EAGLE® XG Diameter Signaling Router

Release 4.0 Feature Notice

Tekelec

Table of Contents

List of Tables

Chapter

1

EAGLE XG DSR

Topics:

This chapter includes feature descriptions, provides the hardware baseline for this release, and explains how to find customer documentation on the Customer Support Site.

Introduction

Diameter Signaling Router (DSR) is a core Diameter signaling and routing solution for operators' LTE, IMS, and 3G networks. This Feature Notice includes feature descriptions, provides the hardware baseline for this release, and explains how to find customer documentation on the Customer Support Site.

Feature notices are distributed to customers with each new release of software.

This Feature Notice includes the following topics:

- *DSR 3-Tiered Topology*
- *Application Aware Answers*
- *Measurements Refactoring*
- *Scheduled Bulk Export*
- *Maximum Message Size*
- *Increased DSR Local Nodes*
- *Alternate-routing across Route Groups in a Route List*
- *Routing Option Sets*
- *Pending Answer Timer*
- *PRT Partitioning*
- *Remote BUSY Congestion*
- *Per Connection Egress Message Control Features*
- *User-Configurable Message Priority*
- *Internet Protocol Front End (IPFE) release enhancements*
- *Scalability*

System architecture

DSR 4.0 introduces the 3-tiered DSR topology.

The DSR can be deployed either as a core router that routes traffic between Diameter elements in the home network, or as a gateway router that routes traffic between Diameter elements in the visited network and the home network.

The DSR product supports:

- A 2-tiered DSR topology
- A 3-tiered DSR topology

In 2-tiered DSR topology, a pair of NOAM servers for each DSR interacts directly with DA-MPs in that DSR system.

In 3-tiered DSR topology, the OAM server function is split into Network OAM (NOAM) servers and System OAM (SOAM) servers. A DSR with a pair of NOAM servers (a DSR NO) is connected to multiple DSRs in the network. Each DSR is connected to a mated pair of SOAM servers. Each DSR SOAM supports up to 16 DA-MPs.

The same functions are provided in both topologies. The 3-tiered DSR topology does not alter existing DSR functions other than separating what can be configured or managed at what level (DSR NOAM or DSR SOAM).

2-tiered DSR Topology

In 2-tiered DSR topology, there are NOAM servers and DA-MPs.

On NOAM servers, GUI screens can be used to configure and manage:

- Network topology data (such as user accounts, network elements, servers, and server groups)
- Diameter signaling data (such as Local Nodes, Peer Nodes, Connections, Route Groups, and Route Lists) and DSR Application data (RBAR, FABR, and CPA)

The DA-MPs process the database updates from NOAM servers and perform the real-time signaling functions. The DA-MPs also supply the Platform measurements, events, alarms, and log (MEAL) data, Diameter signaling MEAL data, and Diameter Application MEAL data to NOAM servers.

3-tiered DSR Topology

The primary change between the 2-tiered DSR topology and the 3-tiered DSR topology is the introduction of the DSR SOAM server. In 3-tiered DSR topology, there are NOAM servers, SOAM servers, and DA-MPs.

The role of the DSR NOAM server is changed to take on network scope instead of the Network Element scope it has with the 2-tiered DSR topology. The role of the DSR SOAM becomes similar to the role of the NOAM in the 2-tiered DSR topology in that it is managing a single DSR system (or DSR Signaling NE).

In 3-tiered DSR topology, GUI screens can be used to configure and manage:

- Network topology data (such as user accounts, network elements, servers, and server groups) on a DSR NOAM
- Diameter signaling data (such as Local Nodes, Peer Nodes, Connections, Route Groups, and Route Lists) and DSR Application data (RBAR, FABR, and CPA) on a DSR SOAM

The DA-MPs process the database updates from NOAM servers and SOAM servers and perform the real-time signaling. The DA-MPs also supply the Platform MEAL data, Diameter signaling MEAL data, and DSR Application MEAL data to SOAM servers. The SOAM servers retain the Diameter signaling MEAL data and DSR Application MEAL data, and send the Platform MEAL data to the NOAM servers.

The 3-Tiered OAM architecture provides the following advantages:

- Centralized management of security for all DSRs in the network.

