

# Introduction to the Diameter Protocol in 3GPP context

Whitepaper by Traffix Systems

## Table of Contents

<b>1</b>	<b>INTRODUCTION TO THE DIAMETER PROTOCOL .....</b>	<b>2</b>
<b>2</b>	<b>DIAMETER STRUCTURE .....</b>	<b>3</b>
<b>3</b>	<b>DIAMETER – HISTORY AND BENEFITS.....</b>	<b>5</b>
<b>4</b>	<b>TYPES OF DIAMETER NODES .....</b>	<b>9</b>
<b>5</b>	<b>DIAMETER UNDER 3GPP UMBRELLA.....</b>	<b>10</b>
<b>6</b>	<b>DIAMETER INTERFACES IN 3GPP/2 RELEASE 7 .....</b>	<b>11</b>
<b>7</b>	<b>SUMMARY .....</b>	<b>13</b>
<b>8</b>	<b>ACRONYMS AND MAIN CONCEPTS.....</b>	<b>14</b>

2010 Traffix Systems Ltd, All Rights Reserved.

This document is copyrighted of Traffix Systems Ltd. The information contained within this document is subject to change without notice.

## 1 Introduction to the Diameter Protocol

Diameter is an AAA (Authentication, Authorization and Accounting) protocol for applications such as network access or IP mobility. The basic concept is to provide a base protocol that can be extended in order to provide AAA services to new access technologies. Diameter is intended to work in both local and roaming AAA situations.

The Diameter protocol was initially developed by the IETF to provide an Authentication, Authorization, and Accounting (AAA). The Diameter protocol has several advantages over previous AAA protocols like RADIUS in that it offers improvements in the areas of reliability, security, scalability, and flexibility. Diameter operates on top of reliable transport protocols like TCP and SCTP

The Diameter base protocol provides the following facilities:

- Connection and session management
- User authentication and capabilities negotiation
- Reliable delivery of attribute value pairs (AVPs)
- Agent support for proxy, redirect, and relay servers
- Extensibility, through addition of new commands and AVPs
- Basic accounting services

Diameter sessions consist of exchange of commands and AVPs between authorized Diameter Clients and Servers. Some of the command values are used by the Diameter protocol itself, while others deliver data associated with particular applications that employ Diameter. The Diameter base protocol provides the minimum requirements needed for AAA protocol, Mobile IPv4, or remote network access applications. In addition to the base

Diameter specification (RFC 3588), the IETF defines several Diameter applications that use the underlying services.

