Oracle® Communications Diameter Signaling Router

IP Front End (IPFE) User's Guide

E73317 Revision 01

August 2016

ORACLE®

Oracle Communications Diameter Signaling Router IP Front End (IPFE) User's Guide

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Topics:

This *IP Front End (IPFE) User's Guide* and Help provide an overview of IPFE functions and procedures to use to configure IPFE. The contents include sections on the scope, audience, and organization of the documentation, and how to contact Oracle for assistance.

Overview

The IPFE documentation provides information about IPFE functions, how to use the GUI and the following procedures to configure an IPFE:

- Specify IPFE Configuration Options
- Configure IPFE Target Sets

Scope and Audience

The IP Front End (IPFE) documentation is intended for anyone responsible for the configuration of the IPFE. Users of this guide must have a working knowledge of telecommunications, of network installations and the product that uses the IPFE functions.

Manual Organization

This manual is organized into the following chapters:

- *Introduction* contains general information about the IPFE help documentation, the organization of this manual, and how to get technical assistance.
- *Introduction to IPFE* provides information about the IPFE function.
- *IPFE Configuration Options* describes how to manage your IPFE configuration.
- *IPFE Target Sets Configuration* describes how to assign a list of application server IP address to a Target Set and associate the Target Set with an IPFE pair.

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: (This icon and text indicate the possibility of *personal injury*.)

Icon	Description
	Warning: (This icon and text indicate the possibility of *equipment damage*.)
	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

User Interface Introduction

Topics:

This section describes the organization and usage of the application's user interface. In it you can find information about how the interface options are organized, how to use widgets and buttons, and how filtering and other page display options work.

User Interface Organization

The user interface is the central point of user interaction within an application. It is a Web-based graphical user interface (GUI) that enables remote user access over the network to an application and its functions.

The core framework presents a common set of Main Menu options that serve various applications. The common Main Menu options are:

- Administration
- Configuration
- Alarm and Events
- Security Log
- Status & Manage
- Measurements
- Help
- Legal Notices
- Logout

Applications, such as DSR, build upon this framework to present features and functions. For example, the DSR Network OAM GUI may present the following Main Menu options in addition to the common options:

- Communication Agent
- Diameter Common
- Diameter
- Policy and Charging
- MAP-Diameter IWF
- SBR
- RADIUS

The DSR System OAM GUI may present even more Main Menu options as listed below. The end result is a flexible menu structure that changes according to the application needs and features activated.

- Transport Manager
- SS7/Sigtran
- RBAR
- FABR
- IPFE
- GLA
- Policy and Charging
- MAP-Diameter IWF
- SBR
- RADIUS
- Mediation

Note that the DSR System OAM Main Menu options differ from the Network OAM options. Some Main Menu options are configurable from the DSR Network OAM server and view-only from the System OAM server. This remains true for other applications.

User Interface Elements

Table 2: User Interface Elements describes elements of the user interface.

Table 2: User Interface Elements

Element	Location	Function
Identification Banner	Top bar across the web page	Displays the company name, product name and version, and the alarm panel.
Session Banner	Next bar across the top of the web page	The left side of the banner just above the Main Menu provides the following session information: • The name of the machine to which the user is connected, and whether the user is connected via the VIP or directly to the machine. • The HA state of the machine to which the user is connected. • The role of the machine to which the user is connected. The right side of the banner: • Shows the user name of the currently logged-in user. • Provides a link to log out of the GUI.
Main Menu	Left side of screen, under banners	A tree-structured menu of all operations that can be performed through the user interface. The plus character (+) indicates a menu item contains subfolders. • To display submenu items, click the plus character, the folder, or anywhere on the same line. • To select a menu item that does not have submenu items, click on the menu item text or its associated symbol.
Work Area	Right side of panel under status	Consists of three sections: Page Title Area, Page Control Area (optional), and Page Area. • Page Title Area: Occupies the top of the work area. It displays the title of the current page being displayed, date and time, and includes a link to context-sensitive help. • Page Control Area: Located below the Page Title Area, this area shows controls for the Page Area (this area is optional). When available as an option, filter controls display in this area. The Page Control Area contains the optional layout element toolbar, which displays different elements depending on which GUI page is selected. For more information, see *Optional Layout Element Toolbar*. • Page Area: Occupies the bottom of the work area. This area is used for all types of operations. It displays all options, status, data, file, and query screens. Information

Element	Location	Function
		or error messages are displayed in a message box at the top of this section. A horizontal and/or vertical scroll bar is provided when the displayed information exceeds the page area of the screen. When a user first logs in, this area displays the application user interface page. The page displays a user-defined welcome message. To customize the message, see *Customizing the Login Message*.

Main Menu Options

Table 3: Main Menu Options describes all main menu user interface options.

Note: The menu options can differ according to the permissions assigned to a user's log-in account. For example, the Administration menu options do not appear on the screen of a user who does not have administrative privileges.

Note: Some menu items are configurable only on the Network OAM and view-only on the System OAM; and some menu options are configurable only on the System OAM.

Note: Some features do not appear in the main menu until the features are activated.

Table 3: Main Menu Options

Menu Item	Function
Administration	The Administration menu allows the user to: • General Options. Configure options such as password history and expiration, login message, welcome message, and the number of failed login attempts before an account is disabled • Set up and manage user accounts • Configure group permissions • View session information • Manage sign-on certificates • Authorize IP addresses to access the user interface • Configure SFTP user information • View the software versions report • Upgrade management including backup and reporting • Authenticate LDAP servers • Configure SNMP trapping services • Configure an export server • Configure DNS elements
Configuration	On the NOAM, allows the user to configure: • Network Elements • Network Devices • Network Routes

Menu Item	Function
	• Services • Servers • Server Groups • Resource Domains • Places • Place Associations • Interface and Port DSCP
Alarms and Events	Allows the user to view: • Active alarms and events • Alarm and event history • Trap log
Security Log	Allows the user to view, export, and generate reports from security log history.
Status & Manage	Allows the user to monitor the individual and collective status of Network Elements, Servers, HA functions, Databases, KPIs, system Processes, and Tasks. The user can perform actions required for server maintenance, database management, data, and ISO file management.
Measurements	Allows the user to view and export measurement data.
Transport Manager (optional)	On the SOAM, allows the user to configure adjacent nodes, configuration sets, or transports. A maintenance option allows the user to perform enable, disable, and block actions on the transport entries.
Communication Agent (optional)	Allows the user to configure Remote Servers, Connection Groups, and Routed Services. The user can perform actions to enable, disable, and block connections. Also allows the user to monitor the status of Connections, Routed Services, and HA Services.
SS7/Sigtran (optional)	On the SOAM, allows the user to configure various users, groups, remote signaling points, links, and other items associated with SS7/Sigtran; perform maintenance and troubleshooting activities; and provides a command line interface for bulk loading SS7 configuration data.
Diameter Common (optional)	Allows the user to view or configure: • Dashboard, configure on the NOAM; view on both OAMs • Network Identifiers on the SOAM - MCC Ranges • Network Identifiers on the NOAM - MCCMNC and MCCMNC Mapping • MPs (on the SOAM) - editable Profile parameters and Profile Assignments The DSR Bulk Import and Export functions are available on both OAMs for the data configured on that OAM.
Diameter (optional)	Allows the user to configure, modify, and monitor Diameter routing: • On the NOAMP, Diameter Topology Hiding and Egress Throttle List configuration

Menu Item	Function
	• On the SOAM, Diameter Configuration, Maintenance, Reports, Troubleshooting with IDIH, AVP Dictionary, and Diameter Mediation configuration
RBAR (Range-Based Address Resolution) (optional)	Allows the user to configure the following Range-Based Address Resolution (RBAR) settings: • Applications • Exceptions • Destinations • Address Tables • Addresses • Address Resolutions • System Options This is accessible from the SOAM only.
FABR (Full Address Based Resolution) (optional)	Allows the user to configure the following Full Address Based Resolution (FABR) settings: • Applications • Exceptions • Default Destinations • Address Resolutions • System Options This is accessible from the SOAM only.

Policy and Charging (optional)	On the NOAMP, allows the user to perform configuration tasks, edit options, and view elements for:
	• General Options
	• Access Point Names
	• Policy DRA
	  • PCRF Pools
	  • PCRF Sub-Pool Selection Rules
	  • Network-Wide Options
	• Online Charging DRA
	  • OCS Session State
	  • Realms
	  • Network-Wide Options
	• Alarm Settings
	• Congestion Options
	Additionally on the NOAMP, users are allowed to perform maintenance tasks, edit options, and view elements for:
	• Maintenance
	  • SBR Database Status

Menu Item	Function

	• SBR Status
	• SBR Database Reconfiguration Status
	• Policy Database Query
	
	On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for:
	• General Options
	• Access Point Names
	• Policy DRA
	  • PCRFs
	  • Binding Key Priority
	  • PCRF Pools
	  • PCRF Pool to PRT Mapping
	  • PCRF Sub-Pool Selection Rules
	  • Policy Clients
	  • Suspect Binding Removal Rules
	  • Site Options
	• Online Charging DRA
	  • OCSs
	  • CTFs
	  • OCS Session State
	  • Realms
	• Error Codes
	• Alarm Settings
	• Congestion Options

Gateway Location Application (optional)	On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for: • Exceptions • Options GLA can deploy with Policy DRA (in the same DA-MP or a separate DA-MP).
IPFE (optional)	Allows the user to configure IP Front End (IPFE) options and IP List TSAs. This is accessible from the SOAM server only.
MAP-Diameter Interworking (optional)	On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for the DM-IWF DSR Application: • DM-IWF Options • Diameter Exception On the NOAMP, allows the user to perform configuration tasks, edit options, and view elements for the MD-IWF SS7 Application:

Menu Item	Function
	• MD-IWF Options • Diameter Realm • Diameter Identity GTA • GTA Range to PC • MAP Exception • CCNDC Mapping
RADIUS (optional)	Allows the user to perform configuration tasks, edit system options, and view elements for: • Network Options • Message Authenticator Configuration Sets • Shared Secret Configuration Sets • Ingress Status Server Configuration Sets • Message Conversion Configuration Sets • NAS Node

SBR (optional)	Allows the user to perform configuration tasks, edit system options, and view elements for:
	• SBR Databases
	• SBR Database Resizing Plans
	• SBR Data Migration Plans
	Additionally, on the NOAMP, users are allowed to perform maintenance tasks, edit options, and view elements for:
	• Maintenance
	  • SBR Database Status
	  • SBR Status
	  • SBR Database Reconfiguration Status

Help	Launches the Help system for the user interface
Legal Notices	Product Disclaimers and Notices
Logout	Allows the user to log out of the user interface

Missing Main Menu options

Permissions determine which Main Menu options are visible to users. Permissions are defined through the **Group Administration** page. The default group, **admin**, is permitted access to all GUI options and functionality. Additionally, members of the **admin** group set permissions for other users.