  - User Authentication, Grouped based Authorization, Single Sign-On, and GUI Session Management.

- Centralized configuration and management of core platform components for all DSRs in the network.

  - Configuration of new DSR network elements.
  - Blade installation and configuration: Role (such as SOAM, DA-MP, IPFE), IP networking, HA configuration, and SNMP Managers.
  - Stop/Start Application, HA Role switch, and Reboot any blade in any DSR in the network.

- Centralized monitoring and collection of health and performance data on core components of all DSRs in the network.

  - CPU, RAM, Swap, Uptime Measurements, KPIs and Alarms for all DSR blades in the network.
  - Database and HA health and performance measurements, KPIs, and Alarms for all DSR blades in the network.
  - Alarm status and Process monitoring for all DSR blades in the network.
  - User-configuration and scheduling of Performance Data report generation and export.

- Centralized installation and upgrade of all DSRs in the network.
- Aligns with Tekelec SDS and HLR Router OAM architecture.

Deployment with SDS

DSR deployments that include support for the DSR Full Address Based Resolution (FABR) application must be deployed with the Subscriber Database Server (SDS). The SDS is used to provision the FABR subscriber data.

The SDS/DP system consists of a Primary Provisioning Site, a Disaster Recovery (DR) Provisioning Site, and up to 24 DSR Signaling Site servers with redundant DP SOAM servers and up to 2 DP blades. Each Provisioning Site has an active/standby pair of servers in a high availability (HA) configuration and a third server configured as a Query Server (QS).

In 2-tiered DSR topology, the SDS has its own independent NOAM and SOAM infrastructure.

In 3-tiered DSR topology, the DSR SOAM and the SDS SOAM servers are run on the DSR OAM blade using virtualization technology. It is assumed that most deployments that support both DSR and SDS will deploy the DSR NOAM on Rack Mount Servers (RMS), as this is how the SDS NOAM is deployed. Small deployments that minimize the amount of hardware investment require the DSR NOAM to be deployed as a virtual server on the OAM blade. This requires running three Virtual Machines (VMs) on the blade – DSR NOAM, DSR SOAM and SDS SOAM.

EAGLE XG DSR 4.0 Hardware Configuration

An EAGLE XG DSR 4.0 network element requires a hardware configuration that uses HP servers. *Table 1: Hardware Frame* shows this requirement. You may contact Tekelec *Customer Care Center* for assistance purchasing or installing the hardware for your configuration.

Table 1: Hardware Frame

Description	Function	Quantity	Notes
Cabinet with power, cabling, and optional aggregation switches	Frame	Minimum: 1 per site Maximum: 1	
HP BL460C G6 Blade Server	OAM Server	Minimum: 2 per site Maximum: 2 per site	One pair per site; provisioned as Active/Standby

Description	Function	Quantity	Notes
	DA-MP Server (Message Processor server)	Minimum: 2 Maximum: 2	DA-MP servers are provisioned as Active/Standby **Note:** In multi-active configurations, the minimum is 1 and the maximum is 16.
	optional Diameter Intelligence Hub (DIH)	Minimum: 0 Maximum: 1	Plus storage blade and hard drives
HP C-7000 enclosure with switches	Houses the HP BL460C G6 blade servers	Minimum: 1 per cabinet Maximum: 2 per cabinet	
DL380 G6 Rack Mount Server (DC) or DL360 G6 Rack Mount Server (AC)	Management Server	Minimum: 1 per site Maximum: 1 per site	
HP ProLiant BLA460C G8 Server Blade	Server Blade	Minimum: 1 per site Maximum: 1 per site	
HP ProLiant DL380P G8 Server Blade	Application Server	Minimum: 1 per site Maximum: 1 per site	
HP ProLiant DL360P G8 Server Blade	Application Server	Minimum: 0 per site Maximum: 16 per site	
HP ProLiant BL620C G7 Server Blade	Server Blade	Minimum: 0 per site Maximum: 16 per site	

Compatibility

The table below shows the compatibility of EAGLE XG DSR 4.0 with the releases of interfacing external systems.