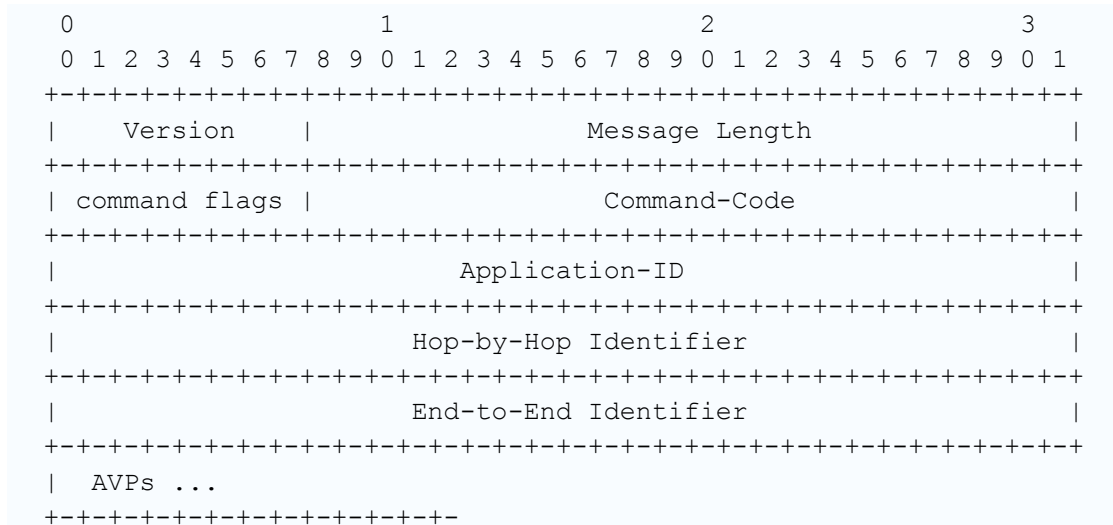
## 2 Diameter Structure

Diameter messages consist of a Diameter header, followed by a certain number of Diameter attribute value pairs (AVPs). The Diameter header comprises binary data and as such is similar to an IP header [RFC0791] or a TCP header [RFC0793]. The format of the Diameter header is shown in Figure 15.1.

The command flags specify the type of Diameter message. A request message has the "R" bit (or the request bit) set; while an answer message has it cleared. The "P" bit (or the proxiable bit) indicates whether the message can be proxied or must instead be processed locally. The "E" bit (or the error bit) indicates that the answer message is an error message. The "T" bit indicates that the message is possibly a retransmission and is set by Diameter agents in fail-over situations to aid detection of duplicate messages. The "r" bits are unused flags that are reserved for future use. Together with the Command-Code, the command flags specify the semantics associated with the particular Diameter message.

The Command-Code field indicates the command associated with the Diameter message. The Command-Code field is 24 bits long and includes values from 0 to 255 that are reserved for RADIUS backward compatibility, as well as values 16777214 and 16777215 that are reserved for experimental use. The Command-Code namespace is maintained by the Internet Assigned Numbers Authority (IANA) and includes either codes that are used by the Diameter Base Protocol or specific codes used by the Diameter applications.

***The Diameter packet format:***



AVPs contain authentication, authorization and accounting information elements, as well as routing, security and configuration information elements that are relevant to the particular Diameter request or answer message. Each AVP contains an AVP header and some AVP-specific data. The AVP-Code field uniquely identifies the attribute together with the Vendor-ID field. The first 256 AVP numbers, or codes, are reserved for backward compatibility with RADIUS, whereas numbers above 256 belong to Diameter attributes.

AVP-Code field values are maintained by the IANA.

AVP flags carry information on how the attribute should be handled by the receiving end. The "V" bit (or the vendor-specific bit) indicates that the AVP-Code belongs to a vendor-specific address space, denoted by the otherwise optional Vendor-ID field. The "M" bit (or mandatory bit) mandates the support for a particular AVP. Any message with an unrecognized AVP carrying the "M" bit is always rejected by the receiver. AVPs that do not have the M bit set are information-only (i.e., they can be ignored by the receiver if

they are not understood). When the "P" bit (or the protected bit) is set it indicates the need for encryption for end-to-end security. The "r" bits are unused flags reserved for future use.

**The AVP format:**

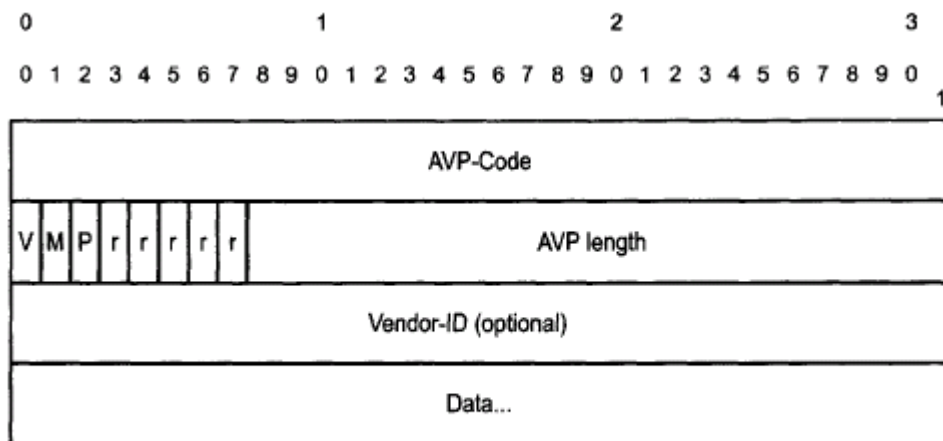


Figure 15.2 Diameter AVP header.

