Oracle® Communications Diameter Signaling Router

IP Front End (IPFE) User's Guide

E53473 Revision 01

July 2014

Oracle® Communications IP Front End (IPFE) User's Guide

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Topics:

This chapter contains an overview of how to configure IP Front End (IPFE). The contents include sections on the scope, audience, and organization of the documentation, and how to contact Oracle for assistance.

Overview

The *IP Front End (IPFE) User's Guide* provides information about how to use the DSR GUI to configure IPFE.

The document provides procedures to:

- Specify IPFE Configuration Options
- Configure IPFE Target Sets

Scope and Audience

This manual does not describe how to install or replace software or hardware.

This manual is intended for personnel who configure IPFE.

This manual contains procedures for configuring IPFE using the DSR GUI.

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

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.

My Oracle Support (MOS)

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

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

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

You will be connected to a live agent who can assist you with MOS registration and provide Support Identifiers. Simply mention you are a Tekelec Customer new to MOS.

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

Emergency Response

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

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

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system’s ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions

- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

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

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 Technology Network (OTN) site. See *Locate Product Documentation on the Oracle Technology Network Site* for more information.

Locate Product Documentation on the Oracle Technology Network Site

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

1. Log into the Oracle Technology Network site at *http://docs.oracle.com*.
2. Under **Applications**, click the link for **Communications**.
   The **Oracle Communications Documentation** window opens with Tekelec shown near the top.
3. Click **Oracle Communications Documentation for Tekelec Products**.
4. Navigate to your Product and then the Release Number, and click the **View** link (the **Download** link will retrieve the entire documentation set).
5. To download a file to your location, right-click the PDF link and select **Save Target As**.

Chapter 2

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 are divided into up to 16 groups, called Target Sets. Each of the target sets are assigned a shared Target Set Address. The IPFE Architecture assumes that 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 to which it can establish a connection if the first connection fails.

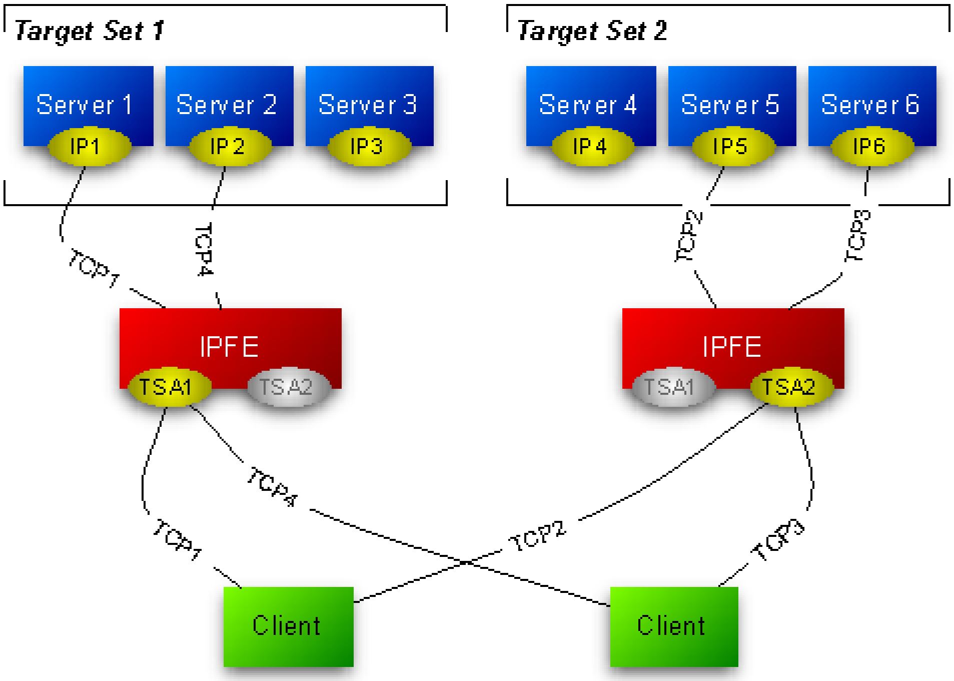

Figure 1: IPFE Architecture

When the IPFE routes packets to application servers, it does not perform any rewriting of the packet. This means 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).

