups Menu** or from the **Scheduled Backup for system backups Menu** and press **Enter**.
11. Edit the following Information:

    - **Name**--A unique name identifying the scheduled backup.
    - **Min**--Minute to perform backup. Valid values are 0 to 59, with a default of 0.
    - **Hour**--Hour to perform backup. Valid values are 0 to 23, with a default of 0.
    - **Weekly**--Select to have the backup performed weekly. When **Weekly** is selected, the **Days of the Month** value is ignored. The default backup is performed weekly.
    - **Days of Week**--Specifies that the backup is performed on specific days. Valid values are sun, mon, tue, wed, thu, fri, and sat.
    - **Monthly**--Select to have the backup performed monthly. When **Monthly** is selected, the **Days of the Week** value is ignored.
    - **Days of the Month**--Day to perform backup. Valid values include 1 and 15.

12. When you have finished, select **OK** and press **Enter**.

Deleting a Scheduled Backup

To delete a scheduled backup:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.
2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```
3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```
4. Or if at the **camiant** prompt, to access a full set of actions, enter:
   a) `su - root`

      Note: The **root** password is not requested.

   b) `su - platcfg`

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select the **Policy Configuration** from the **Main Menu** and press **Enter**.

7. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.

8. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.

9. Select **Scheduled Backup Settings** from the **Backup and Restore Menu** and press **Enter**.

10. Select either **Scheduled Backup for Server Backups** or **Scheduled Backup for System Backups** from the **Scheduled Backup Settings Menu** and press **Enter**.

11. Select **Delete Schedule** from the **Scheduled Backup for server backups Menu** or from the **Scheduled Backup for system backups Menu** and press **Enter**.

12. When you have finished, select **OK** and press **Enter**. The scheduled backup is deleted.

Displaying a Scheduled Backup

To a display scheduled backup:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```

3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```

4. Or if at the **camiant** prompt, to access a full set of actions, enter:

   a) `su - root`

      Note: The **root** password is not requested.

   b) `su - platcfg`

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select the **Policy Configuration** from the **Main Menu** and press **Enter**.

7. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.

8. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.

9. Select **Scheduled Backup Settings** from the **Backup and Restore Menu** and press **Enter**.

10. Select **Display Scheduled Backups** from the **Scheduled Backup Settings Menu** and press **Enter**. The scheduled backups are displayed.

Performing a System Restore

The system restore option restores the Policy Management information that is unique to this system, including topology, policies, and feature configuration.

To perform a system restore:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.

2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```
3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```
4. Or if at the **camiant** prompt, to access a full set of actions, enter:
   a) `su - root`

      Note: The **root** password is not requested.

   b) `su - platcfg`

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select the **Policy Configuration** from the **Main Menu** and press **Enter**.
7. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.
8. Select **System Restore** from the **Backup and Restore Menu** and press **Enter**.
9. Enter the path that contains the backup and select either **Application** or **Full** for the type of restore.

Performing a Server Restore

The server restore restores the OS information unique to the server. This operation applies the data from a previously saved server configuration backup file.

To perform a server restore:

1. Log in to your system as **root** if logging in from the system console. Otherwise, use SSH to access your system remotely as **camiant** or **admusr**.
2. If at the **root** prompt, enter:
   ```
   su - platcfg
   ```
3. If at the **camiant** prompt, to access a limited set of actions, enter:
   ```
   su - platcfg
   ```
4. Or if at the **camiant** prompt, to access a full set of actions, enter:
   a) `su - root`

      Note: The **root** password is not requested.

   b) `su - platcfg`

5. If at the **admusr** prompt, enter:
   ```
   sudo su - platcfg
   ```

   Note: The dash (-) is required in the `su - platcfg` or the `sudo su - platcfg` command to ensure proper permissions.

6. Select the **Policy Configuration** from the **Main Menu** and press **Enter**.
7. Select **Backup and Restore** from the **Policy Configuration Menu** and press **Enter**.
8. Select **Server Restore** from the **Backup and Restore Menu** and press **Enter**.

9. Enter the path that contains the backup, select **OK,** and press **Enter**. The system restores to the
   backup version specified.

Glossary

B

BoD

Bandwidth on Demand

An application that provides dynamic allocation of bandwidth; for example, a broadband speed promotion.

C

CA

Certificate Authority: An entity that issues digital certificates

CMP

Configuration Management Platform

A centralized management interface to create policies, maintain policy libraries, configure, provision, and manage multiple distributed MPE policy server devices, and deploy policy rules to MPE devices. The CMP has a web-based interface.

D

DNS

Domain Name System

A system for converting Internet host and domain names into IP addresses.

DSCP

Differentiated Services Code Point

Provides a framework and building blocks to enable deployment of scalable service discrimination in the internet. The differentiated services are realized by mapping the code point contained in a field in the IP packet header to a

D

particular forwarding treatment or per-hop behavior (PHB). Differentiated services or DiffServ is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying and managing network traffic and providing quality of service (QoS) on modern IP networks.

H

HTTP   Hypertext Transfer Protocol

I

IP   Intelligent Peripheral

Internet Protocol - IP specifies the format of packets, also called datagrams, and the addressing scheme. The network layer for the TCP/IP protocol suite widely used on Ethernet networks, defined in STD 5, RFC 791. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and re-assembly through the data link layer.

ISO   International Standards Organization

M

MA   Management Agent

MDF   Message Distribution Function. A standalone hardware system, situated between a Mediation Gateway and an Oracle Communications subscriber profile repository (SPR), that exchanges

M

messages between a Mediation
Gateway and SPR systems

MPE   Multimedia Policy Engine

A high-performance,
high-availability platform for
operators to deliver and manage
differentiated services over
high-speed data networks. The
MPE includes a
protocol-independent policy rules
engine that provides authorization
for services based on policy
conditions such as subscriber
information, application
information, time of day, and edge
resource utilization.

MRA   Multi-Protocol Routing Agent -
Scales the Policy Management
infrastructure by distributing the
PCRF load across multiple Policy
Server devices.

N

NTP   Network Time Protocol

P

PMAC   Platform Management &
Configuration (also referred to as
PM&C)

Provides hardware and platform
management capabilities at the site
level for the Tekelec Platform. The
PMAC application manages and
monitors the platform and installs
the TPD operating system from a
single interface.

V

VIP   Virtual IP Address

V

Virtual IP is a layer-3 concept employed to provide HA at a host level. A VIP enables two or more IP hosts to operate in an active/standby HA manner. From the perspective of the IP network, these IP hosts appear as a single host.

VLAN

Virtual Local Area Network

A logically independent network. A VLAN consists of a network of computers that function as though they were connected to the same wire when in fact they may be physically connected to different segments of a LAN. VLANs are configured through software rather than hardware. Several VLANs can co-exist on a single physical switch.