Table 2: DSR 4.0 Compatibility with External Systems

Product	Release	Compatibility
DIH	7.0 and 7.1	Fully compatible
SDS	4.0	Fully compatible
PCRF	9.0	Fully compatible

Chapter
2

Communication Agent

Topics:

This chapter provides an overview of the EAGLE XG DSR 4.0 Communication Agent.

Communication Agent Overview

Communication Agent (ComAgent) is included with DSR 4.0 to provide infrastructure features and services for enabling inter-server communication. ComAgent provides the connection management, reliable routing services and software compatibility management, and supports mechanisms for exchange of StackEvents between stacks hosted on different Message Processors (DA-MPs). ComAgent successfully routes messages between layers across processes and servers.

The Communication Agent's Routed Service provides a means by which local applications hosted on an DA-MP can send traffic to applications on other DA-MPs. The Communication Agent's Routed Service will have Connection Groups associated with the service assigned with different priorities. When an application sends events to other servers using a routed service, the Communication Agent chooses a connection in the highest priority group for that routed service and sends the event on that connection. The load-balancing accounts for:

- Connection Group status (an aggregation of member connection status)
- Connection availability status (same as server availability status)
- Connection Egress Congestion Level (CL)

  - Transport Connection Congestion Level (TCL)
  - DA-MP Overload Level (OL) of peer server

Note: ComAgent supports one Routed Service and one Connection Group per Routed Service.

The Communication Agent menu also provides a means to monitor the operational status of High-Availability (HA) Services Sub-Resources. The HA Services enables a server application, such as DSR (Charging) SBR, to load-share its active functions across a set of servers and to notify clients, such as DSR and CPA, of the placement of its active functions onto servers in a manner that allows the clients to send stack events to the active functions. The set of active functions is called a Resource and each active function instance is called a Sub-Resource.

Chapter

3

EAGLE XG DSR 4.0 Features

Topics:

EAGLE XG DSR creates a centralized core Diameter signaling layer that relieves LTE, IMS, and 3G Diameter endpoints of routing, traffic management, and load balancing tasks and provides a single interconnect point to other networks.

EAGLE XG DSR 4.0 inherits all functionality of DSR 3.0 with the addition of new and enhanced features/functionality as described herein.

DSR 3-Tiered Topology

In 3-tiered DSR topology, the OAM server function is split into Network OAM (NOAM) servers and System OAM (SOAM) servers. A DSR with a pair of NOAM servers is connected to multiple DSRs with SOAM servers in the network. Each DSR with NOAM servers is connected to a mated pair of SOAM servers. The DA-MP servers reside with a pair of SOAM servers that interact directly with the DA-MP servers on that DSR.

The 3-tiered DSR topology does not alter existing DSR functions other than separating what can be configured or managed at what level (DSR NOAM or DSR SOAM).

The architecture includes the following characteristics:

- Each DSR services signaling traffic to and from a collection of Diameter clients, servers, and agents.
- The DSR DA-MPs provide the Diameter message handling function. The DSR MP supports connections to all of the DSR Peers.
- DSRs are deployed in mated pairs for purposes of geo-redundancy. Each DSR operates at 40% capacity under normal conditions.
- The Diameter Intelligence Hub (DIH) provides the ability to filter, access, and troubleshoot Diameter transactions.

The primary change between the 2-tiered DSR topology and the 3-tiered DSR topology is the introduction of the DSR SOAM server. The role of the DSR NOAM server is changed to take on network scope instead of the Network Element scope it has with the 2-tiered DSR topology. The role of the DSR SOAM becomes similar to the role of the NOAM in the 2-tiered DSR topology in that it is managing a single DSR system (or DSR Signaling NE).

In 3-tiered DSR topology, there are NOAM servers, SOAM servers, and DA-MP servers.

In 3-tiered DSR topology, GUI screens can be used to configure and manage:

- Network topology data (such as user accounts, network elements, servers, and server groups) on a DSR NOAM
- Diameter signaling data (such as Local Nodes, Peer Nodes, Connections, Route Groups, and Route Lists) and DSR Application data (RBAR, FABR, and CPA) on a DSR SOAM

The DA-MP servers process the database updates from NOAM servers and SOAM servers and perform the real-time signaling. The DA-MP servers also supply the Platform MEAL data, Diameter signaling MEAL data, and DSR Application MEAL data to SOAM servers. The SOAM servers retain the Diameter signaling MEAL data and DSR Application MEAL data, and merge the Platform MEAL data to the NOAM servers.