### 3 Diameter – History and Benefits

The name Diameter is a pun on the RADIUS protocol, which is the predecessor (a diameter is twice the radius). Diameter is not directly backwards compatible, but provides an upgrade path for RADIUS.

There are several general shortcomings of the RADIUS protocol that were addressed in the design of the Diameter base protocol. In addition to the protocol shortcomings, there are further application-specific RADIUS deficiencies that limit its capability to support AAA services in specific areas.

**Diameter benefits are:*****Better Transport***

Diameter runs over a reliable transport, TCP or SCTP.

Lost packets are retransmitted at each hop.

A persistent connection with an application-level heartbeat message (Watchdog message) supports timely failover.

TCP and SCTP adapt to network congestion.

***Better Proxying***

Hop-by-hop transport failure detection allows failover to occur at the appropriate place — proxies can locally failover to an alternate next-hop peer.

The proxy automatically does retransmission of pending request messages following a failover.

An AVP that identifies the ultimate destination allows multiple transactions for a given session to be routed to the same home server.

***Better Session Control***

Session management is independent of accounting. Accounting information can be routed to a different server than authentication/authorization messages. Session termination is conveyed by a specific Session-Termination message rather than an Accounting Stop message.

The server may initiate a message to request session termination.

The server may initiate a message to request re-authentication and/or reauthorization of a user.

***Better Security***

Hop-by-hop security is provided using IPsec or TLS.

End-to-end security protects the integrity and/or confidentiality of sensitive AVPs through intermediate proxies.

***Interoperability***

The RADIUS protocol supports vendor-specific attributes but not vendor-specific commands. This has enticed vendors to create private command codes with resulting interoperability problems.

The Diameter protocol supports both vendor-specific attributes and vendor-specific commands.

**A brief overview of SCTP**

Diameter, unlike RADIUS, operates over a reliable transport layer (either TCP or SCTP) that provides flow control, transport-level acknowledgements, and retransmissions. While TCP is well known, Stream Control Transmission Protocol (SCTP) is a fairly new IP transport protocol, existing at the level of UDP and TCP. In 2000, SCTP became a Proposed Standard and is specified in RFC 2960.

***SCTP is similar to TCP in that:***

- SCTP provides a connection-oriented transport service between two endpoints.
- SCTP provides reliable transmission, ensuring that data is delivered in order, without loss or duplication.
- SCTP is full duplex.
- SCTP employs a windowing mechanism to provide flow control.

***SCTP capabilities not provided by TCP:***

- SCTP provides multiple data streams between the two endpoints. Within each data stream, messages are delivered in order without loss or duplication. Independent data exchanges may be delivered over different streams; message loss in any one stream does not affect data delivery within other streams (TCP provides a single stream of data, where a message loss delays delivery of all subsequent messages. This is sometimes referred to as the head-of-line blocking problem)
- SCTP is message oriented; that is, SCTP maintains message boundaries and delivers complete messages (chunks), between the upper layer protocols employing SCTP (TCP is byte oriented; that is, TCP does not preserve data units within a transmitted byte stream, requiring the upper layer protocol to count and accumulate the bytes of each message)
- SCTP understands, and makes use of, the notion of multi-homed hosts. A multi-homed host is one with more than one IP interface. At initialization time, SCTP peers exchange lists of their IP interface addresses. An SCTP message requiring retransmission can be sent to an alternate IP address, which increases the survivability of an SCTP session in the event of network failures. SCTP uses multi-homing for redundancy, not for load-sharing (TCP session involves a single IP address at each endpoint; resulting in session failure should that single IP interface become unreachable).

Note: Some of Diameter functionalities defined by IEEE (like NASreq, EAP and other IP applications) are not discussed in the scope of this document since they are not relevant and used by the 3GPP Diameter variants.

## 4 Types of Diameter Nodes

In addition to clients and servers, the Diameter protocol defines relay, proxy, redirect, and translation agents.