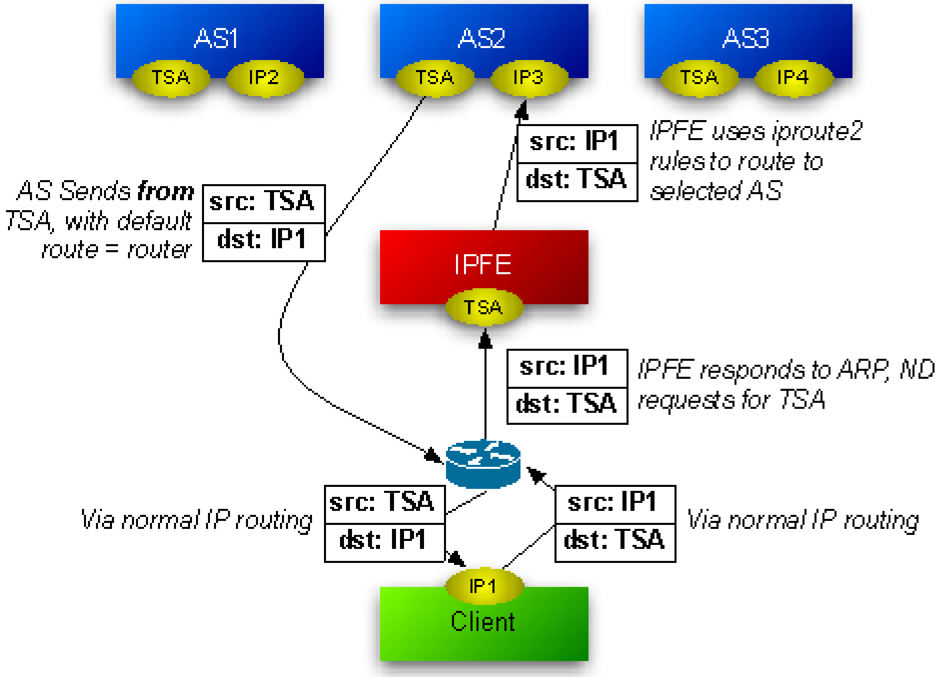

Figure 2: Packet Routing Through and Around the IPFE

Traffic distribution

The IPFE (IP Front End) is a packet-based load balancer that makes a large DSR 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. 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 IPv4 or IPv6 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.

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.

Association Aging

Because the IPFE has no visibility into the transaction state between client and application server, it cannot know if an association no longer represents an active connection. The IPFE makes available a per **Target Set** configuration parameter, known as **Delete Age**, that specifies the elapse of time after which an association is to be deleted. The IPFE will treat packets that had their associations deleted as new packets and will run the application server selection function for them.

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 achieved 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.

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 colocated 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.

DSR Bulk Import and Export

The following documents describe the use and operation of DSR Bulk Import and Export functions:

- *Diameter Common User's Guide*,
- **Help** > **Diameter Common** > **DSR Bulk Import**
- **Help** > **Diameter Common** > **DSR Bulk Export**

The DSR Bulk Import and Export functions can be used to export Diameter, IPFE, and DSR 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.

Configuration data refers to any data that is configured for one of the Export **Export Application** types (FABR, RBAR, PDRA, GLA , MAPIWF, or CPA and SBR DSR Applications; IPFE; and the Diameter components). "Diameter" includes Diameter Configuration components and Diameter Common Network Identifiers and MPs components.

DSR Bulk Export

The DSR Bulk Export operation creates ASCII Comma-Separated Values (CSV) files (.csv) containing Diameter , IPFE, and DSR Application configuration data. Exported configuration data can be edited and used with the DSR 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 DSR 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.

The following configuration data can be exported in one Export operation:

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

Exported files can be written to the File Management Directory in the local File Management area (**Status & Manage > File** 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.

DSR Bulk Import

The DSR 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 "DSR Bulk Import" section of 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 DSR 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 DSR release that is used to import the file.

Files that are created using the DSR 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 on a computer; 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.

The following 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.

Chapter 3

IPFE Configuration Options

Topics:

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

Configuration Options elements

An asterisk after the value field means that the configuration is mandatory.

Table 2: IPFE Configuration Elements

Element	Description	Data Input Notes
Inter-IPFE Synchronization		
IPFE-A1 IP Address	The IPv4 or IPv6 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 IPv4 or IPv6 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 IPv4 or IPv6 address of IPFE-B1.	Format: IPv4 or IPv6 address, or left blank

Element	Description	Data Input Notes
	This selection is disabled when a Target Set has IPFE-B1 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.	Default: blank
IPFE-B2 IP Address	The IPv4 or IPv6 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: IPv4 or IPv6 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		

Element	Description	Data Input Notes
* Application Traffic Min Port	TCP/SCTP port range for traffic distribution. This is the minimum of the range. This is the range of ports for which the IPFE will accept traffic. If the port is outside of the specified range, the IPFE will ignore the packet and not forward it. Setting the range to 0-65535 removes the port constraint.	Format: numeric Range: 0 - less than or equal to the **Application Traffic Max Port** Default: 0
* Application Traffic Max Port	TCP/SCTP port range for traffic distribution. This is the maximum of the range. This is the range of ports for which the IPFE will accept traffic. If the port is outside of the specified range, the IPFE will ignore the packet and not forward it. Setting the range to 0-65535 removes the port constraint.	Format: numeric Range: greater than or equal to the **Application Traffic Min Port** - 65535 Default: 65535
* 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 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.	Format: pull-down list Range: • TCP Reset • 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 STCP 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	Format: pull-down list Range: • Drop Packet • ICMP Host Unreachable • ICMP Port Unreachable • ICMP Administratively Prohibited Default: ICMP Host Unreachable