Main Menu options vary according to the group permissions assigned to a user's account. Depending on your user permissions, some menu options may be missing from the Main Menu. For example, Administration menu options do not appear on your screen if you do not have administrative

permissions. For more information about user permissions, see *Group Administration* in the OAM section of the online help, or contact your system administrator.

Common Graphical User Interface Widgets

Common controls allow you to easily navigate through the system. The location of the controls remains static for all pages that use the controls. For example, after you become familiar with the location of the display filter, you no longer need to search for the control on subsequent pages because the location is static.

Supported Browsers

This application supports the use of Microsoft® Internet Explorer 8.0, 9.0, or 10.0.

System Login Page

Access to the user interface begins at the System Login page. The System Login page allows users to log in with a username and password and provides the option of changing the password upon login. The System Login page also features a date and time stamp reflecting the time the page was last refreshed. Additionally, a customizable login message appears just below the **Log In** button.

The user interface is accessed via HTTPS, a secure form of the HTTP protocol. When accessing a server for the first time, HTTPS examines a web certificate to verify the identity of the server. The configuration of the user interface uses a self-signed web certificate to verify the identity of the server. When the server is first accessed, the supported browser warns the user that the server is using a self-signed certificate. The browser requests confirmation that the server can be trusted. The user is required to confirm the browser request to gain access.

Customizing the Login Message

Before logging in, the **System Login** page appears. You can create a login message that appears just below the **Log In** button on the **System Login** page.

Figure 1: Oracle System Login

1. From the **Main Menu**, click **Administration** > **General Options**.
   The **General Options Administration** page appears.
2. Locate **LoginMessage** in the **Variable** column.
3. Enter the login message text in the **Value** column.
4. Click **OK** or **Apply** to submit the information.
   A status message appears at the top of the Configuration Administration page to inform you if the operation was successful.

The next time you log in to the user interface, the login message text displays.

Accessing the DSR Graphical User Interface

In a DSR, some configuration is done at the NOAM server, while some is done at the SOAM server. Because of this, you will access the DSR graphical user interface (GUI) from two servers. Certificate Management (Single Sign-On) can be configured to simplify accessing the DSR GUI on the NOAM and the SOAM.

For information on configuring Single Sign-On certificates, see **OAM** > **Administration** > **Access Control** > **Certificate Management** in the DSR online help.

After the certificates have been configured, you can log into the DSR GUI on any NOAM or SOAM, and then access the DSR GUI on other servers (NOAM or other SOAMs) without having to re-enter your login credentials.

1. In the browser URL field, enter the fully qualified hostname of the NOAM server, for example https://dsr-no.yourcompany.com.

   When using Single Sign-On, you cannot use the IP address of the server.
2. When prompted by the browser, confirm that the server can be trusted.

   The System Login page appears.
3. Enter the Username and Password for your account.

   The DSR GUI for the NOAM appears.
4. To access the DSR GUI for the SOAM, open another browser window and enter the fully qualified hostname of the SOAM.

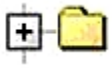
   The DSR GUI for the SOAM appears

You can toggle between the DSR GUI on the NOAM and the DSR GUI on the SOAM as you perform configuration tasks.

Main Menu Icons

This table describes the icons used in the **Main Menu**.

Table 4: Main Menu Icons

Icon	Name	Description
	Folder	Contains a group of operations. If the folder is expanded by clicking the plus (+) sign, all available operations and sub-folders are displayed. Clicking the minus (-) collapses the folder.
	Config File	Contains operations in an Options page.
	File with Magnifying Glass	Contains operations in a Status View page.
	File	Contains operations in a Data View page.
	Multiple Files	Contains operations in a File View page.
	File with Question Mark	Contains operations in a Query page.

Icon	Name	Description
	User	Contains operations related to users.
	Group	Contains operations related to groups.
	Help	Launches the Online Help.
	Logout	Logs the user out of the user interface.

Work Area Displays

In the user interface, tables, forms, tabbed pages, and reports are the most common formats.

Note: Screen shots are provided for reference only and may not exactly match a specific application's GUI.

Tables

Paginated tables describe the total number of records being displayed at the beginning and end of the table. They provide optional pagination with **First | Prev | Next | Last** links at both the beginning and end of this table type. Paginated tables also contain action links on the beginning and end of each row. For more information on action links and other page controls, see *Page Controls*.

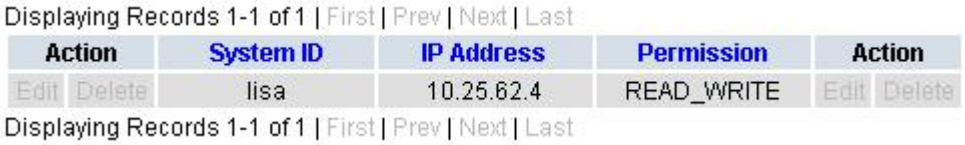
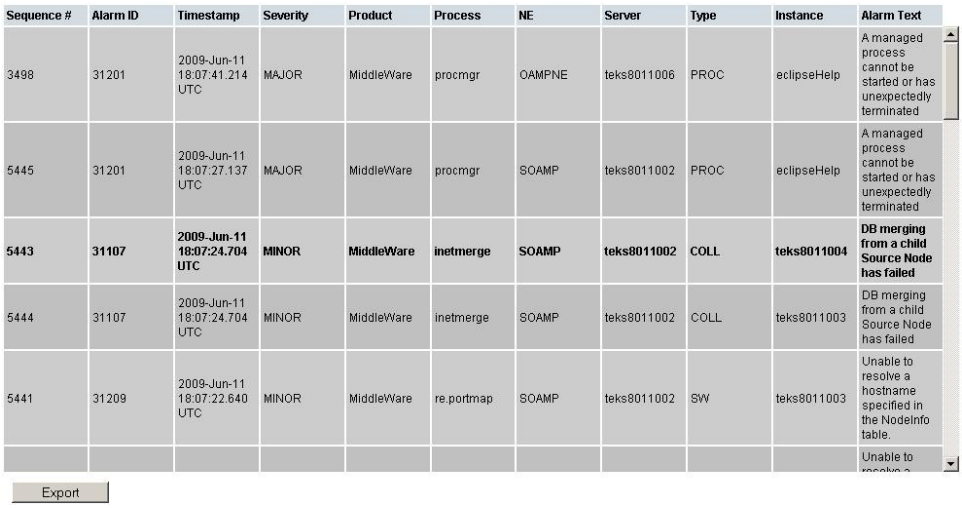


Figure 2: Paginated Table

Scrollable tables display all of the records on a single page. The scroll bar, located on the right side of the table, allows you to view all records in the table. Scrollable tables also provide action buttons that operate on selected rows. For more information on buttons and other page controls, see *Page Controls*.



Sequence #	Alarm ID	Timestamp	Severity	Product	Process	NE	Server	Type	Instance	Alarm Text
3498	31201	2009-Jun-11 18:07:41.214 UTC	MAJOR	MiddleWare	procmgr	OAMPNE	teks8011006	PROC	eclipseHelp	A managed process cannot be started or has unexpectedly terminated
5445	31201	2009-Jun-11 18:07:27.137 UTC	MAJOR	MiddleWare	procmgr	SOAMP	teks8011002	PROC	eclipseHelp	A managed process cannot be started or has unexpectedly terminated
5443	**31107**	**2009-Jun-11 18:07:24.704 UTC**	**MINOR**	**MiddleWare**	**inetmerge**	**SOAMP**	**teks8011002**	**COLL**	**teks8011004**	**DB merging from a child Source Node has failed**
5444	31107	2009-Jun-11 18:07:24.704 UTC	MINOR	MiddleWare	inetmerge	SOAMP	teks8011002	COLL	teks8011003	DB merging from a child Source Node has failed
5441	31209	2009-Jun-11 18:07:22.640 UTC	MINOR	MiddleWare	re.portmap	SOAMP	teks8011002	SW	teks8011003	Unable to resolve a hostname specified in the NodeInfo table.
										Unable to

Export

Figure 3: Scrollable Table

Note: Multiple rows can be selected in a scrollable table. Add rows one at a time using CTRL-click. Add a span of rows using SHIFT-click.

Forms

Forms are pages on which data can be entered. Forms are typically used for configuration. Forms contain fields and may also contain a combination of pulldown lists, buttons, and links.