Application Aware Answers

Application Awareness Answers provides to the following DSR Applications the capability to add additional AVPs to Answer messages in response to egress Diameter Requests, based on the Diameter Application ID and Command Code:

- Full Address Based Resolution (FABR)
- Range Based Address Resolution (RBAR)

Measurements Refactoring

Measurements Refactoring is a feature in DSR 4.0 that refactors DSR measurements to reduce the number of measurements that are collected in 5-minute intervals. This increases the interval for measurements that are not practical to collect every 5 minutes. This refactoring function uses these guidelines:

- Measurements deemed to add little or no value when collected on 5-minute intervals will have their collection interval increased.
- Measurements deemed to be redundant or of little value can be removed entirely or designated for Tekelec use only and/or on demand.

Note: The DSR OAM stores all the DSR NE measurement data for 7 days.

Scheduled Bulk Export

The DSR Bulk Export operation creates ASCII Comma-Separated Values (CSV) files (.csv) containing Diameter and DSR Application configuration data. Exported CSV files 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.

Selected configuration data can be exported once immediately, or can be periodically automatically exported on a defined schedule. The schedule can be changed if needed.

Maximum Message Size

The maximum Diameter message size has been increased to 16 K bytes. The feature includes:

- The default maximum message size is 8 K bytes.
- A Tekelec-supported procedure is available to change the default maximum message size. The default maximum message size can be set to a value between 8 - 16 K bytes (in increments of 1 K bytes). The current maximum message size is available via the DSR GUI.

Each individual DA-MP must be restarted for a new maximum message size value to take effect.

Increased DSR Local Nodes

The number of Local Nodes supported by a single DSR NE is 32, and each DA-MP in a DSR NE is capable of hosting all Local Nodes in the DSR NE.

A minimum of 8 local IP addresses for each DA-MP in the DSR NE is supported by a single DSR Local Node. The IP addresses can be any combination of IPv4 and IPv6 formats.

This feature also provides an optional TCP or SCTP Listening Port configuration parameter in a DSR Local Node:

• Initiator-only connections are supported for DSR Local Nodes that do not have a configured Listening Port.
• Initiator and Responder and Responder-only connections are not supported for DSR Local Nodes that do not have a configured Listening Port.

Alternate-routing across Route Groups in a Route List

Previously, DSR performed alternate-routing across peers/connections with the selected route group. After the peers/connections within the selected route groups were exhausted, no additional routing attempts were made, and the request was rejected. This occurred even if eligible peers existed in the remaining route groups.

The Alternate-routing across Route Groups in a Route List feature improves request delivery by using eligible peers/connections from the other priority route groups of the route list. This occurs after all of the peers/connections in the current route group have been exhausted. This ensures that priority 1 timed out requests will be attempted to peers in the priority 2 Route Group.

Note: Alternate-routing across route groups is attempted only if the maximum forwarding attempts (configured in system options) is not exceeded.

A prioritized list of Route Groups for each Route List is maintained and used for routing Request messages. The Route List defines the Route Groups order within the Route List. Priority is based upon the Operational Status and Priority of each Route Group and the user-defined Minimum Route Group Availability Weight value assigned to the Route.

Note: The highest priority Route Group within a Route List is referred to as the Active Route Group for that Route List.

Alternate-routing can be operator enabled or disabled on a Route List basis.

Routing Option Sets

This feature increases flexibility in managing certain peer behaviors related to Request discards in relation to Answer timeouts. By supporting Routing Option Sets, configuration requirements are reduced, but the flexibility of different behaviors for various peers is preserved.

Routing Option Sets provides a way to group some existing behaviors and introduces new behaviors that can be optionally associated with a peer or a Diameter Application-Id.

The Routing Options Sets feature allows an operator to create up to 20 Routing Option Sets (including a Default). These can then be associated with each peer or Diameter Application-Id.

