HANNES TSCHOFENIG • SÉBASTIEN DECUGIS
JEAN MAHONEY • JOUNI KORHONEN

DIAMETER

NEW GENERATION AAA PROTOCOL

DESIGN, PRACTICE, AND APPLICATIONS

WILEY

Diameter

Diameter

New Generation AAA Protocol – Design, Practice, and Applications

Hannes Tschofenig

Sébastien Decugis

Jean Mahoney

Jouni Korhonen

WILEY

This edition first published 2019

Registered Offices
John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, UK

Editorial Office
The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, UK

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Wiley also publishes its books in a variety of electronic formats and by print-on-demand. Some content that appears in standard print versions of this book may not be available in other formats.

Library of Congress Cataloging-in-Publication Data

Names: Tschofenig, Hannes, author.
Title: Diameter : new generation AAA protocol – design, practice, and applications / Hannes Tschofenig, Sébastien Decugis, Jean Mahoney, Jouni Korhonen.
Description: Hoboken, NJ, USA : John Wiley & Sons, Ltd, [2019] | Includes bibliographical references and index. |
Identifiers: LCCN 2019003182 (print) | LCCN 2019009248 (ebook) | ISBN 9781118875858 (Adobe PDF) | ISBN 9781118875834 (ePub) | ISBN 9781118875902 (hardcover)
Subjects: LCSH: Diameter (Computer network protocol)
Classification: LCC TK5105.5663 (ebook) | LCC TK5105.5663 .T75 2019 (print) | DDC 004.6/2–dc23
LC record available at https://lccn.loc.gov/2019003182

Cover Design: Wiley
Cover Image : © catalby/Getty images

Set in 10/12pt WarnockPro by SPi Global, Chennai, India

Printed in Great Britain by TJ International Ltd, Padstow, Cornwall

10 9 8 7 6 5 4 3 2 1

This book is dedicated to the next AAA.
Hannes, Sébastien, Jean, Jouni

Contents

Disclaimer *xiii*
About the Authors *xv*
Foreword *xvii*
Preface *xix*
Acknowledgements *xxiii*
List of Abbreviations *xxv*

1 Introduction *1*
1.1 What is AAA? *1*
1.2 Open Standards and the IETF *2*
1.3 What is Diameter? *3*
1.3.1 Diameter versus RADIUS *4*
1.3.2 Diameter Improvements *5*
1.4 What is `freeDiameter`? *6*
References *6*

2 Fundamental Diameter Concepts and Building Blocks *9*
2.1 Introduction *9*
2.2 Diameter Nodes *9*
2.3 Diameter Protocol Structure *10*
2.4 Diameter Applications *10*
2.5 Connections *11*
2.5.1 Transport Layer *11*
2.5.2 Peer-to-Peer Messaging Layer *12*
2.5.3 Setting up a Connection between `freeDiameter` Peers *12*
2.6 Diameter Message Overview *12*
2.6.1 The Command Code Format *13*
2.6.2 Message Structure *15*
2.6.3 Attribute–Value Pairs *16*
2.6.3.1 Format *16*
2.6.4 Derived AVP Data Formats *20*
2.7 Diameter Sessions *20*
2.8 Transaction Results *21*

2.8.1 Successful Transactions *21*
2.8.2 Protocol Errors *21*
2.8.3 Transient Failures *22*
2.8.4 Permanent Failures *23*
2.9 Diameter Agents *25*
2.9.1 Saving State *25*
2.9.2 Redirect Agents *25*
2.9.3 Relay Agents *25*
2.9.4 Proxy Agents *27*
2.9.5 Translation Agents *27*
References *27*

3 Communication between Neighboring Peers *29*
3.1 Introduction *29*
3.2 Peer Connections and Diameter Sessions *29*
3.3 The DiameterIdentity *29*
3.4 Peer Discovery *31*
3.4.1 Static Discovery *31*
3.4.1.1 Static Discovery in `freeDiameter` *31*
3.4.2 Dynamic Discovery *32*
3.4.2.1 Dynamic Discovery and DiameterURI *35*
3.4.2.2 DNS Further Reading *36*
3.5 Connection Establishment *36*
3.5.1 The Election Process: Handling Simultaneous Connection Attempts *37*
3.6 Capabilities Exchange *37*
3.6.1 `freeDiameter` example *38*
3.6.2 The Capabilities Exchange Request *39*
3.6.3 Capabilities Exchange Answer *40*
3.6.4 Hop-by-Hop Identifiers *41*
3.7 The Peer Table *42*
3.8 Peer Connection Maintenance *43*
3.8.1 Transport Failure, Failover, and Failback Procedures *45*
3.8.2 Peer State Machine *49*
3.9 Advanced Transport and Peer Topics *49*
3.9.1 TCP Multi-homing *50*
3.9.2 SCTP Multi-homing *51*
3.9.2.1 Multi-homing in `freeDiameter` *53*
3.9.3 Avoiding Head-of-Line Blocking *56*
3.9.4 Multiple Connection Instances *56*
References *59*

4 Diameter End-to-End Communication *61*
4.1 Introduction *61*
4.2 The Routing Table *61*
4.3 Diameter Request Routing *63*
4.3.1 AVPs to Route Request Messages *64*
4.3.1.1 `Destination-Realm` AVP *64*