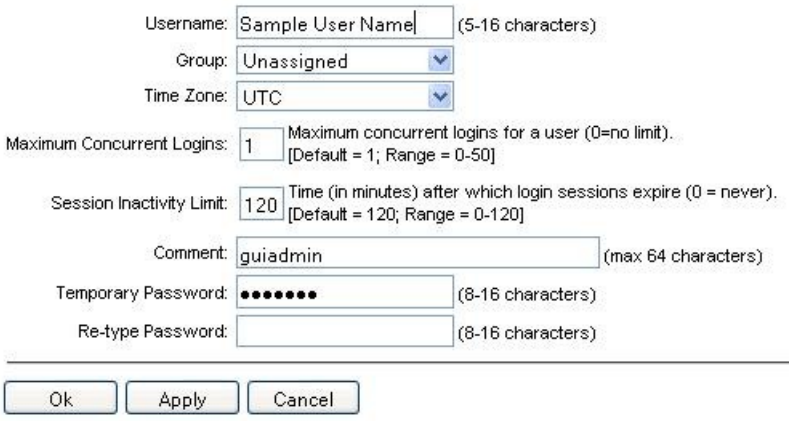
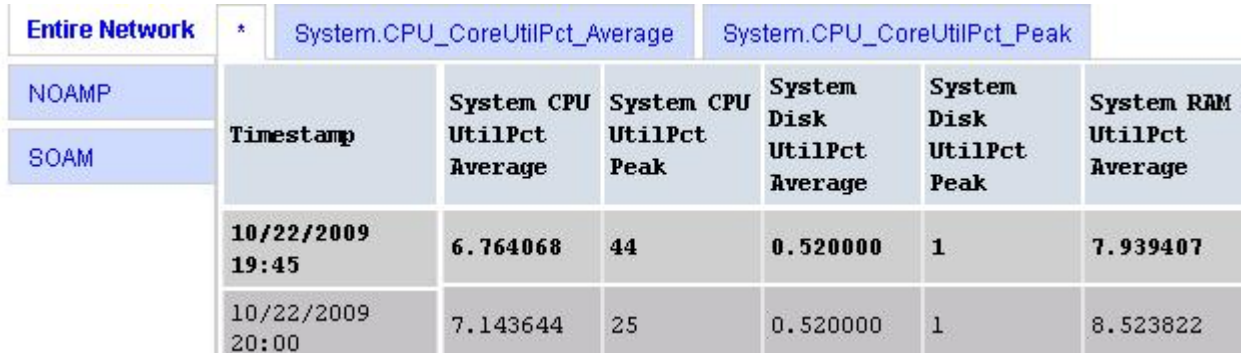


Figure 4: Form Page

Tabbed pages

Tabbed pages provide collections of data in selectable tabs. Click on a tab to see the relevant data on that tab. Tabbed pages also group Retrieve, Add, Update, and Delete options on one page. Click on the relevant tab for the task you want to perform and the appropriate fields populate on the page. Retrieve is always the default for tabbed pages.



Timestamp	System CPU UtilPct Average	System CPU UtilPct Peak	System Disk UtilPct Average	System Disk UtilPct Peak	System RAM UtilPct Average
10/22/2009 19:45	6.764068	44	0.520000	1	7.939407
10/22/2009 20:00	7.143644	25	0.520000	1	8.523822

Figure 5: Tabbed Pages

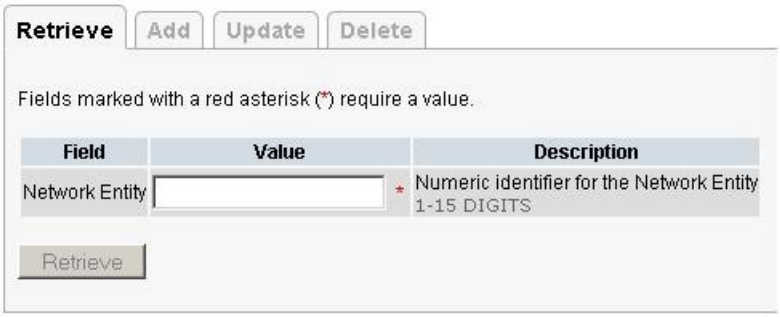


Figure 6: Tabbed Pages

Reports

Reports provide a formatted display of information. Reports are generated from data tables by clicking **Report**. Reports can be viewed directly on the user interface, or they can be printed. Reports can also be saved to a text file.

```
================================================================================

User Account Usage Report

================================================================================

Report Generated: Fri Jun 19 19:30:55 2009 UTC
From: Unknown Network OAM&P on host teks5001701
Report Version: 1.0
User: guiadmin

--------------------------------------------------------------------------------

Username          Date of Last Login    Days Since Last Login   Account Status
----------------  --------------------  ----------------------  ---------------
guiadmin          2009-06-19 19:00:17   0                       enabled

--------------------------------------------------------------------------------

End of User Account Usage Report

================================================================================
```

Figure 7: Report Output

Customizing the Splash Page Welcome Message

When you first log in to the user interface, the splash page appears. Located in the center of the main work area is a customizable welcome message. Use this procedure to create a message suitable for your needs.

1. From the **Main Menu**, click **Administration** > **General Options**.

   The **General Options** page appears.

2. Locate **WelcomeMessage** in the **Variable** column.
3. Enter the desired welcome message text in the **Value** column.
4. Click **OK** to save the change or **Cancel** to undo the change and return the field to the previously saved value.
   A status message appears at the top of the page to inform you if the operation was successful.

The next time you log in to the user interface, the new welcome message text is displayed.

Column Headers (Sorting)

You can sort a table by a column by clicking the column header. However, sorting is not necessarily available on every column. Sorting does not affect filtering.

When you click the header of a column that the table can be sorted by, an indicator appears in the column header showing the direction of the sort. See *Figure 8: Sorting a Table by Column Header*. Clicking the column header again reverses the direction of the sort.

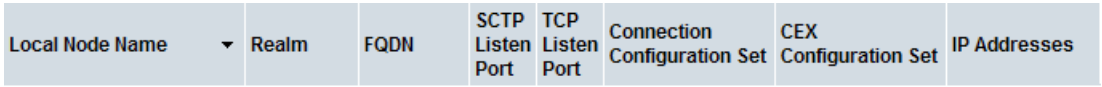


Figure 8: Sorting a Table by Column Header

Page Controls

User interface pages contain controls, such as buttons and links, that perform specified functions. The functions are described by the text of the links and buttons.

Note: Disabled buttons are grayed out. Buttons that are irrelevant to the selection or current system state, or which represent unauthorized actions as defined in **Group Administration**, are disabled. For example, **Delete** is disabled for users without Global Data Delete permission. Buttons are also disabled if, for example, multiple servers are selected for an action that can only be performed on a single server at a time.

Table 5: Example Action Buttons contains examples of Action buttons.

Table 5: Example Action Buttons

Action Button	Function
Insert	Inserts data into a table.
Edit	Edits data within a table.

Action Button	Function
Delete	Deletes data from table.
Change	Changes the status of a managed object.

Some Action buttons take you to another page.

Submit buttons, described in *Table 6: Submit Buttons*, are used to submit information to the server. The buttons are located in the page area and accompanied by a table in which you can enter information. The Submit buttons, except for **Cancel**, are disabled until you enter some data or select a value for all mandatory fields.

Table 6: Submit Buttons

Submit Button	Function
OK	Submits the information to the server, and if successful, returns to the View page for that table.
Apply	Submits the information to the server, and if successful, remains on the current page so that you can enter additional data.
Cancel	Returns to the View page for the table without submitting any information to the server.

Clear Field Control

The clear field control allows you to clear the value from a pulldown list. The clear field control is available only on some pulldown fields.

Click the **X** next to a pulldown list to clear the field.

Figure 9: Clear Field Control X

Optional Layout Element Toolbar

The optional layout element toolbar appears in the Page Control Area of the GUI.

Figure 10: Optional Layout Element Toolbar

The toolbar displays different elements depending on which GUI page is selected. The elements of the toolbar that can appear include:

- Filter – Allows you to filter data in a table.
- Errors – Displays errors associated with the work area.
- Info – Displays information messages associated with the work area.
- Status – Displays short status updates associated with the main work area.

- Warning – Displays warnings associated with the work area.

Notifications

Some messages require immediate attention, such as errors and status items. When new errors occur, the Errors element opens automatically with information about the error. Similarly, when new status items are added, the Status element opens. If you close an automatically opened element, the element stays closed until a new, unacknowledged item is added.

Figure 11: Automatic Error Notification

Note: Viewing and closing an error does not clear the Errors element. If you reopen the Errors element, previously viewed errors are still in the list.

When new messages are added to Warning or Info, the styling of the element changes to indicate new messages are available. The styling of the Task element changes when a task changes state (such as, a task begins or ends).

Opening an Element in the Toolbar

Use this procedure to open an element in the optional layout element toolbar.

1. Click the text of the element or the triangle icon to open an element.
   The selected element opens and overlays the work area.
2. Click **X** to close the element display.

Filters

Filters are part of the optional layout element toolbar and appear throughout the GUI in the Page Control Area. For more information about optional layout element toolbar functionality, see *Optional Layout Element Toolbar*.

Filters allow you to limit the data presented in a table and can specify multiple filter criteria. By default, table rows appear unfiltered. Three types of filters are supported, however, not all filtering options are available on every page. The types of filters supported include:

- Network Element – When enabled, the Network Element filter limits the data viewed to a single Network Element.

  Note: Once enabled, the Network Element filter will affect all pages that list or display data relating to the Network Element.

- Collection Interval – When enabled, the collection interval filter limits the data to entries collected in a specified time range.

- Display Filter – The display filter limits the data viewed to data matching the specified criteria.

Once a field is selected, it cannot be selected again. All specified criteria must be met in order for a row to be displayed.

The style or format of filters may vary depending on which GUI pages the filters are displayed. Regardless of appearance, filters of the same type function the same.