The following associations are available:

• When associated with a peer, the ingress actions specified in an associated Routing Option Set are used to determine the actions performed by the DSR.

- When a Routing Option Set is associated with a Diameter Application-Id, the actions are applicable towards all peers for Requests that match the Application-Id, but this is only true if the peer has not been assigned a Routing Option Set.

A Default Routing Set is provided and is used if a Routing Option Set is not associated with the peer or with the Diameter Application-Id present in the request.

Note: The values of the Default Routing Option Set are user-configurable, and deletion of the Default Routing Option Set is not allowed.

The Routing Option Set specifies the actions for the following Routing attributes:

- Maximum Per Message Forwarding Allowed
- Resource Exhausted Action
- Transaction Lifetime
- No Peer Response Action
- Connection Failure Action
- Connection Congestion Action

Pending Answer Timer

The Pending Answer Timer feature allows operators to define the maximum amount of time that DSR waits for an Answer response to a pending Diameter transaction.

Previously, DSR allowed the operator to specify a single system-wide value for the Pending Answer Timer as part of system options. Now, the Pending Answer Timer enhancement allows an operator to create up to 8 Pending Answer Timer values (including the Default). This value will be used when a Pending Answer Timer is not associated with the Peer or with the Diameter Application-Id.

Note: The default value can be modified but not deleted by the operator.

A peer and/or a Diameter Application-Id can optionally be associated with one of the 8 Pending Answer Timer values. The Pending Answer Timer associated with a peer takes precedence over one associated with the Diameter Application-Id present in the Request.

A single Default Pending Answer Timer is used when the peer or the Diameter Application-Id is not assigned a Pending Answer Timer value.

PRT Partitioning

The PRT (Peer Route Table) Partitioning feature improves PRT administration and management, as well as helps hubbing providers manage routing rules.

This feature supports up to 100 user-configurable PRTs on the DSR. Then, any one of the PRTs can be optionally associated with either the (ingress) Peer or a Diameter Application-Id. A local application can also specify the PRT that needs to be used for routing a Request. Each of these PRTs can have no more than 1000 rules, and the maximum number of rules across all combined PRTs is 10000. By default, a system-wide PRT is also present and is used if a PRT has not been assigned to the ingress peer or the Diameter Application-Id present in the Request, or if one is not specified by the local application.

Note: Although it is possible to associate PRT instances with peers, Diameter Application-Ids, and so on, a single PRT is used for request routing.

In addition to the 100 PRT instances, DSR supports a configurable single system-wide PRT. This system-wide PRT supports the same attributes and operators that are supported in the PRT in previous releases of DSR.

Remote BUSY Congestion

The Remote BUSY Congestion function provides remedial measures if a DSR peer node is unable to process messages as fast as they are sent to it on a given DSR connection to the peer node. A connection is considered congested (BUSY) if an Answer message containing 'Diameter_TOO_BUSY' result code is received on the connection and was originated by the peer node.

Message traffic reduction is managed through the use of 4 Remote Busy Congestion Levels: CL0-CL3, where CL0 indicates no congestion" and CL3 is the highest level of congestion. The Remote Busy Congestion feature can be enabled and disabled per Diameter connection.

A Remote Busy Congestion Level for a connection is determined from the Priority of the egress transactions rejected by a "DIAMETER_TOO_BUSY" response.

Whenever the Remote Busy Congestion Level is increased, Remote Busy Congestion abatement is re-started, by starting a user-configurable Remote Busy Congestion Abatement Timer. When the Abatement Timer expires, the congestion level is decremented by one, thus allowing transactions with the next lower Priority to be forwarded on the connection; and the Abatement Timer is restarted. This process continues until the transactions of the connection drops back to CL0.

Per Connection Egress Message Control Features

The following Per Connection Egress Message Control features collectively provide a comprehensive solution for managing the egress message traffic loading per Diameter connection from a DSR to adjacent (Peer) Diameter Nodes:

- Remote Busy Congestion
- Egress Transport Congestion
- Per-Connection Egress Message Throttling

Each feature controls the flow of egress traffic by setting a feature-specific congestion level for a Diameter connection. The Connection Priority Level (CPL) is an overall congestion level for the connection that is based upon the highest congestion level of the various egress traffic control features. The CPL is used by the Diameter Routing Function when making egress message routing decisions based on the Message Priority feature. A message can only be forwarded to a connection if the message's priority is greater than or equal to the CPL for the connection.