**Client** - A Diameter Client is a device at the edge of the network that performs access control.

*Example:* Network Access Servers (NAS) and mobility agents (Foreign Agent).

**Server** - A Diameter Server is one that handles authentication, authorization, and accounting requests for a particular realm.

**Relay Agent** - A Relay Agent routes Diameter messages based on information found in the messages. This routing decision is performed using a list of supported realms and known peers.

Relay agents are largely transparent. A Relay Agent may modify Diameter messages only by inserting and/or removing routing information but may not modify any other portion of a message

**Proxy Agent** - A Proxy agent also routes Diameter messages. However, a proxy agent may modify messages to implement policy decisions, such as controlling resource usage, providing admission control, and provisioning.

**Redirect Agent** - A redirect agent also provides a routing function, generally acting as a centralized source of Realm to Server address mappings for members of a roaming consortium.

Unlike the other agents that relay requests, a redirect agent returns a special type of answer message to the peer that sent the request.

This answer message contains routing information that allows the peer to resend the request directly to the correct destination server.

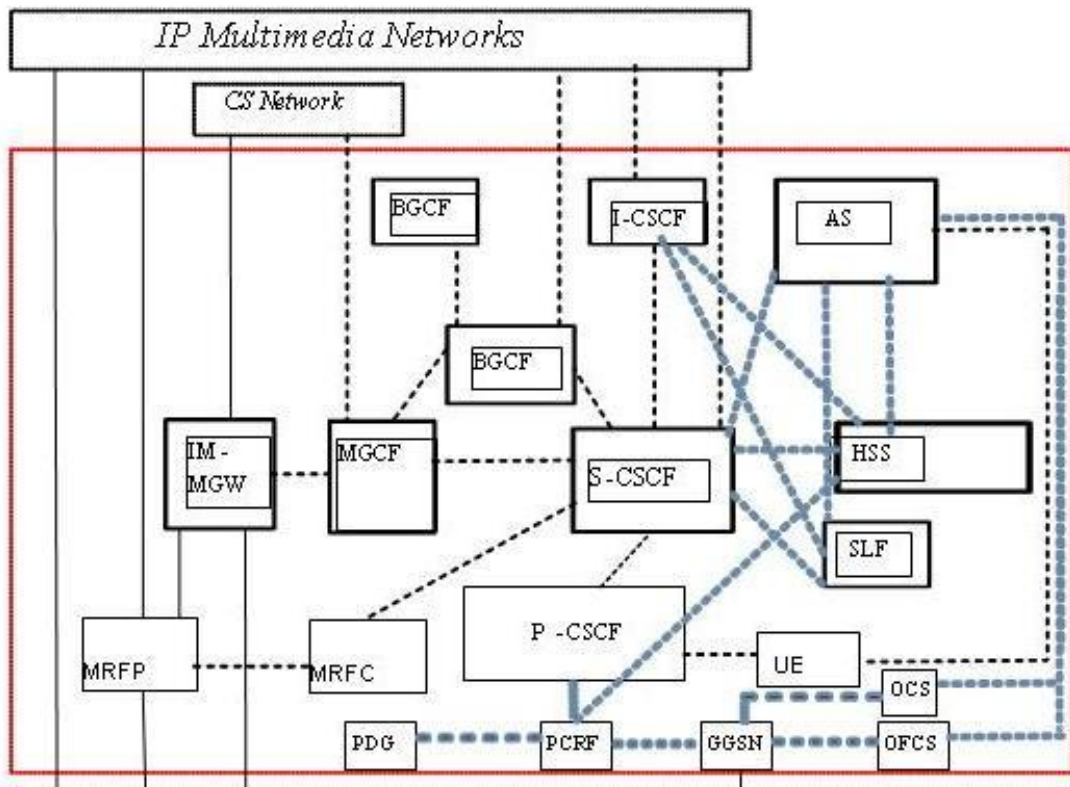
Note: A redirect agent does not relay requests.

**Translation Agent** - A Translation Agent translates between two protocols, such as RADIUS and Diameter. In this case, the translation agent supports a RADIUS to Diameter migration, allowing server conversions to Diameter.

