EAGLE® XG Diameter Signaling Router

IP Front End (IPFE) User Guide

910-6637-001 Revision A
April 2013

Table of Contents

List of Tables

Chapter 1

Introduction

Topics:

This chapter contains an overview of how to configure IPFE. The contents include sections on the scope, audience, and organization of the documentation, and how to contact Tekelec for assistance.

Overview

The IP Front End (IPFE) document 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.

Manual Organization

This document 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

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

	**WARNING**: (This icon and text indicate the possibility of *equipment damage*.)
	**CAUTION**: (This icon and text indicate the possibility of *service interruption*.)

Related Publications

The Diameter Signaling Router (DSR) product set includes the following publications, which provide information for the configuration and use of DSR and related applications.

Getting Started includes a product overview, system architecture, and functions. It also explains the DSR GUI features including user interface elements, main menu options, supported browsers, and common user interface widgets.

Feature Notice describes new features in the current release, provides the hardware baseline for this release, and explains how to find customer documentation on the Customer Support Site.

Roadmap to Hardware Documentation provides links to access manufacturer online documentation for hardware related to the DSR.

Operation, Administration, and Maintenance (OAM) Guide provides information on system-level configuration and administration tasks for the advanced functions of the DSR, both for initial setup and maintenance.

Communication Agent User Guide explains how to use the Communication Agent GUI pages to configure Remote Servers, Connection Groups, and Routed Servers, and to maintain configured connections.

Diameter and Mediation User Guide explains how to use the Diameter GUI pages to manage the configuration and maintenance of Local and Peer Nodes, connections, Configuration Sets, Peer Routing Rules, Application Routing Rules, and System, DNS, and Local Congestion options; and explains how to configure and use Diameter Mediation.

IP Front End (IPFE) User Guide explains how to the use the IPFE GUI pages to configure IPFE to distribute IPv4 and IPv6 connections from multiple clients to multiple nodes.

Range-Based Address Resolution (RBAR) User Guide explains how to use the RBAR GUI pages to configure RBAR to route Diameter end-to-end transactions based on Diameter Application ID, Command Code, Routing Entity Type, and Routing Entity address ranges and individual addresses.

Full-Address Based Resolution (FABR) User Guide explains how to use the FABR GUI pages to configure FABR to resolve designated Diameter server addresses based on Diameter Application ID, Command Code, Routing Entity Type, and Routing Entity addresses.

Charging Proxy Application (CPA) and Offline Charging Solution User Guide describes the Offline Charging Solution and explains how to use the CPA GUI pages to set System Options for CPA, configure the CPA's Message Copy capability, and configure the Session Binding Repository for CPA.

Policy DRA User Guide describes the topology and functions of the Policy Diameter Routing Agent (Policy DRA or P-DRA) DSR application and the Policy Session Binding Repository, and explains how to use the Policy DRA GUI pages to configure P-DRA.

DSR Alarms, KPIs, and Measurements Reference Guide provides detailed descriptions of alarms, events, Key Performance Indicators (KPIs), and measurements; indicates actions to take to resolve an alarm, event, or unusual Diameter measurement value; and explains how to generate reports containing current alarm, event, KPI, and measurement information.

DSR Administration Guide describes DSR architecture, functions, configuration, and tools and utilities (IPsec, Import/Export, DIH, and database backups); and provides references to other publications for more detailed information.

Customer Care Center

The Tekelec Customer Care Center is your initial point of contact for all product support needs. A representative takes your call or email, creates a Customer Service Request (CSR) and directs your requests to the Tekelec Technical Assistance Center (TAC). Each CSR includes an individual tracking number. Together with TAC Engineers, the representative will help you resolve your request.

The Customer Care Center is available 24 hours a day, 7 days a week, 365 days a year, and is linked to TAC Engineers around the globe.

Tekelec TAC Engineers are available to provide solutions to your technical questions and issues 7 days a week, 24 hours a day. After a CSR is issued, the TAC Engineer determines the classification of the trouble. If a critical problem exists, emergency procedures are initiated. If the problem is not critical, normal support procedures apply. A primary Technical Engineer is assigned to work on the CSR and provide a solution to the problem. The CSR is closed when the problem is resolved.