DSR supports a maximum of 5 congestion levels (CL0 to CL4), with CL0 indicating no congestion and CL4 indicating that the connection is blocked. The intermediate congestion levels CL1, CL2, and CL3 indicate the increasing severity of congestion. Each Per Connection Egress Message Control feature has a congestion level range, as follows:

Remote Busy Congestion Levels	CL0-CL3
Egress Transport Congestion Levels	CL0-CL4
Per Connection Egress Message Throttling Congestion Levels	CL0-CL3

User-Configurable Message Priority

The User-Configurable Message Priority feature allows DSR administrators to assign message priorities to incoming Diameter requests.

Priorities can be based on a combination of Application-Id, command-code, and the connection upon which the request arrives. This combination is called a Message Priority Rule. This feature allows request messages arriving at the DSR to be marked with a message priority by use of a configuration set association with a:

- Connection
- Peer node
- Application Routing Rule
- Peer Routing Rule

Note: Message priority is determined partially on the connection where the request arrives and the first DSR to handle the request. A second DSR to handle the request is not able to establish the priority based on the original ingress connection.

DSR 4.0 implements the following functionality associated with Message Priority and connection congestion:

- DSR egress Request routing incorporates Request message priority and connection congestion level in its connection selection criteria
- The Routing Option Set associated with the ingress Request will specify what action is taken by the DSR when routing of a Request is abandoned and the last connection evaluated was congested
- The maintenance status for a congested connection shall indicate whether the congestion is due to Remote BUSY Congestion, Egress Transport Congestion, or Egress Message Throttling

Message Priority Configuration Sets (MPCS) have an ID that is used when associating the configuration set with a connection. The ID is a combination of Application-Id, command-code, and message priority rules.

Application-ID	The Diameter application-ID. The application-id can be a wildcard indicating that all application-ids match this message priority rule.
Command-code	The Diameter command-code. The command-code can be a wildcard indicating that all command-codes within the specified application match this message priority rule. If multiple command-codes with the same appl-id are to get the same message priority, then there will be a separate message priority rule for each command-code.
Priority	The priority applied to all request messages that match the Application-ID, Command-Code combination.

The DSR administrator can configure a connection or a peer with either an MPCS or to get message priority from the ingress request for:

- Peer connections
- Peer nodes
- Application routing rules
- Peer routing rules

Note: If configured to get message priority from the ingress request then it is not possible to configure a MPCS for the connection or peer.

Internet Protocol Front End (IPFE) release enhancements

The Internet Protocol Front End (IPFE) is a traffic distributor that:

- Presents a routable IP address representing a set of application servers to application clients.
- The use of IPFE results in the IP addresses of the application servers remaining hidden from the clients; the only IP addressed the clients are aware of are the routable IP addresses supported by the IPFE (for example, the Target Set Address).
- Routes packets that would establish new TCP connections to a selected application server.
- Routes packets in existing TCP connections to the correct server for the connection.

In this release, IPFE is integrated with the DSR to allow multiple Active DA-MP (application servers) in a DSR to be accessed by Diameter clients (application clients) using a reduced set of public signaling IP addresses. Additionally, using the services provided by the IPFE, additional DA-MP can be added to the DSR to increase its capacity, and the increased capacity can be accessed transparently by Diameter clients connecting to the DSR (for example, Diameter clients do not need to modify their DSR addressing).

The following are the IPFE DSR 4.0 release enhancements:

- Stream Control Transmission Protocol (SCTP) (Uni-homing)
- Support for Weighted Target Set Entries
- Bandwidth increase
- Multiple IPFE pairs support

SCTP (Uni-homing)

The IPFE is a traffic distributor that provides the following features:

- Provides a routable IP address representing a set of application servers to application clients
- Removes the need for application clients to be configured to know the IP addresses of every application server
- Routes packets that establish new TCP connections to a selected application server
- Routes packets in existing TCP connections to the correct server for the connection

The IPFE distributes traffic among a set of application servers. SCTP in the IPFE supports only one network path for a flow. The SCTP association is uni-homed because it has exactly one IP address for each endpoint.