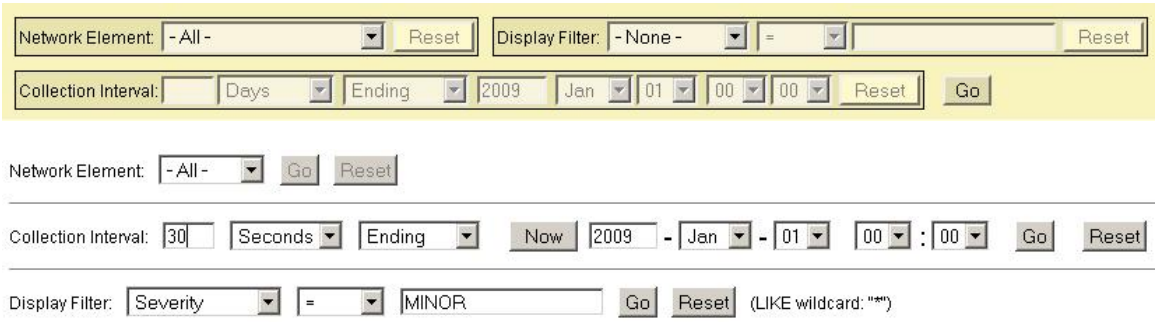


Figure 12: Examples of Filter Styles

Filter Control Elements

This table describes filter control elements of the user interface.

Table 7: Filter Control Elements

Operator	Description
=	Displays an exact match.
!=	Displays all records that do not match the specified filter parameter value.
>	Displays all records with a parameter value that is greater than the specified value.
>=	Displays all records with a parameter value that is greater than or equal to the specified value.
<	Displays all records with a parameter value that is less than the specified value.
<=	Displays all records with a parameter value that is less than or equal to the specified value.
Like	Enables you to use an asterisk (*) as a wildcard as part of the filter parameter value.
Is Null	Displays all records that have a value of **Is Null** in the specified field.

Note: Not all filterable fields support all operators. Only the supported operators will be available for you to select.

Filtering on the Network Element

The global Network Element filter is a special filter that is enabled on a per-user basis. The global Network Element filter allows a user to limit the data viewed to a single Network Element. Once

enabled, the global Network Element filter affects all sub-screens that display data related to Network Elements. This filtering option may not be available on all pages.

1. Click **Filter** in the optional layout element toolbar.
   The filter tool appears.
2. Select a Network Element from the **Network Element** pulldown menu.
3. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Filtering on Collection Interval

The Collection Interval filter allows a user to limit the data viewed to a specified time interval. This filtering option may not be available on all pages.

1. Click **Filter** in the optional layout element toolbar.
   The filter tool appears.
2. Enter a duration for the **Collection Interval** filter.
   The duration must be a numeric value.
3. Select a unit of time from the pulldown menu.
   The unit of time can be seconds, minutes, hours, or days.
4. Select **Beginning** or **Ending** from the pulldown menu.
5. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Filtering Using the Display Filter

Use this procedure to perform a filtering operation. This procedure assumes you have a data table displayed on your screen. This process is the same for all data tables. However, all filtering operations are not available for all tables.

1. Click **Filter** in the optional layout element toolbar.
   The filter tool appears.
2. Select a field name from the **Display Filter** pulldown menu.
   This selection specifies the field in the table that you want to filter on. The default is **None**, which indicates that you want all available data displayed.
   The selected field name displays in the **Display Filter** field.
3. Select an operator from the operation selector pulldown menu.
   The selected operator appears in the field.
4. Enter a value in the value field.
   This value specifies the data that you want to filter on. For example, if you specify Filter=Severity with the equals (=) operator and a value of MINOR, the table would show only records where Severity=MINOR.
5. For data tables that support compound filtering, click **Add** to add another filter condition. Then repeat steps 2 through 4.

Multiple filter conditions are joined by an AND operator.

6. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Pause Updates

Some pages refresh automatically. Updates to these pages can be paused by selecting the **Pause updates** checkbox. Uncheck the **Pause updates** checkbox to resume automatic updates. The **Pause updates** checkbox is available only on some pages.

Max Records Per Page Controls

Max Records Per Page is used to control the maximum number of records displayed in the page area. If a page uses pagination, the value of Max Records Per Page is used. Use this procedure to change the Max Records Per Page.

1. From the **Main Menu**, click **Administration** > **General Options**.

   The **General Options Administration** page appears.

2. Change the value of the **MaxRecordsPerPage** variable.

   Note: Maximum Records Per Page has a range of values from 10 to 100 records. The default value is 20.

3. Click **OK** or **Apply**.

   OK saves the change and returns to the previous page.

   Apply saves the change and remains on the same page.

The maximum number of records displayed is changed.

Chapter 3

Introduction to IPFE

Topics:

The IP Front End (IPFE) is a traffic distributor that transparently does the following:

- Presents a routable IP address representing a set of up to 16 application servers to application clients. This reduces the number of addresses with which the clients need to be configured.
- Routes packets from the clients that establish new TCP or SCTP connections to selected application servers.
- Routes packets in existing TCP or SCTP connections to the correct servers for the connection.

IPFE Description

The IPFE acts as a specialized layer-3 router. The various servers to which the IPFE routes packets are divided into up to 16 groups, called Target Sets. Each of the target sets are assigned a shared Target Set Address, a publicly exposed service address.

Figure 13: IPFE Architecture shows either two connections are maintained at all times, in active/active or active/standby, or that a single connection is maintained, with a backup address for clients to establish a connection, if the first connection fails.

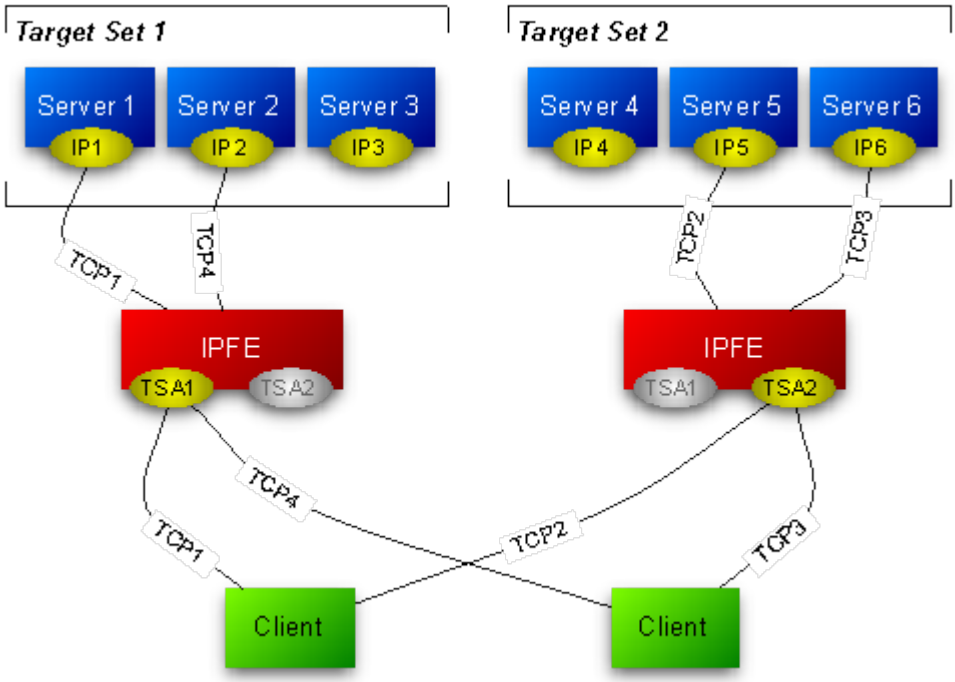


Figure 13: IPFE Architecture

When the IPFE routes packets to application servers, it does not perform any rewriting of the packet. *Figure 14: Packet Routing Through and Around the IPFE* shows that neither the source IP address nor the destination IP address changes as it passes through the IPFE. The IPFE behaves as an IP router and does not act as a network address translator (NAT).

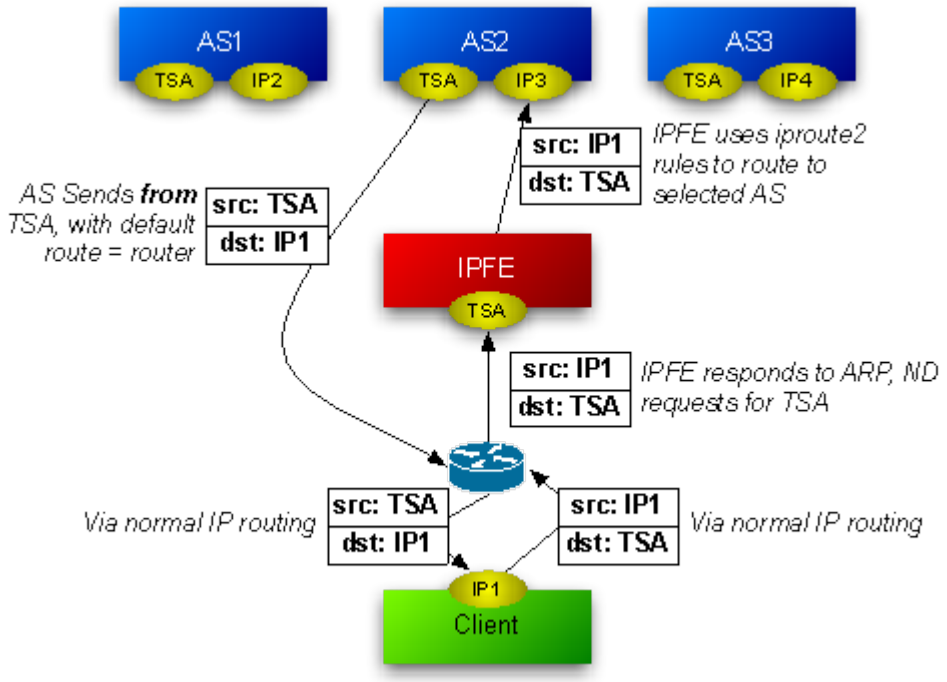


Figure 14: Packet Routing Through and Around the IPFE

Traffic distribution

The IPFE is a packet-based load balancer that makes a large cluster accessible to incoming connections through a minimal number of IP addresses. These incoming connections can be TCP, unihomed SCTP, or multihomed SCTP. The IPFE distributes these connections among a list of target IP addresses by forwarding incoming packets. The list is called the **Target Set IP List**, and an outward-facing IP address is called a Target Set Address (TSA). A packet arriving at the IPFE and destined for the TSA is forwarded to an address in the **Target Set IP List**.