## 5 Diameter under 3GPP umbrella

The 3<sup>rd</sup> Generation Partnership Project (3GPP) standardization organization has adopted Diameter as the primary signaling protocol for AAA and mobility management. Diameter was first introduced by 3GPP in Release 5 for the IP Multimedia Subsystem (IMS). In the beginning Diameter was used alongside other control protocols such as COPS and SOAP, but in 3GPP Releases 6 and 7 Diameter received sole responsibility for control plane signaling and in the LTE related 3GPP Release 8 and 9 it continued widespread as continued to more interfaces and network functionalities.

The following diagram is an example of how Diameter is used in the IMS network (relates to 3GPP Release 7) and highlights some of the Diameter defined interfaces.



## 6 Diameter interfaces in 3GPP/2 Release 7

- Diameter base Protocol (*RFC 3588*)
- Diameter Command for 3GPP (*RFC 3589*)
- AAA Transport Profile (*RFC 3539*)
- Sh interface (*3GPP TS 29.328 & TS 29.329, 3GPP2 TSG-X X.S0013-0011*)
- Dh interface (*3GPP TS 29.328 & TS 29.329, 3GPP2 TSG-X X.S0013-0011*)
- Rf interface (*RFC 4006, 3GPP TS 32.225 & TS 32.299, 3GPP2 X.S0013-007 & X.S0013-008*)
- Ro interface (*RFC 4006, 3GPP TS 32.225 & TS 32.299, 3GPP2 X.S0013-007 & X.S0013-008*)
- Re interface (*3GPP TS 32.296*)
- Cx interface (*3GPP TS 29.228 & TS29.229, 3GPP2 TSG-X X.S0013-006*)

- Dx interface (3GPP TS 29.228 & TS29.229, 3GPP2 TSG-X X.S0013-006)
- Sp interface (3GPP TS 23.203, TS 29.328 & TS 29.329) *(1)*
- Rx interface (3GPP TS 23.203 & TS 29.214)
- Gx interface (3GPP TS 29.212 & TS 23.203)
- Gy interface (3GPP TS 32.299)
- Gz interface (3GPP TS 32.240)
- Gq interface (3GPP TS 29.209)
- Zh/Dz/Zn interfaces (3GPP TS 29.109 & 3GPP TS 33.220)
- Dw/Wa/Wd/Wx/Wg/Pr/Wo/Wf/Wm interfaces (3GPP TS 29.234)
- Ty interface (3GPP2 TSG-X X.S0013-014)
- Tx interface (3GPP2 TSG-X X.S0013-013)
- Rx interface: 3GPP TS 23.203 and 3GPP TS 29.214
- Gx interface: 3GPP TS 29.212 and 3GPP TS 23.203
- Gy interface: 3GPP TS 32.299
- Gq interface: 3GPP TS 29.207
- Zh/Dz/Zn Interfaces: 3GPP TS 29.109 and 3GPP TS 33.220

*(1)* Sp interface specifications are still work in progress at the time of writing

*Note:* The Gq interface (TS 209.27) defined in 3GPP Release 6 (between P-CSCF to PDF) was replaced by the updated Rx interface in 3GPP Release 7 with the introduction of the PCRF and the encapsulation of the PDF function within.

## 7 Summary

The Diameter protocol is used to provide AAA services for a range of access technologies. Diameter is loosely based on an existing AAA protocol called RADIUS, which has been used widely for dial-up and terminal server access. The Diameter protocol uses a binary header format and is capable of transporting a range of data units called AVPs. The Diameter base protocol specifies the delivery mechanisms, capability negotiation, error handling and extensibility of the protocol, whereas individual Diameter applications specify service-specific functions and AVPs. In addition to the base protocol which includes accounting, the 3GPP's in it's mobile architecture from Releases 5,6 and 7 (IMS) to Releases 8 and 9 (LTE) make wide use of Diameter in over 90% of core network functionalities for the purpose of Authentication and Authorization, Accounting, Credit control and Policy and charging negotiation.