Note: Prior to this feature, the IPFE only supported the distribution of Transmission Control Protocol (TCP) traffic.

SCTP is a transport layer protocol that acts in a similar role to TCP. Like TCP, SCTP is a connection-oriented reliable protocol with congestion-control features. Unlike TCP, SCTP is message-oriented and avoids head-of-line blocking of messages.

Weighted Target Set Entries

This enhancement to IPFE supports more than one pair of IPFEs and supports disparate weights between different application servers. Previously, support was limited to a single pair of IPFEs. Regarding load weighting, applications have handled traffic load evenly. This enhancement pertains to software only; in particular, the IPFE GUI and core software.

The replication between IPFE mates is bidirectional one-to-one replication. Traffic apportioning is on a best-effort basis. The IPFE can direct new connections to an application server in an attempt to distribute the load according to the configured weights. However, the IPFE cannot move existing connections to a different application server; therefore, a predictable traffic load is dependent on the connections having a degree of statistical smoothness.

In this release, a new attribute is associated with each IP in the list of TSA IPs. The attribute is called Weighting. Weighting is an integer value between 0 - 65535, and it indicates the proportion of connections that IP can receive. The default value of Weighting is 100.

Bandwidth increase

In this release, IPFE Bandwidth supports system configurations that allows client-to-server traffic of up to 3.2 Gbps.

Multiple IPFE pairs support

The deployment of additional mated IPFE pairs is provided; however, this requires additional TSAs.

Multiple pairs are beneficial when each pair supports a distinct service, or a distinct set of clients for a particular service, or in other cases where overlapping target sets do not introduce issues. In particular, if overlapping target sets are used by the same clients for the same purpose, it becomes possible for a client to have both a primary and a secondary connection that terminate on the same application server.

Scalability

The DSR product must scale beyond the capacity of a single DA-MP and provide support for hosting multiple DSR Local Applications simultaneously in order to meet market demands for functionality, message processing capacity, and Diameter connection capacity.

The DSR Scalability feature introduces the capability for a DSR to contain multiple Active Diameter Agent Message Processors (DA-MPs). This provides increased message processing and Diameter connection capacity. When additional message processing or Diameter connection capacity is required, additional Active DA-MPs can be added to the DSR. The scalability enhancements increase the capacity of a single DA-MP and provide support for hosting multiple DSR Local Applications simultaneously. This meets increased demands for functionality, message processing capacity, and Diameter connection capacity.

In a scaled DSR that contains multiple Active DA-MPs:

• All DA-MPs in the DSR are managed by a single OAM system

- All DA-MPs in the DSR share a common static configuration and pertinent dynamic routing status
- Diameter messages which ingress a DA-MP may egress any DA-MP in the DSR based on the user-configurable routing database and egress connection status
- The IP Front-End (IPFE) component can be used to simplify DSR addressing and capacity management for Diameter nodes initiating Diameter connections to the DSR

The DSR Multiple Application Support feature introduces the capability for a DSR to host multiple DSR Local Applications simultaneously. This feature allows all or a subset of the following DSR Local Applications to be enabled for traffic processing on each DA-MP in a DSR individually:

- Range Based Address Resolution (RBAR)
- Full Address Based Resolution (FABR)
- Charging Proxy Application (CPA)

The following major DSR scalability architecture areas are addressed in DSR Release 4.0:

- The distribution of the DSR Diameter functionality across multiple DA MPs within a DSR NE
- Logical clustering of DA MPs within a DSR NE by function
- Simplified addressing and load-balancing of DSR client connections across DA MPs within a DSR NE

Online Help

The DSR provides context-sensitive online help documentation that can be launched from the application GUI. There are two ways to access the online help from the GUI:

- Click the Help link located in the application's Main Menu.
- Click the Help icon located in the top right corner of any GUI page. When you click the Help icon the online help will open to the section of the documentation most relevant to the current page.

For more information about the usage and organization of the documentation, see the Getting Started section of the online help.