There can be as many as 16 IP addresses in the Target Set IP List and thus the IPFE may distribute traffic among as many as 16 physical or virtual application servers. Each server in the Target Set IP List can have a **Weighting** indicating that the IPFE should apportion more or fewer connections to that server. The load balancing algorithm for apportioning connections is also configurable through a number of settings. The TSA, Target Set IP List, Weighting, and Load Balancing Algorithm settings are together called a **Target Set**. There can be as many as 32 independent **Target Sets** configured on one IPFE.

The IPFE neither interprets nor modifies anything in the TCP or SCTP payload. The IPFE also does not maintain TCP or SCTP state, but keeps sufficient state to route all packets for a particular session to the same application server.

Return traffic from the application server to the client (both TCP and SCTP) does not pass through the IPFE, but routes directly to the gateway.

High Availability

The IPFE supports active-standby or active-active high availability (HA) when paired with a second IPFE instance. The mated pair of IPFEs expose typically one or two TSAs per configured IP version.

Each TSA can operate in an active-standby mode, where all traffic to a given TSA goes to the active (for that TSA) IPFE, if it is available. If the active IPFE fails or if its mate is explicitly selected as Active, traffic to the TSA will go to the mate IPFE. For active-active HA, the addresses must be configured in pairs, where one IPFE is active for one address in a pair, and the mate is active for the other.

Note that the IPFE supports more than 2 TSAs, and in fact when both IPv4 and IPv6 are supported, the IPFE will usually be configured with at least 4 TSAs. An IPFE and its mate are numbered 1 and 2, whereas an IPFE pair is numbered A and B. The four IPFEs are numbered A1, A2, B1, and B2.

For multihomed SCTP connections, the **Target Set** is represented by both a Primary Address and a Secondary Address. Each application server in the Target Set must also be configured for multihomed SCTP.

IPFE Associations

The IPFE stores an Association record about each connection. The Association contains the information necessary to identify packets belonging to a connection and to identify the application server that the IPFE has selected for the connection. The IPFE routes all packets associated with a particular connection to the selected application server.

The specific packet-identifying information is the source IP address and the source port number. For each **Target Set**, packets matching both by source address and source port will be routed to the same target application server. SCTP verification tags are also used as identifiers since, with the SCTP protocol, the source IP address can change.

All association information is replicated between mated IPFEs, but not between IPFE pairs.

Association information is isolated to a Target Set so that the Target Sets behave independently.

Because returning packets bypass the IPFE, the IPFE has limited knowledge of the state of the connection. The IPFE cannot determine if a connection has reconnected from the same source port, nor whether the connection has been terminated. The IPFE attempts to use the available state information to make the best possible judgments about when an association is stale. A stale connection is removed and subsequent packets originating from the same IP address and from the same source port are treated as a new connection: the load balancing algorithm is freshly applied.

An association is considered stale if:

- No packets have been received for the duration of the **Delete Age** setting in the **Target Set** configuration.
- The transactions of the form Connect-CER-CEA-Disconnect are the only transactions to have taken place for a period of time of **Delete Age**.
- The IPFE is able to track the TCP sequence numbers and then determined that an authentic FIN and subsequence SYN are evidence that a TCP connection has disconnected and reconnected. This tracking works for certain idealized TCP connections only.

- The IPFE is able to track the SCTP verification tag and then determined that an authentic SHUTDOWN and subsequence INIT are evidence that a SCTP connection has disconnected and reconnected. This tracking works for certain idealized SCTP connections only.

Load Balancing

If a packet is not matched by any association the IPFE will create a new association by choosing an application server from the **Target Set IP List.** The choice is based on the **Load Balance Algorithm** setting.

Regardless of the algorithm, the IPFE will raise a minor alarm of Out of Balance: High or Out of Balance: Low on an application server whenever it is receiving a statistically high or low amount of traffic in comparison to others within the same **Target Set.**

If an application server determines that it has reached fully loaded capacity, then it will notify the IPFE not to send it further new connections. This is called Stasis. Application servers may go in and out of Stasis automatically according to the current traffic.

There are two **Load Balance Algorithms** available:

- **Hash**: load balancing achieves by sending the new connection to a server based on hashing the originating port and IP address. **Hash** load balancing will remove an application server from consideration for new connections whenever it is incurring an Out of Balance: High alarm. In this way reconnecting connections will always be directed to application servers that are moderately loaded. This feature is independent of Stasis notifications.
- **Least load** : chooses the server with the least load as reported by the application server. If the loads of two or more of the least-loaded servers are within a configurable percentage of each other, they are considered equally loaded, and the IPFE distributes connections to them in a round-robin fashion.

IPv4 and IPv6 support

A **Target Set** can be created as either IPv4 or IPv6. However a **Target Set** cannot support mixed address types. This means that SCTP multihomed endpoints can contain address types of either IPv4 or IPv6 but not both.

Throttling

In the case of signaling storms, the IPFE provides a configurable parameter which limits the IPFE's throughput rate and prevents the maxing out of its CPU. **Throttling** causes the IPFE to drop packets in order to keep the load from overwhelming the IPFE. The packet/second rate limit implementation creates an even dropping of packets that would cause client TCP/SCTP stacks to withhold their rates to just below the threshold, as happens when there is an overloaded router in the path. Throttling is on per-local-port bases, for example, each local port (such as 3868) is apportioned the configured amount.

Failure and recovery scenarios

An IPFE that has a mate and at least two Target Set Addresses can handle different failure and recovery scenarios.

Note: The following failover scenarios describe what happens with the IPFE-A1 and IPFE-A2 pair. A failover involving the IPFE-B1 and IPFE-B2 pair is handled exactly the same way.

This section discusses how the following IPFE setup can gracefully handle the failure and recovery of various components in the system:

- Two IPFEs, IPFE-A1 and IPFE-A2, each responsible for one Target Set Address. IPFE-A1 is primary for TSA1, and IPFE-A2 is primary for TSA2.
- Two Target Sets, each with three application servers and the Target Set Addresses TSA1 and TSA2.
  - TSA1 has application servers Server1, Server2, and Server3
  - TSA2 has application servers Server4, Server5, and Server6
- Two clients, each configured with TSA1 and TSA2.

These failure and recovery scenarios apply to a single component outage.

IPFE failure and recovery

If IPFE-A1 fails, the system handles it in the following manner:

- IPFE-A1's mate, IPFE-A2, detects the failure.
- IPFE-A2 takes over IPFE-A1's TSA, TSA1.
- There are no changes to the application servers in TSA1. TSA1 continues to comprise Server1, Server2, and Server3
- Traffic for TSA1 continues to go to TSA1, which is now managed by IPFE-A2
- IPFE-A2 continues to route TSA1 traffic to Server1, Server2, and Server3 - no different than they were before the failure.
- IPFE-A2 also continues to route traffic for TSA2 to Server4, Server5, and Server6.
- No disruption of service occurs.
- New connection requests for TSA1 will be routed to Server1, Server2 or Server3.
- New connection requests for TSA2 will be routed to Server4, Server5 or Server6.

When IPFE-A1 recovers, the following happens:

- IPFE-A2 detects that IPFE-A1 has recovered and relinquishes control of TSA1.
- IPFE-A1 assumes control of TSA1.
- Traffic that went to TSA1 continues to go to TSA1.
- The clients are unaware that a recovery has occurred.
- New connection requests for TSA1 continue to be routed to Server1, Server2, or Server3.
- New connection requests for TSA2 continue to be routed to Server4, Server5, or Server6.

Application server failure and recovery

When an application server, say Server1, fails, the following occurs:

- The connections from the client will also fail.
- Other connections through TSA1 to Server2 and Server3 will survive.
- Clients who were sending traffic to the failed application server must send traffic to their secondary TSA (TSA2).
- IPFE-A1 will route new connection requests to the remaining application servers (Server2 and Server3). If all application servers in a target set fail, and IPFE-A1 receives a request for a new connection to TSA1, it will optionally notify the client that the request cannot be fulfilled, using either a TCP RST packet (for TCP connections), or a configurable ICMP message.

When Server1 recovers:

- IPFE-A1 will detect Server1's availability.
- IPFE-A1 will route new connection requests to Server1.
- Some imbalance across application servers in TSA1 will exist after recovery. IPFE-A1 will monitor for imbalances in traffic and distribute new connections to reduce the imbalance.

Enclosure failure and recovery

In the enclosure failure scenario we assume that the IPFE is co-located with the application servers in its Target Set. In this case, IPFE-A1 is in an enclosure with Server1, Server2, and Server3.

When the enclosure containing IPFE-A1, Server1, Server2, and Server3 fails:

- All connections to all servers in the enclosure will fail.
- IPFE-A2 will detect that IPFE-A1 is down and start servicing TSA1.
- Clients with existing connections to TSA1 will detect that TSA1 is unavailable and send traffic to TSA2.
- Depending on configuration, IPFE-A2 will send optionally send a TCP RST (for TCP connections) or a configured ICMP message in response to client connection requests to TSA1.

When the enclosure recovers:

- IPFE-A2 will detect that IPFE-A1 has recovered and relinquish control of TSA1.
- IPFE-A1 will take over control of TSA1.
- Since TSA1 did not have any existing connections during the failure, no special handling of existing connections is required.
- Over a period of time, clients are expected to route new connections to TSA1, resulting in connections to recovered servers in the associated Target Set.
- In the interim, there will be a substantial imbalance between the two IPFEs as well as between the servers in the two TSAs. The IPFEs will monitor the traffic for imbalances and distribute new connections to reduce the imbalance.

External connectivity failure and recovery

If external connectivity to the IPFE, say IPFE-A1, fails:

- Connections to IPFE-A1 and TSA1 fail.
- IPFE-A2 will not take over TSA1 since it sees IPFE-A1 as available. That is, internal connections still work.
- Clients with failed connections to TSA1 must send traffic to TSA2.
- Clients attempting to create new connections to TSA1 will fail.