## 8 Acronyms and main concepts

**3GPP** - Acronym for the 3rd Generation Partnership Project. 3GPP is a user and definer of Diameter protocols as applied to 3rd Generation Wireless Networks and the IMS.

**3GPP2** - Acronym for the 3rd Generation Partnership Project 2. 3GPP2 is a user and definer of Diameter protocols as applied to 3rd Generation Wireless Networks and the IMS.

**AAA** - Acronym for Authentication, Authorization, and Accounting. Among other capabilities, Diameter is a type of AAA protocol.

**Accounting** - The act of collecting information on resource usage for the purpose of capacity planning, auditing, billing, or cost allocation. Diameter provides an accounting capability.

**Application-ID** - A field defined in a Diameter Header for standard and vendor-specific Diameter applications and maintained by the IANA.

**Authentication** - The act of verifying the identity of an entity. Diameter provides an authentication capability.

**Authorization** - The act of determining whether a requesting entity will be allowed access to a resource. Diameter provides an authorization capability.

**AVP** - Acronym for Attribute Value Pair. The Diameter protocol consists of a header followed by one or more Attribute Value Pairs (AVPs). An AVP includes a header and is used to encapsulate protocol-specific data (as well as AAA information).

**AVP-Code** - A field in the header of a Diameter AVP that uniquely identifies the object attribute. Standardized AVP-Codes are maintained by the IANA.

**Bearer Charging Function (BCF)** - performs bearer charging using the Ro reference point towards other network entities in the access domain.

**Billing** - The act of charging for usage or events normally derived from accounting information. Diameter provides accounting information.

**Broker** - A broker is a business term commonly used in AAA infrastructures. A broker is either a relay, proxy, or redirect agent,

and may be operated by roaming consortiums. Depending on the business model, a broker may either choose to deploy either relay agents or proxy agents.

**Diameter Base Protocol** - A base foundation protocol that provides transfer of Diameter messages, negotiation capabilities, routing capabilities, error handling, and Diameter extensibility.

**Event Charging Function (ECF)** - performs event-based charging using the Ro reference point or variants thereof.

**IANA** - Acronym for the Internet Assigned Number Authority.

**IETF** - Acronym for the Internet Engineering Task Force. The IETF is the first user and definer of the Diameter Base protocol as well as the first application-level protocols that use Diameter.

**IMS** - Acronym for the Internet Protocol Multimedia Subsystem. Through the efforts of the 3GPP, it is one of the first functional subsystems that is a user and definer of the Diameter protocol and extensions.

**IPsec** - Acronym for Internet Protocol Security. A network layer security protocol defined in the IETF.

**Offline Billing** - The act of charging after a usage or event that is normally based on non-real-time accounting information.

**Postpaid Billing** - A type of offline billing system.

**RADIUS** - Acronym for Remote Authentication Dial In User Service. RADIUS is a type of AAA protocol.

**Rating** - The act of applying charging based on specific usage or event content and rules.

**Session Charging Function (SCF)** performs IMS session charging using the Ro reference point towards the CSCF.

**SCTP** - Acronym for Stream Control Transmission Protocol. A reliable transport protocol used for the exchange of Diameter protocols.

**TCP** - Acronym for Transmission Control Protocol. A reliable transport layer protocol used for the exchange of Diameter protocols.

**TLS** - Acronym for Transport Layer Security. A transport layer security protocol that encapsulates and secures application layer protocols.

**User** - The entity requesting or using some resource, in support of which a Diameter client has generated a request.

### **About Traffix Systems**

Traffix Systems is the Diameter control plane expert. Traffix supports telecom operators on their way to Next Generation Network (NGN, IMS or LTE) technology by providing cost saving Diameter solutions such as Diameter gateways and load-balancing solutions for the Diameter control plane achieving network connectivity and scalability and thus enabling the opportunities to generate new service revenues based on the Diameter control plane innovation.

*For info please contact us at:*  
*Mail: [info@traffixsystems.com](mailto:info@traffixsystems.com)*  
*Web: [www.traffixsystems.com](http://www.traffixsystems.com)*