

Juniper Networks Diameter Base Platform

Custom Diameter Applications Development Solution

Key Benefits

- Lower barrier of entry into Diameter based solutions markets
- Create IMS-compliant network elements
- Reduce development costs and time to market
- Gain performance advantage by licensing proven implementation
- Allow application developers to focus on application logic instead of network protocols and traffic management

Mobile service providers must offer innovative multimedia services that operate across various access methods and device types in order to retain their existing customers and attract new ones. To address this need, the leading providers are building converged services delivery architectures in which voice, data and video are delivered across an IP-based network. The 3GPP IP Multimedia Subsystem (IMS) provides a complete architecture for a suite of converged services in an all IP-based network. IMS standards provide open interfaces for access control and session management.

IMS transforms the network from a connection-based architecture to subscriber-based in which applications and services are readily requested and delivered to a range of devices and on multiple networks. Diameter is the next generation protocol for Authentication, Authorization, and Accounting in the IMS architecture.

The Diameter Base Protocol (RFC 3588) is an IETF Proposed Standard, covering the network behavior of all Diameter applications designed on top of it. It differs from RADIUS in that it allows the implementer to define their own applications and request/response pairs. As such, it is completely open and extensible. However, regardless of the specific Diameter application, all Diameter nodes must conform to the base protocol specification.

The Diameter Base Platform is an IMS-compliant development kit that allows application developers to implement arbitrary Diameter applications. It provides a framework for implementation of a carrier-grade Diameter node to run on standard computer hardware. The platform implements the base protocol in full conformance with the relevant specifications. By choosing the Diameter Base Platform, you can quickly create fully standards-compliant Diameter solutions.

However, the development kit is much more than just an implementation of the base protocol. It is a platform that maintains connections to Diameter peers, manages traffic flow, detects anomalous conditions, and allows your application code to direct its operation when your application developers require it. All the networking functionality required to correctly service Diameter requests and responses is included. The time and effort necessary to build in-house networking expertise can be extensive and add unforeseen costs to any development project. Instead, you can let the Diameter Base Platform take care of all the networking details and allow your team to concentrate on designing your application. Whether you are building session and policy control elements such as Call Session Controller (CSCF, BGCF), Management and Service Fulfillment elements (CCF) or a Centralized Subscriber Database (HSS), the end result of leveraging this proven solution is reduced time to market for your own products.

The Diameter Protocol

Diameter is the next-generation protocol for Authentication, Authorization, and Accounting. Originally an IETF draft in March 2001, Diameter has since become a proposed standard RFC, namely RFC 3588. Some of the first Diameter applications to be defined were those that expand on existing RADIUS solutions, such as EAP authentication, accounting, and Mobile IP.

Diameter in IMS

However, the importance of Diameter increased dramatically with the selection of Diameter as the signaling protocol to be used between many components of the 3GPP IP Multimedia Subsystem (IMS). Several Diameter applications are defined for use within this architecture, and all of them must be implemented on conformant implementations of the Diameter base protocol.

These Diameter applications within IMS carry signaling information that affects every phase of the delivery of multimedia services to subscribers. Therefore, the load on these applications increases with the size of the subscriber base. As a result, the Diameter implementation becomes a critical component of any scalable IMS solution.

Diameter Base Platform

The Diameter Base Platform is a high performance software implementation of a Diameter node. As shipped, the platform is capable of managing transports, connections to other peers, protocol sequences required by the Diameter RFCs, and manages an appropriate thread model for a high performance server.

Applications, even those written by the customer, can operate on top of this platform. All applications benefit from one shared framework and one implementation of the base protocol. By programming to a C API, custom applications can be defined by the customer, which can then be called from other Diameter nodes. The API used is designed along object-oriented principles and presented as standard C entry points for maximum binary compatibility. Juniper Network's engineers also provide global support services to complement our products and can consult on IMS development and custom software solutions.