Element	Description	Data Input Notes
	can be best handled by the application client.	
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 (MOS)*. Contact the *My Oracle Support (MOS)* before disabling measurements and overload detection.	Format: pull-down list Range: • Enabled • Disabled Default: Enabled
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	Format: numeric Range: 1-65535 Default: 9675

Element	Description	Data Input Notes
	address and this port. The application server must listen on this port and should send heartbeats.	
* 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 heartbeat messages from the application servers. When the protocol is set to Heartbeat, the IPFE connects to the monitoring port, sustains the	Format: pull-down list Range: • Heartbeat • None Default: Heartbeat

Element	Description	Data Input Notes
	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 **Configuration Options** fields set up data replication between IPFEs, specify port ranges for TCP traffic, and set application server monitoring parameters.

1. Select **IPFE > Configuration > Options**.

   The **Configuration Options** page appears. Field descriptions are provided by *Configuration Options elements*.

2. 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.

3. Specify the traffic port range by entering a minimum port number in the **Application Traffic Minimum Port** field and a maximum port number in the **Application Traffic Maximum Port** field.

   This is the range of ports for which the IPFE will accept traffic. If the port is outside of the specified range, the IPFE will ignore the packet and not forward it to the application servers.

   Setting the range to 0-65535 removes the port constraint.

4. Set the Packet Counting options.
5. Set the Application Server Monitoring options.
6. 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*.

Chapter 4

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 STCP heartbeat interval may require this value to be increased from default.

The **Target Sets** Page describes the fields on the Target Sets View, Insert, and Edit pages. Data Input Notes apply only to the Insert and Edit pages; the View page is read-only.

Table 3: 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: radio buttons 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: radio buttons Range: IPFE-A1, IPFE-A2, IPFE-B1, IPFE-B2

Field	Description	Data Input Notes
		Default: IPFE-A1 If a radio button 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 4: Target Sets configuration elements (Insert and Edit pages)

Field	Description	Data Input Notes
Target Set		
* TS Number	Unique ID identifying the TSA.	Format: pulldown menu Range:1-32 Default: 1
Protocols	A Target Set can support SCTP, TCP, or both.	Format: radio boxes 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.	Format: Radio box Range: Hash, Least Load Default: Least Load

Field	Description	Data Input Notes
	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 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.	
* 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 box; 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 box; 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	Format: text box; numeric Range: 0 - 50 Default: 5

Field	Description	Data Input Notes
	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.	
Primary Public IP Address		
* Address	Public IPv4 or IPv6 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 radio buttons are diasbled, IPFE Addresses under IPFE>Configuration>Options need to be configured.	Format: Radio buttons
Secondary Public IP Address		
Secondary Address	Optional secondary Public IPv4 or IPv6 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

Field	Description	Data Input Notes
Active IPFE for secondary address	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: Radio buttons
Target Set IP List		
IP Address	Primary IPv4 or IPv6 address for the application server.	Format: Pulldown menu
Secondary IP Address	Secondary IPv4 or IPv6 address for the application server.	Format: Pulldown menu
Description	Free-form description for the application server.	Format: Text box; 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 box; numeric Range: 0 - 65535

Viewing Target Sets

Use this task to view currently configured Target Sets.

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

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

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.

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

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

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

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

   If no IPFE has been configured, an error message is displayed.
3. Select the Target Set number for the Target Set.
4. 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.
5. Select the transport protocols this Target Set will support.
6. If you want to configure the Target Set, but not enable its use, select **Disable**.
7. Select the **Active IPFE** that the Target Set will be associated with.

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

   If configured, the partner of the active IPFE will be the standby IPFE.
8. Provide a list of IP addresses for the application servers.
   a) Select an IP address in the **IP Address** field.

      This IP address must reside on the XSI network.

   b) Enter a textual description for the application server in the **Description** field.

   c) Provide a weighting value in the **Weighting** field.

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

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

      You may add up to 16 IP addresses per Target Set.
9. 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

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.

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 *Target Sets configuration elements*.

   An IP Address can be removed from the **Target Set IP List** by clicking the X at the end of the **Weighting** field.

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

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.

Auto Reply service. Personalized SMS auto reply service. This service is provided by the Mobile Messaging XS-ARP component.

Allocation and Retention Priority. A mechanism to downgrade lower-priority bearers, or upgrade higher-priority bearers, in cases of network congestion or emergency. Used when a service or bearer is admitted, allocated, or handed over.

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.

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.

T

TCP

Transfer-Cluster-Prohibited

Transfer Control Protocol

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.