- IPFE-A2 and TSA2 will carry all the traffic for all the clients.

When external connectivity is restored:

- There will be no existing connections for TSA1 to handle.
- IPFE-A1 will still retain control over TSA1.
- Clients will route new connections to TSA1 over time.
- In the interim, there will be a substantial imbalance between the two IPFEs as well as between the servers in the two TSAs. The IPFEs will monitor the traffic for imbalances and distribute new connections to reduce the imbalance.

Bulk Import and Export

The *Diameter Common User's Guide* describes the use and operation of Bulk Import and Export functions:

- **Help** > **Diameter Common** > **Bulk Import**
- **Help** > **Diameter Common** > **Bulk Export**

The Bulk Import and Export functions can be used to export Diameter, IPFE, and Application configuration data in CSV files to a location outside the system, and to import the files (usually edited) into the system where the Import function is executed.

Bulk Import

The Bulk Import operations use configuration data in ASCII Comma-Separated Values (CSV) files (.csv), to insert new data into, update existing data in, or delete existing data from the configuration data in the system.

Note: Some configuration data can be imported only with the Update operation, and other data can be imported with Insert and Delete operations but not Update. Refer to the *Diameter Common User's Guide* or the **Diameter Common** > **Import** Help for valid Import operations.

Import CSV files can be created by using a Bulk Export operation, or can be manually created using a text editor.

Note: The format of each Import CSV file record must be compatible with the configuration data in the release that is used to import the file. Across different release versions, column counts may not be compatible, and the import will fail.

Files that are created using the Bulk Export operation can be exported either to the local Status & Manage File Management Directory (**Status & Manage** > **Files** page), or to the local Export Server Directory.

CSV files that are in the local File Management area can be used for Bulk Import operations on the local system.

Files can be created manually using a text editor; the files must be uploaded to the File Management area of the local system before they can be used for Import operations on the local system.

Multiple Import operations can be performed:

- Insert new configuration data records that do not currently exist in the system
- Update existing configuration data in the system
- Delete existing configuration data from the system

Each Import operation creates a log file. If errors occur, a Failures CSV file is created that appears in the File Management area. Failures files can be downloaded, edited to correct the errors, and imported to successfully process the records that failed. Failures files that are unchanged for more than 14 days and log files that are older than 14 days are automatically deleted from the File Management area.

Bulk Export

The Bulk Export operation creates ASCII Comma-Separated Values (CSV) files (.csv) containing Diameter, IPFE, and Application configuration data. Exported configuration data can be edited and used with the Bulk Import operations to change the configuration data in the local system without the use of GUI pages. The exported files can be transferred to and used to configure another system.

Each exported CSV file contains one or more records for the configuration data that was selected for the Export operation. The selected configuration data can be exported once immediately, or exports can be scheduled to periodically occur automatically at configured times.

Configuration data can be exported in one Export operation:

- All exportable configuration data in the system
- All exportable configuration data from the selected Application, IPFE, or Diameter (each component's data is in a separate file)
- Exportable configuration data from a selected configuration component for the selected Application, IPFE, or Diameter

Exported files can be written to the File Management Directory in the local File Management area (**Status & Manage** > **Files** page), or to the Export Server Directory for transfer to a configured remote Export server.

CSV files that are in the local File Management area can be used for Bulk Import operations on the local system.

If the export has any failures or is unsuccessful, the results of the export operation are logged to a log file with the same name as the exported file but with a .log extension. Successful export operations will not be logged.

Chapter 4

IPFE Configuration Options

Topics:

The **IPFE -> Configuration -> Options** page allows you to manage IPFE configuration.

Configuration Options elements

Table 8: IPFE Configuration Elements describe the fields on the **IPFE -> Configuration -> Options** . An asterisk after the value field means that the configuration is mandatory.

Table 8: IPFE Configuration Elements

Element	Description	Data Input Notes
Inter-IPFE Synchronization		
IPFE-A1 IP Address	The IP address of IPFE-A1. This selection is disabled when a Target Set has IPFE-A1 selected as Active. This address must reside on the IMI (internal management interface) network. This address is used for replicating association data between IPFEs and is not exposed to application clients. If left blank, the IPFE will not replicate association data. Although optional, this configuration is required for a fully functioning installation.	Format: IPv4 or IPv6 address, or left blank Default: blank
IPFE-A2 IP Address	The IP address of IPFE-A2. This selection is disabled when a Target Set has IPFE-A2 selected as Active. This address must reside on the IMI (internal management interface) network. This address is used for replicating association data between IPFEs and is not exposed to application clients. If left blank, the IPFE will not replicate association data. Although optional, this configuration is required for a fully functioning installation.	Format: IPv4 or IPv6 address, or left blank Default: blank
IPFE-B1 IP Address	The IP address of IPFE-B1. This selection is disabled when a Target Set has IPFE-B1 selected as Active.	Format: IP address, or left blank Default: blank

Element	Description	Data Input Notes
	This address must reside on the IMI (internal management interface) network. This address is used for replicating association data between IPFEs and is not exposed to application clients. If left blank, the IPFE will not replicate association data. Although optional, this configuration is required for a fully functioning installation.	
IPFE-B2 IP Address	The IP address of IPFE-B2. This selection is disabled when a Target Set has IPFE-B2 selected as Active. This address must reside on the IMI (internal management interface) network. This address is used for replicating association data between IPFEs and is not exposed to application clients. If left blank, the IPFE will not replicate association data. Although optional, this configuration is required for a fully-functioning installation.	Format: IP address, or left blank Default: blank
* State Sync TCP Port	TCP port to use for syncing kernel state between IPFEs. This port is used on both IPFEs.	Format: numeric Range: 1-65535 Default: 19041
* State Sync Reconnect Interval	Reconnect interval, in seconds, for syncing kernel state between IPFEs.	Format: numeric, seconds Range: 1-255 seconds Default: 1
* Gratuitous ARP Type	Specify type of gratuitous ARP broadcast to send.	Format: ARP Request, ARP Reply, Send both types Default: ARP Request
Traffic Forwarding		
* Application Traffic TCP Reject Option	How to reject TCP connections when no application servers are available. When no application servers are available, the IPFE must reject the TCP	Format: pull-down list Range: • TCP Reset

Element	Description	Data Input Notes
	traffic that it receives. The IPFE can either drop packets or it can communicate to the application clients with TCP or ICMP messages. Select the option that can be best handled by the application client.	• Drop Packet • ICMP Host Unreachable • ICMP Port Unreachable • ICMP Administratively Prohibited Default: TCP Reset
* Application Traffic SCTP Reject Option	How to reject SCTP connections when no application servers are available. When no application servers are available, the IPFE must reject the SCTP traffic that it receives. The IPFE can either drop packets or it can communicate to the application clients with ICMP messages. Select the option that can be best handled by the application client.	Format: pull-down list Range: • Drop Packet • ICMP Host Unreachable • ICMP Port Unreachable • ICMP Administratively Prohibited Default: ICMP Host Unreachable
Packet Counting		
* Imbalance Detection Throughput Minimum	This value applies only to the hash algorithm selection. This is the value below which no throughput analysis is performed regarding the distribution of connections. This setting should not be changed from its default unless the IPFE is being tested with a very low load. This setting ensures that the IPFE will not mark application servers as imbalanced when it is distributing very few messages between them.	Format: numeric, packets per second Range: 1-2147483647 Default: 20000
* Least Load Threshold	This value can be set to a packets-per-second rate below which the Least Load algorithm reverts to round robin.	Format: numeric, packets per second Range: 1-2147483647 Default: 1
* Cluster Rebalancing and Accounting	Support for cluster rebalancing and packet accounting in measurements. When this is disabled, all accumulation of packet and byte measurements cease. Overload detection also stops. The disabled state is useful only for troubleshooting, which should be done by the *My Oracle Support*.	Format: pull-down list Range: • Enabled • Disabled Default: Enabled

Element	Description	Data Input Notes
	Contact the *My Oracle Support* before disabling measurements and overload detection.	
Application Server Monitoring		
* Monitoring Port	TCP port to try periodic connections or monitoring of application servers. The IPFE opens a TCP connection to the application server's IP address and this port. The application server must listen on this port and should send heartbeats.	Format: numeric Range: 1-65535 Default: 9675
* Monitoring Connection Timeout	How long to wait for a connection to complete when polling the application servers for aliveness in seconds. If the IPFE detects that an application server has missed a configurable number of heartbeats - that is, more than that number of seconds have elapsed since the most recent heartbeat was received - then it considers the application server to be down. The IPFE will remove a down application server from the traffic balancing pool and attempt to reconnect to the server.	Format: numeric: seconds Range: 1 - 255 Default: 3
Monitoring Connection Try Interval	Interval in seconds of periodically connecting to application servers to test for aliveness. While an application server is down, the IPFE will periodically attempt to reconnect to it based on this configuration.	Format: numeric: seconds Range: 1 - 255 Default: 10
Monitoring Protocol	Application liveness monitoring method. If any Target Set has load balancing of **Least Load** then this setting cannot be changed from **Heartbeat** due to the need for load information in the monitoring packets. The monitoring protocol allows the IPFE to determine the liveness of the application servers. The IPFE determines this either by listening for	Format: pull-down list Range: • Heartbeat • None Default: Heartbeat

Element	Description	Data Input Notes
	heartbeat messages from the application servers. When the protocol is set to Heartbeat, the IPFE connects to the monitoring port, sustains the connection, and receives heartbeat packets from the application server. In this case, the failure to receive a heartbeat packet within the period **Back-end Connection Timeout** indicates the server is dead. A dead server is removed from the traffic balancing pool. The IPFE attempts connections on the monitoring port until the server responds. When the server responds, the IPFE adds it back to the pool.	
Throttling and DoS Protection		
Global Packet Rate Limit	Combined packet rate limit for a single IPFE at which overload throttling is applied.	Format: text box; numeric Range: 10000 - 10000000 Default: 500000

Configuring the IPFE

The **IPFE -> Configuration -> Options** page set up data replication between IPFEs, specify port ranges for TCP traffic, and set application server monitoring parameters.