Tekelec Technical Assistance Centers are located around the globe in the following locations:

Tekelec - Global

Email (All Regions): support@tekelec.com

- **USA and Canada**

  Phone:

  1-888-FOR-TKLC or 1-888-367-8552 (toll-free, within continental USA and Canada)

  1-919-460-2150 (outside continental USA and Canada)

  TAC Regional Support Office Hours:

  8:00 a.m. through 5:00 p.m. (GMT minus 5 hours), Monday through Friday, excluding holidays

- **Caribbean and Latin America (CALA)**

  Phone:

  +1-919-460-2150

  TAC Regional Support Office Hours (except Brazil):

  10:00 a.m. through 7:00 p.m. (GMT minus 6 hours), Monday through Friday, excluding holidays

  - **Argentina**

    Phone:

    0-800-555-5246 (toll-free)

- **Brazil**

  Phone:

  0-800-891-4341 (toll-free)

  TAC Regional Support Office Hours:

  8:00 a.m. through 5:48 p.m. (GMT minus 3 hours), Monday through Friday, excluding holidays
- **Chile**

  Phone:

  1230-020-555-5468
- **Colombia**

  Phone:

  01-800-912-0537
- **Dominican Republic**

  Phone:

  1-888-367-8552
- **Mexico**

  Phone:

  001-888-367-8552
- **Peru**

  Phone:

  0800-53-087
- **Puerto Rico**

  Phone:

  1-888-367-8552 (1-888-FOR-TKLC)
- **Venezuela**

  Phone:

  0800-176-6497

- **Europe, Middle East, and Africa**

  Regional Office Hours:

  8:30 a.m. through 5:00 p.m. (GMT), Monday through Friday, excluding holidays

  - **Signaling**

    Phone:

    +44 1784 467 804 (within UK)
  - **Software Solutions**

    Phone:

    +33 3 89 33 54 00

- **Asia**
  - **India**

    Phone:

    +91-124-465-5098 or +1-919-460-2150

    TAC Regional Support Office Hours:

    10:00 a.m. through 7:00 p.m. (GMT plus 5 1/2 hours), Monday through Saturday, excluding holidays
  - **Singapore**

    Phone:

    +65 6796 2288

    TAC Regional Support Office Hours:

    9:00 a.m. through 6:00 p.m. (GMT plus 8 hours), Monday through Friday, excluding holidays

Emergency Response

In the event of a critical service situation, emergency response is offered by the Tekelec Customer Care Center 24 hours a day, 7 days a week. 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 the Tekelec Customer Care Center.

Locate Product Documentation on the Customer Support Site

Access to Tekelec's Customer Support site is restricted to current Tekelec customers only. This section describes how to log into the Tekelec Customer Support site and locate a document. Viewing the document requires Adobe Acrobat Reader, which can be downloaded at www.adobe.com.

1. Log into the *Tekelec Customer Support* site.

Note: If you have not registered for this new site, click the **Register Here** link. Have your customer number available. The response time for registration requests is 24 to 48 hours.

2. Click the **Product Support** tab.
3. Use the Search field to locate a document by its part number, release number, document name, or document type. The Search field accepts both full and partial entries.
4. Click a subject folder to browse through a list of related files.
5. To download a file to your location, right-click the file name 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.

Traffic distribution

The IPFE presents one or more externally routable IP addresses to accept TCP or unihomed SCTP traffic from clients. These externally visible addresses are known as Target Set Addresses (TSAs). Each TSA has an associated set of IP addresses for application servers, up to 16 addresses, known as a Target Set. The IP addresses in a given Target Set are of the same IP version (that is, IPv4 or IPv6) as the associated TSA.

A typical client is configured to send TCP or SCTP traffic to one or more of the TSAs, rather than directly to an application server. When the IPFE receives a packet at a TSA, it first checks to see if it has state that associates the packet's source address and port to a particular application server.

This state is known as an "association." If no such association exists (that is, the packet was an "initial" packet), the IPFE runs a selection function to choose an application server address from the eligible addresses in the Target Set. The selection function uses a configurable weighting factor when selecting the target address from the list of eligible addresses. The IPFE routes the packet to the selected address, and creates an association mapping the source address and port to the selected address. When future packets arrive with the same source address and port, the IPFE routes them to the same selected address according the association.

The IPFE sees only packets sent from client to server. Return traffic from server to client bypasses the IPFE for performance reasons. However, the client's TCP or SCTP stack "sees" only one address for the TSA; that is, it sends all traffic to the TSA, and perceives all return traffic as coming from the TSA.