Chapter

4

Tekelec Resources and Services

Topics:

Tekelec provides a number of resources for EAGLE XG DSR. These include the availability of product documentation online, customer training, and access to the Customer Care Center.

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:

  USA access code +1-800-658-5454, then 1-888-FOR-TKLC or 1-888-367-8552 (toll-free)

  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:

    +91 124 436 8552 or +91 124 436 8553

    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.

Customer Training

Tekelec offers a variety of technical training courses designed to provide the knowledge and experience required to properly provision, administer, operate, and maintain Tekelec products. To enroll in any of the courses or for schedule information, contact the Tekelec Training Center at (919) 460-3064 or E-mail `training@tekelec.com`.

A complete list and schedule of open enrollment can be found at `www.tekelec.com`.

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.

Glossary

C

ComAgent

Communication Agent

A common infrastructure component delivered as part of a common plug-in, which provides services to enable communication of message between application processes on different servers.

Communication Agent

See ComAgent.

CPA

Charging Proxy Application

A local application running on the DSR.

D

DA

Destination Address

Digit Action

DA-MP

Diameter Agent MP

A DSR MP (Server Role = MP, Server Group Function = Diameter Signaling Router). A local application such as CPA can optionally be activated on the DA-MP.

Diameter

Protocol that provides an Authentication, Authorization, and Accounting (AAA) framework for applications such as network access or IP mobility. Diameter works in both local and roaming AAA situations.

Diameter can also be used as a signaling protocol for mobility management which is typically associated with an IMS or wireless

D

type of environment. Diameter is the successor to the RADIUS protocol. The MPE device supports a range of Diameter interfaces, including Rx, Gx, Gy, and Ty.

DIH   Diameter Intelligence Hub

A troubleshooting solution for LTE, IMS, and 3G Diameter traffic processed by the DSR. DIH does not require separate probes or taps.

DR   Disaster Recovery

DSR   Diameter Signaling Router

A set of co-located Message Processors which share common Diameter routing tables and are supported by a pair of OAM servers. A DSR Network Element may consist of one or more Diameter nodes.

F

FABR   Full Address Based Resolution

Provides an enhanced DSR routing capability to enable network operators to resolve the designated Diameter server addresses based on individual user identity addresses in the incoming Diameter request messages.

H

HA   High Availability

High Availability refers to a system or component that operates on a continuous basis by utilizing redundant connectivity, thereby circumventing unplanned outages.

I

I

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

M

MEAL	Measurements, Events, Alarms, and Logs
Message Processor	See MP
MP	Message Processor
	The role of the Message Processor is to provide the application messaging protocol interfaces and processing. However, these servers also have OAM&P components. All Message Processors replicate from their Signaling OAM's database and generate faults to a Fault Management System.

N

NE	Network Element

N

An independent and identifiable
piece of equipment closely
associated with at least one
processor, and within a single
location.

Network Entity

NOAM

Network Operations,
Administration, and Maintenance

O

OAM

Operations, Administration, and
Maintenance

The application that operates the
Maintenance and Administration
Subsystem which controls the
operation of many Tekelec products.

Q

QS

Query Server

Query Service

R

RBAR

Range Based Address Resolution

A DSR enhanced routing application
which allows the user to route
Diameter end-to-end transactions
based on Application ID, Command
Code, "Routing Entity" Type, and
Routing Entity address ranges.

RMS

RAM Management Services

S

SBR

Session Binding Repository

A highly available, distributed
database for storing Diameter
session binding data.

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.

SDS	Subscriber Database Server

Subscriber Database Server (SDS) provides the central provisioning of the Full-Address Based Resolution (FABR) data. The SDS, which is deployed geo-redundantly at a Primary and Disaster recovery site, connects with the Query Server and the Data Processor System Operations, Administration, and Maintenance (DP SOAM) servers at each Diameter Signaling Router (DSR) site or a standalone DP site to replicate and recover provisioned data to the associated components.

SOAM	System Operations, Administration, and Maintenance

T

TCP	Transfer Control Protocol

TSA	Target Set Address

An externally routable IP address that the IPFE presents to application

T

clients. The IPFE distributes traffic
sent to a target set address across a
set of application servers.