1. Select **IPFE > Configuration > Options**.
   The **IPFE -> Configuration -> Options** page appears. The fields are described in *Table 8: IPFE Configuration Elements*.
2. Under the **Inter-IPFE Synchronization** section complete the following entries:
   a) Enter the IP addresses for IPFE-A1, IPFE-A2, IPFE-B1, and IPFE-B2 in the corresponding **IPFE-Xn IP Address** field.

      These are internal addresses used by the IPFEs to replicate association data. These addresses should reside on the IMI (Internal Management Interface) network.

   b) Select the **State Sync TCP Port** used for syncing kernel state between IPFE.
   c) Set the **State Sync Reconnect Interval** for syncing kernel state between IPFE.
   d) Select the type of **Gratuitous ARP Type** broadcast to send.
3. Under the **Traffic Forwarding** section complete the following entries:
   a) If not application servers are available, select how to reject TCP connections in the**Application Traffic TCP Reject Option** pull down box.

b) If not application servers are available, select how to reject SCTP connections in the**Application Traffic SCTP Reject Option** pull down box.

4. Under the **Packet Counting** section complete the following entries:
   a) Set a value for **Imbalance Detection Throughput Minimum**.

      The default setting is 20000 and should not be changed from its default unless the IPFE is being tested with a very low load.

   b) Set a value for **Least load Threshold**.

      This value can be set to a packets-per-second rate below which the Least Load algorithm reverts to round robin.

   c) If you want the support for cluster rebalancing and packet accounting in measurements, select **Enabled** from the pull down menu in the **Cluster Rebalancing and Accounting** field.

      When this is disabled, all accumulation of packet and byte measurements cease.

5. Under the **Application Server Monitoring** section complete the following entries:
   a) Set a value for **Monitoring Port**

      The application server must listen on this port and should send heartbeats.

   b) Set the wait time for a connection to complete when polling the application servers for aliveness in the **Monitoring Connection Timeout** field
   c) Set the interval for periodically connecting to application servers to test for aliveness in the **Monitoring Connection Try Interval** field.
   d) If you want to monitor the liveness of application servers, select **Heartbeat** in the **Monitoring Protocol** field.

      If any Target Set has load balancing of Least Load then this setting cannot be changed from **Heartbeat** due to the need for load information in the monitoring packets.

6. Under the **Throttling and DoS protection** section complete the following entry:
   a) Set the overload throttling in the **Global Packet Rate Limit**field. combined packet rate limit for a single IPFE at which is applied.

7. Click:

   - **OK** to save your changes.
   - **Apply** to apply your changes. The changes will go into effect immediately.

   If **OK** or **Apply** are clicked and any of the following conditions exist, an error message appears:

   - Any required field is empty; no value was entered or selected
   - The entry in any field is not valid (wrong data type or out of valid range)
   - An IP address is assigned to more than one IPFE.
   - An IP address is assigned to an IPFE, but is already used as a Target Set Address
   - An IP address is assigned to an IPFE, but is already used as the address of an Application Server

For the IPFE to be fully functional, you must assign application servers to a Target Set and associate the Target Set with the IPFE. See *Adding a Target Set* to add a new Target Set.

Chapter 5

IPFE Target Sets Configuration

Topics:

The **IPFE -> Configuration -> Target Sets** page allows you to assign a list of application server IP addresses to a Target Set and associate the Target Set with an IPFE pair.

Target Sets configuration elements

A Target Set associated with an IPFE maps a single externally available IP address to a set of IP addresses for application servers.

In general, it is inadvisable to reduce **Delete Age** value to less than the default. However, a TSA that has connections with longer SCTP heartbeat interval may require this value to be increased from default.

The *Table 9: Target Sets configuration elements (View pages)* describes the fields on the **IPFE -> Configuration -> Target Sets** page.

The *Table 10: Target Sets configuration elements (Insert and Edit pages)* describes the fields on the Insert, and Edit pages.

Table 9: Target Sets configuration elements (View pages)

Field	Description	Data Input Notes
Target Set Number	Unique ID identifying the Target Set.	Format: Numeric Range: 1-32
Target Set Address	Public IP address to present to the outside world.	Format: IPv4 or IPv6 address The Target Set Address must be on the XSI network
Target Set IP List	List of IP addresses of the associated application servers.	Format: IPv4 or IPv6 address. IP address type must match that of the Target Set Address. The IP addresses in Target Set IP List must be on the XSI network.
Weighting	Weighting value is used to apportion load between application servers within the Target Set.	Format: Numeric Range: 0-65535 Default: 100
Supported Protocols	The protocols supported by this Target Set.	Format: Options Range: TCP only, SCTP only, Both TCP and SCTP Default: Both TCP and SCTP
Preferred Active	The IPFE that will primarily handle traffic for this Target Set. **`Disabled`** means that the Target Set is defined, but not currently in use by an IPFE.	Format: Options Range: IPFE-A1, IPFE-A2, IPFE-B1, IPFE-B2 Default: IPFE-A1

Field	Description	Data Input Notes
		If an option is not activate, you need configure the IPFE address under **IPFE** > **Configure** > **Options**.
Preferred Standby	The mate of the Preferred Active IPFE. If the Preferred Active IPFE is unavailable, the Preferred Standby server takes over.	If the Preferred Standby IPFE has been configured, it will be set when you select the Preferred Active IPFE.

Table 10: Target Sets configuration elements (Insert and Edit pages)

Field	Description	Data Input Notes
Target Set		
*TS Number	Unique ID identifying the TSA.	Format: Drop down menu Range:1-32 Default: 1
Protocols	A Target Set can support SCTP, TCP, or both.	Format: Options Range: TCP only, SCTP only, Both TCP and SCTP Default: Both TCP and SCTP
Disable	Select to disable this Target Set, but preserve it in this configuration.	Format: Checkbox Range: Disable
*Delete Age	Connections are dropped if idle for this time (seconds). When setting this value please take into account that TCP connections can sometimes be idle for long periods of time depending on the application protocol.	Format: Text box, numeric Range: 10 - 3110400 Default: 600
Load Balance Algorithm	Algorithm used to determine where new connections should go. **`Hash`**: load balancing by sending the new connection to a server based on hashing the originating port and IP address. **`Least Load`**: load balancing by choosing the server with the least load as reported by the application server. (Requires Monitoring Protocol to be set to Heartbeat.) The load of an application server is calculated using the load equation: $L(m,c) = (F_m * m/m_{total} + F_c * c/_{ctotal}) * W_{high}/w$ where m and m_{total} are the currently reserved and	Format: Options Range: **`Hash`**, **`Least Load`** Default: Least Load

Field	Description	Data Input Notes
	total capacity of ingress MPS (messages per second), respectively; c and c_{total} are the number of current connections and total connection capacity, respectively; w and w_{high} are the application server weighing and the highest weighting in the Target IP List, respectively. The value c includes, as an added component, the rate of new connections, in order to smooth the distribution of a sudden flood of new connections.	
Least Load Parameters		
*MPS Factor	Factor F_m in load equation. The total $F_m + F_c$ will be normalized to 100 on commit of this form.	Format: Text field; numeric Range: 0 - 100 Default: 50
*Connection Count Factor	Factor F_c in load equation. The total $F_m + F_c$ will be normalized to 100 on commit of this form.	Format: Text field; numeric Range: 0 - 100 Default: 50
*Allowed Deviation	Percentage within which two application servers' L(m,c) results are considered to be equal, which is used to smooth out load distribution. If the difference in load between the lowest and next least-loaded application server is greater than or equal to this value, then the IPFE applies the Least Load algorithm and assigns new connections to the least loaded application server. If the difference in load between the lowest and next least-loaded application server is less than this value, then the IPFE distributes the connection in a weighted round-robin fashion between the application servers that are within the Allowed Deviation range.	Format: Text field; numeric Range: 0 - 50 Default: 5
Peer Node Aware Least Load	Enable Peer Node Group awareness when directing connections. When enabled, the IPFE distribute connections from the same Peer Node Group across servers in the Target Set to provide server redundancy for that group of peers. The IPFE will keep a group count of the connections from a Peer Node Group to each server in the Target Set. Servers with a group count difference that is equal to or greater than D from the lowest group count will generally not be considered, such as, if D is 1, the effect is to	Format: Checkbox Default: Enable

Field	Description	Data Input Notes
	send the connection to the server with the lowest group count.	
Peer Node Group Distribution Threshold	The value D in Peer Node Aware	Format: Text field; numeric Range: 1 - 10 Default: 1
Primary Public IP Address		
*Address	Public IP address presented to the outside world. Do not edit if in use by a local node.	Format: IPv4 or IPv6 address
Active IPFE	IPFE that will primarily handle traffic for this TSA. If the active IPFE fails, then its mate will take over. IPFE-A1 and IPFE-A2 are mates. IPFE-B1 and IPFE-B2 are mates. If these options are disabled, IPFE Addresses under **IPFE>Configuration>Options** need to be configured.	Format: Options
Secondary Public IP Address		
Secondary Address	Optional secondary Public IP address presented to the outside world. For SCTP, this address will serve as a non-primary protocol-linked failover address. For TCP, this address can serve as an independent address. IF this field is populated, then the column Secondary IP Address Target Set IP List must be populated. Do not edit if in use by a local nodes.	Format: IPv4 or IPv6 address
Active IPFE for secondary address IPFE	The IPFE that will primarily handle traffic for this TSA's secondary address. If the active IPFE fails then its mate will take over. IPFE-A1 and IPFE-A1 are mates. IPFE-B1 and IPFE-B2 are mates. The setting for this field should complement the setting of Active IPFE in order to provide and alternative path for SCTP dual-homed traffic. This will allow SCTP connections with a very short heartbeat interval to transmit on the secondary path if the heartbeat timeout is short than the IPFE switchover delay.	Format: Options
Target Set IP List		

Field	Description	Data Input Notes
IP Address	Primary IPv4 or IPv6 address for the application server.	Format: Drop down menu
Secondary IP Address	Secondary IP address for the application server.	Format: Drop down menu
Description	Free-form description for the application server.	Format: Text field; alphanumeric
*Weighting	Weighting value used to apportion load between application servers within the Target Set. The following formula determines the selection of an application server: Application server's % chance of selection = (Application server weight / Sum of all weights in the Target Set) * 100. If all application servers have an equal weight, they have an equal chance of being selected. If application servers have unequal capacities, give a higher weight to the servers with the greater capacity.	Format: Text field; numeric Range: 0 - 65535

Viewing Target Sets

Use this task to view currently configured Target Sets.