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

In high-availability configurations, four IPFEs may be deployed as two mated pairs, with each pair sharing TSAs and Target Sets. The mated pairs share sufficient state so that they may identically route any client packet sent to a given TSA.

Connection balancing

Under normal operation, the IPFE distributes connections among application servers according to the weighting factors defined in the Target Sets. However, certain failure and recovery scenarios can result in an application server having significantly more or fewer connections than is intended by its weighting factor. The IPFE considers the system to be "out of balance" if this discrepancy is so large that the overall system cannot reach its rated capacity even though individual application servers still have capacity to spare, or so that a second failure is likely to cause one of the remaining servers to become overloaded. The IPFE determines this by measuring the number of packets sent to each server and applying a "balance" heuristic.

When the IPFE detects that the system is out of balance, it sets an alarm and directs any new connections to underloaded application servers to relieve the imbalance.

Overload handling

If the IPFE itself becomes overloaded, it will drop packets. From the application server and client perspectives, this packet loss will appear as network congestion. Their transport stacks will transparently recover from minor packet loss.

If the IPFE becomes overloaded because it has exceeded the rated number of connections, it will invalidate related state entries on a least recently used basis.

If an application server becomes overloaded, the IPFE will remove the application server from the Target Set and direct client connections to the other application servers within the Target Set.

High availability

When paired with another IPFE instance and configured with at least two Target Set Addresses, the IPFE supports high availability. In the case of an IPFE pair and two Target Set Addresses, each IPFE is configured to handle one Target Set Address. Each IPFE is automatically aware of the ruleset for the secondary Target Set Address. If one IPFE should become unavailable, the other IPFE becomes active for the failed IPFE's Target Set Address while continuing to handle its own.

In the case of an IPFE pair, but only one Target Set Address, then one IPFE is active for the Target Set Address and the other is standby.

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.

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 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 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. This address must reside on the IMI (internal management interface) network. This address is used for replicating association	Format: IPv4 or IPv6 address, or left blank Default: blank

Element	Description	Data Input Notes
	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 IPv4 or IPv6 address of IPFE-B2. 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
Traffic Forwarding		
Per-TSA Association Limit	The maximum number of concurrent TCP or SCTP connections for one TSA. To limit memory consumption, the IPFE limits the number of associations with the most recent packet activity to this setting. Memory is consumed at a rate of 224 bytes per association per TSA.	Format: numeric Range: 0-65535 Default: 12000

Element	Description	Data Input Notes
	This configuration should be set to 10% higher than the expected load. If this value is set to a lower value than the current number of associations stored, then the IPFE will remove the oldest entries until the number of stored associations is no more than this setting. Setting this value too low could cause current connections to be dropped when the state of the application servers change.	
Application Traffic Min Port	Traffic balancing port range. 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 **Load Balance Max Port** Default: 0
Application Traffic Max Port	Traffic balancing port range. 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 **Load Balance Min Port** - 65535 Default: 65535
Application Traffic TCP Reject Option	How to reject 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	Format: pull-down list Range: • TCP Reset • Drop Packet • ICMP Host Unreachable • ICMP Port Unreachable

Element	Description	Data Input Notes
	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.	• ICMP Administratively Prohibited Default: TCP Reset
Application Traffic SCTP Reject Option	How to reject 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 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	Value below which no throughput analysis is performed regarding imbalance detection. 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
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 Tekelec Customer Care.	Format: pull-down list Range: • Enabled • Disabled Default: Enabled

Element	Description	Data Input Notes
	Contact Tekelec Customer Care 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 it should either accept TCP connections or send heartbeats, depending on the monitoring protocol selected.	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 re-connect to it based on this configuration. This configuration is used for both monitoring protocols.	Format: numeric, seconds Range: 1 - 255 Default: 10

Element	Description	Data Input Notes
Monitoring Protocol	Application liveness monitoring method. The monitoring protocol allows the IPFE to determine the liveness of the application servers. The IPFE can determine this either by sending TCP traffic to the application servers or by listening for heartbeat messages from the application servers. • TCP Connection - The IPFE connects to the monitoring port and drops the connection immediately if it is successful, which indicates that the application server is live. This is only selected if the application server (for instance, a non-Tekelec server) cannot send a heartbeat. • 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.	Format: pull-down list Range: • TCP Connection • Heartbeat • None Default: Heartbeat

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

Table 3: Target Sets configuration elements 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

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. The following formula is used to determine 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: 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

Field	Description	Data Input Notes
		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 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.

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

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. 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	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.

T

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.