Designed for Performance

A Diameter-based network of servers is very different from appropriate architectures in pre-3G networks. Because most network elements are software running over an IP network, the performance of these IP-based signaling systems is critical. Furthermore, Diameter is a peer-to-peer protocol. Nodes are neither purely servers nor clients. Both sides of a Diameter link must have similar performance characteristics in order to be able to scale the entire solution while being assured of interoperability when it comes time for integration testing.

Standards-Based

Because the Diameter Base Platform's external Diameter interface is entirely based on standards-track RFCs, it will also interoperate with other vendors' implementation of the protocol. This characteristic allows vendors to create only some of the components of a larger solution while being assured of interoperability when it comes time for integration testing.

Complete and Flexible Networking Solution

The platform does not require the customer to implement every detail involved in managing the network connections and request / response processing. Hence, it allows the application developers to create a complete application without requiring experience in building high-performance server applications. If the customer chooses to let the application handle all networking situations autonomously, the platform will react appropriately to network events:

The platform will defend against rogue nodes (unauthorized network elements) that are not part of the trusted solution, ensuring that the application code will not need to handle attacks from hostile network participants. Even the simplest application built on the platform enjoys the benefits of this functionality.

Furthermore, congestion or disconnect conditions in the network are detected and handled. For example, when a network connection is found to be backing up with traffic, the platform will redirect appropriate requests to another available connection, if possible. The application code is informed of these events, and it may choose to intercede.

However, it is not strictly required that the application code take any action in these scenarios. As a result, a typical first version of an application will have appropriate behavior even during anomalous networking conditions, even if the application does not include explicit handling of any such situations.

If, on the other hand, the application programmer decides to handle such situations explicitly, they can use the platform's rich API for handling events and directing recovery behaviors. This API allows the application to selectively direct or override any part of the platform's default behaviors, so that advanced scenarios can be tailored to the specific application's needs.

Another way the application programmer may choose to direct the platform's recovery operation is by deep queue inspection. This functional area of the platform allows the developer to make application-level decisions regarding the correct way to handle requests that are currently in the platform's queues. Some developers may feel that the application code, with its superior understanding of the semantics of each message, can best determine which messages should be rerouted or failed or retried. At the developer's discretion, the platform can allow this level of intervention by the application, without adversely affecting performance.

Even the most advanced application developer's requirements can be addressed, while making a fully operational but minimal application extremely easy to create.

Specifications

Supported Standards: RFC 3588 Diameter Base Protocol, RFC 3539 AAA Transport Profile

Supported Hardware: Sun SPARC Server running Solaris, Intel x86-based Server running Linux

Supported Transport Protocols: TCP and SCTP, IPv4 and IPv6

Interfaces: Diameter (acting as both "server" and "client," as appropriate)

C API used to control the operation of the platform, send requests/responses, react to events, and gather status information

Compatibility: Any Diameter RFC 3588 compliant peer



CORPORATE HEADQUARTERS AND SALES HEADQUARTERS FOR NORTH AND SOUTH AMERICA
 Juniper Networks, Inc.
 1194 North Mathilda Avenue
 Sunnyvale, CA 94089 USA
 Phone: 888-JUNIPER (888-586-4737)
 or 408-745-2000
 Fax: 408-745-2100
 www.juniper.net

EAST COAST OFFICE
 Juniper Networks, Inc.
 10 Technology Park Drive
 Westford, MA 01886-3146 USA
 Phone: 978-589-5800
 Fax: 978-589-0800

ASIA PACIFIC REGIONAL SALES HEADQUARTERS
 Juniper Networks (Hong Kong) Ltd.
 Suite 2507-11, Asia Pacific Finance Tower
 Citibank Plaza, 3 Garden Road
 Central, Hong Kong
 Phone: 852-2332-3636
 Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA REGIONAL SALES HEADQUARTERS
 Juniper Networks (UK) Limited
 Juniper House
 Guildford Road
 Leatherhead
 Surrey, KT22 9JH, U. K.
 Phone: 44(0)1372-385500
 Fax: 44(0)1372-385501

Copyright 2006, Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.