Select **IPFE** > **Configuration >** > **Target Sets** from the active SOAM in a DSR topology.

The **IPFE -> Configuration -> Target Sets** page appears. The fields are described in *Table 9: Target Sets configuration elements (View pages)*.

Adding a Target Set

Before you can add a Target Set, you must configure at least one IPFE in **IPFE** > **Configuration** > **Options**.

Use this task to add a Target Set to the IPFE configuration. Define the list of application server IP addresses for the Target Set and associate the Target Set with an IPFE.

Target Sets associated with an IPFE may be completely overlapping, but may not be partially overlapping. A warning will appear if overlapping Target Sets are associated with an IPFE.

Partially overlapping target set example:
Target Set 1: Application Server 1, Application Server 2
Target Set 2: Application Server 2, Application Server 3

Completely overlapping target set example:

Target Set 1: Application Server 1, Application Server 2
Target Set 2: Application Server 1, Application Server 2

1. Select **IPFE > Configuration > Target Sets**.

   The **IPFE -> Configuration -> Target Sets** page appears. The fields are descibe in *Table 10: Target Sets configuration elements (Insert and Edit pages)*.

2. Click either **Insert IPv4** or **Insert IPv6**.

   The **IPFE -> Configuration -> Target Sets [Forminsert]** page appears.

   If no IPFE has been configured, an error message is displayed.

3. Under the **Target Set** section complete the following entries:
   a) Select the **TS Number** for the Target Set.
   b) Select the **Protocols** this Target Set will support.
   c) If you want to configure the Target Set, but not enable its use, select **Disable**.
   d) Set the **Delete Age** timer. The timer must be greater than Diameter Watchdog timer.
   e) Select **Hash** or **Least Load** in the **Load Balance Algorithm** field.

4. Under the **Least Load Parameters** section complete the following entries:
   a) Set the **MPS Factor**.
   b) Set the **Connection Count Factor**.
   c) Set the deviation percentage of **MPS Factor** and **Connection Count Factor** in the **Allowed Deviation** field.
   d) If you want to **Enable** Peer Node Group awareness when directing connections, check the box in the **Peer Node Aware Least Load** field.

      When enabled, the IPFE will distribute connections from the same Peer Node Group across servers in the Target Set to provide server redundancy for that group of peers. The IPFE keeps a group count of the connections from a Peer Node Group to each server in the Target Set. Servers with a group count difference that is equal to or greater than D from the lowest group count will generally not be considered, such as, if D is 1, the effect is to send the connection to the server with the lowest group count.

   e) Set the D value as describe in step 4d (**Peer Node Aware Least Load**) in the **Peer Node Group Distribution Threshold field**.

5. Under the **Primary Public IP Address** section complete the following entries:
   a) Provide an IP **Address** to represent this Target Set to the outside world.

      The IP address format will be either IPv4 or IPv6 depending on which button you selected in step 2. This IP address must reside on the XSI network.

   b) Select the **Active IPFE** that will primarily handle traffic for this TSA.

      If an IPFE is unavailable for selection, that IPFE has not been configured.

      If the Active IPFE fails then its mate will take over.

      If configured, the partner of the active IPFE will be the standby IPFE.

6. Under the **Secondary Public IP Address** section complete the following entries:
   a) Provide an optional **Secondary Address** that is a public IPv4 IP address to represent this Target Set to the outside world.

      For SCTP this address will serve as a non-primary protocol-linked failover address.

For TCP, this address can serve as an independent address.

If this field is populated then the column Secondary IP Address under Target Set IP List must be populated. Do not edit if in use by a local node.

b) Select the **Active IPFE for secondary address** that will handle traffic for this TSA's secondary address.

If the Active IPFE fails then its mate will take over.

7. Under the **Target Set IP List** section complete the following entries:
   a) Select an IP address in the **IP Address** field.

   This IP address must reside on the XSI network.

   b) Optionally, select a secondary IP address in the **Secondary IP Address** field.
   c) Enter a textual description for the application server in the **Description** field.
   d) Provide a weighting value in the **Weighting** field.

   The weighting value is used to control the traffic distribution among the application servers.

   e) Click **Add** to add another IP address to the list.

   You may add up to 16 IP addresses per Target Set.

8. Click:

   - **OK** to save the data and return to the **IPFE Configuration** page.
   - **Apply** to save the data and remain on this page.
   - **Cancel** to return to the **IPFE Configuration** page without saving any changes.

   If OK or Apply is clicked and any of the following conditions exist, an error message appears:

   - Any required field is empty (no entry was made)
   - Any field is not valid or is out of range
   - The maximum number of Target Sets (32) already exists in the system
   - The Target Set Address is already assigned to an IPFE
   - The Target Set Address is already assigned another Target Set
   - The Target Set Address is already used as the address of an application server
   - An IP address appears more than once in the Target Set IP List

   If **OK** or **Apply** is clicked and any of the following conditions exist, a warning message appears:

   - Partially overlapping **Target Sets** are associated with an IPFE.

After application servers have been added to a Target Set, the IPFE will distribute traffic across them.

Editing a Target Set

Use this task to edit a Target Set.

When the **IPFE Configuration Target Sets [Edit]** page opens, the fields are initially populated with the current values for the selected Target Set.

Target Sets associated with an IPFE may be completely overlapping, but may not be partially overlapping. A warning will appear if overlapping Target Sets are associated with an IPFE.

Partially overlapping target set example:
Target Set 1: Application Server 1, Application Server 2
Target Set 2: Application Server 2, Application Server 3

Completely overlapping target set example:
Target Set 1: Application Server 1, Application Server 2
Target Set 2: Application Server 1, Application Server 2

1. Select **IPFE > Configuration > Target Sets**.

   The **IPFE Configuration Target Sets** page appears.

2. Select the Target Set you want to edit, then click the **Edit**.

   The **Target Sets [Edit]** page appears.

3. Update the relevant fields.

   For more information about each field please see *Table 10: Target Sets configuration elements (Insert and Edit pages)*.

   An IP Address can be removed from the **Target Set IP List** by clicking the X at the end of the **Weighting** field. The Target Set IP cannot be modified.

4. Click:

   - **OK** to save the changes and return to the **IPFE Configuration Target Sets** page.
   - **Apply** to save the changes and remain on this page.
   - **Cancel** to return to the **IPFE Configuration Target Sets** page without saving any changes.

   If **OK** or **Apply** is clicked and any of the following conditions exist, an error message appears:

   - The selected Target Set no longer exists; it has been deleted by another user
   - Any required field is empty; no value was entered or selected
   - The entry in any field is not valid (wrong data type or out of the valid range)
   - The Target Set Address is already assigned to an IPFE
   - The Target Set Address is already assigned another Target Set
   - The Target Set Address is already used as the address of an application server
   - An IP address appears more than once in the Target Set IP List
   - The DA-MP is deleted from the Target Set IP.

   If **OK** or **Apply** is clicked and any of the following conditions exist, a warning message appears:

   - Partially overlapping Target Sets are associated with an IPFE.

Deleting a Target Set

Use this task to delete a Target Set.

1. Select **IPFE > Configuration > Target Sets**.

   The **IPFE Configuration Target Sets** page appears.

2. Select the Target Set you want to delete then click **Delete**.

A popup window appears to confirm the delete.

3. Click:

   - **OK** to delete the Target Set.
   - **Cancel** to cancel the delete function and return to the **IPFE Configuration Target Sets** page.

   If **OK** is clicked and the Target Set Address is specified as an IP Address for Diameter transport connections to a Local Node, an error message is displayed and the Target Set is not deleted.

   If **OK** is clicked and the selected Target Set no longer exists (it was deleted by another user), an error message is displayed and the Target Sets view is refreshed.

Glossary

A

ARP	Address Resolution Protocol ARP monitoring uses the Address Resolution Protocol to determine whether a remote interface is reachable.
Association	An association refers to an SCTP association. The association provides the transport for protocol data units and adaptation layer peer messages.

I

IMI	Internal Management Interface
IPFE	IP Front End A traffic distributor that routes TCP traffic sent to a target set address by application clients across a set of application servers. The IPFE minimizes the number of externally routable IP addresses required for application clients to contact application servers.

N

NOAM	Network Operations, Administration, and Maintenance

S

SCTP	Stream Control Transmission Protocol An IETF transport layer protocol, similar to TCP, that sends a message in one operation.

S

	The transport layer for all standard IETF-SIGTRAN protocols. SCTP is a reliable transport protocol that operates on top of a connectionless packet network such as IP and is functionally equivalent to TCP. It establishes a connection between two endpoints (called an association; in TCP, these are sockets) for transmission of user messages.
SOAM	System Operations, Administration, and Maintenance

T

Target Set Address	See TSA.
TCP	Transmission Control Protocol A connection-oriented protocol used by applications on networked hosts to connect to one another and to exchange streams of data in a reliable and in-order manner.
Throttling	A mechanism to limit the number of messages being routed to a particular destination based on the various factors, like Event Type, Event Origination, Event Destination, and Shed Rate.
TSA	Target Set Address An externally routable IP address that the IPFE presents to application clients. The IPFE distributes traffic sent to a target set address across a set of application servers.