4.3.1.2 `Destination-Host` AVP *64*
4.3.1.3 `Auth-Application-Id` and `Acct-Application-Id` AVPs *64*
4.3.1.4 `User-Name` AVP *65*
4.3.2 Routing AVPs *66*
4.3.2.1 `Route-Record` AVP *66*
4.3.2.2 `Proxy-Info` AVP *66*
4.4 Request Routing Error Handling *67*
4.4.1 Detecting Duplicated Messages *67*
4.4.2 Error Codes *67*
4.5 Answer Message Routing *68*
4.5.1 Relaying and Proxying Answer Messages *69*
4.6 Intra-Realm versus Inter-Realm Communication *69*
4.7 Diameter Routing and Inter-Connection Networks *70*
4.7.1 Inter-Connection Approaches *70*
4.7.2 Dynamic Diameter Node Discovery *72*
4.7.2.1 Alternative 1 *73*
4.7.2.2 Alternative 2 *73*
4.7.2.3 Alternative 3 *73*
4.8 Diameter Overload Control *75*
4.8.1 Overload Reports *77*
4.8.2 Overload Control State *77*
4.8.3 Overload Abatement Considerations *79*
References *79*

5 Diameter Security *81*
5.1 Introduction *81*
5.2 Background *82*
5.2.1 Unkeyed Primitives *83*
5.2.2 Symmetric Key Primitives *84*
5.2.3 Asymmetric Key Primitives *84*
5.2.4 Key Length Recommendations *86*
5.3 Security Threats *87*
5.4 Security Services *90*
5.4.1 Diameter Security Model *90*
5.4.1.1 Secure Transports *91*
5.4.1.2 Authorization *92*
5.4.2 Relation to Threats *93*
5.4.3 Mitigating Other Threats *93*
5.5 PKI Example Configuration in `freeDiameter` *94*
5.5.1 The Configuration File *94*
5.5.2 The Certificate *96*
5.5.3 Protecting Exchanges via TLS *97*
5.5.3.1 Common Name and Hostname Mismatch *98*
5.5.3.2 Unprotected Exchanges *99*
5.5.3.3 Certificate Revocation *100*
5.6 Security Evolution *102*
References *102*

6 Diameter Applications *105*
6.1 Introduction *105*
6.2 Base Accounting *105*
6.2.1 Actors *106*
6.2.2 Accounting Application Setup *106*
6.2.3 Accounting Services *107*
6.2.4 Accounting Records *109*
6.2.5 Correlation of Accounting Records *109*
6.2.6 Sending Accounting Information *110*
6.2.7 Accounting AVPs *110*
6.2.8 `freeDiameter` Example *112*
6.2.9 Fault Resilience *113*
6.2.10 Example: 3GPP Rf Interface for Mobile Offline Charging *113*
6.2.10.1 Rf Interface Commands *114*
6.3 Credit Control *115*
6.3.1 Credit-Control-Request Command *116*
6.3.2 Credit-Control-Answer Command *118*
6.3.3 Failure Handling *120*
6.3.4 Extensibility *121*
6.3.5 Example: 3GPP Ro Interface for Online Charging *121*
6.4 Quality of Service *122*
6.4.1 Actors *122*
6.4.2 Modes of Operation *123*
6.4.2.1 Push Mode *123*
6.4.2.2 Pull Mode *123*
6.4.3 Authorization *124*
6.4.3.1 Push Mode Authorization Schemes *124*
6.4.3.2 Pull Mode Authorization *124*
6.4.4 Establishing and Managing a QoS Application Session *126*
6.4.4.1 Establishing a Session *126*
6.4.5 Re-Authorizing a Session *129*
6.4.5.1 Re-Authorization Initiated by the NE *129*
6.4.5.2 Re-Authorization Initiated by the Authorizing Elements *129*
6.4.6 Terminating a Session *129*
6.4.6.1 Session Terminated by the NE *129*
6.4.6.2 Session Terminated by the AE *129*
6.5 Interworking RADIUS and Diameter *130*
6.6 S6a Interface *137*
6.6.1 Evolved Packet Core *137*
6.6.2 S6a Overview *138*
6.6.2.1 Common AVPs for S6a Commands *139*
6.6.3 Authentication *140*
6.6.3.1 Authentication-Information-Request Command *140*
6.6.3.2 Authentication-Information-Answer Command *141*
6.6.4 Location Management *142*
6.6.4.1 Update-Location-Request Command *142*
6.6.4.2 Cancel-Location-Request Command *144*

6.6.4.3 Cancel-Location-Answer Command *145*
6.6.4.4 Update-Location-Answer Command *145*
6.6.5 Subscriber Data Handling *146*
6.6.5.1 Insert-Subscriber-Data-Request Command *146*
6.6.5.2 Insert-Subscriber-Data-Answer Command *147*
6.6.5.3 Delete-Subscriber-Data-Request Command *149*
6.6.5.4 Delete-Subscriber-Data-Answer Message *150*
6.6.6 Fault Recovery *150*
6.6.6.1 Reset-Request Command *150*
6.6.6.2 Reset-Answer Command *151*
6.6.7 Notifications *152*
6.6.7.1 Notify-Request Command *152*
6.6.7.2 Notify-Answer Command *154*
6.6.8 Ending Subscriber Sessions *154*
6.6.8.1 Purge-UE-Request AVPs *154*
6.6.8.2 Purge-UE-Answer Command *155*
6.6.9 Extensibility *156*
References *156*

7 Guidelines for Extending Diameter *159*
7.1 Introduction *159*
7.2 Registration Policies *160*
7.3 Overview of Extension Strategies *161*
7.4 Extending Attribute–Value Pairs *162*
7.4.1 Extending Existing AVPs *162*
7.4.1.1 Creating New AVP Flags *162*
7.4.1.2 Adding AVP Extension Points *162*
7.4.1.3 Adding New AVP Values *162*
7.5 Extending Commands *163*
7.5.1 Allocating New Command Flags *163*
7.5.2 Adding New AVPs *163*
7.5.2.1 Adding New AVPs to Base Commands *165*
7.5.3 Creating New Commands *165*
7.5.3.1 Routing AVPs *165*
7.6 Creating New Applications *166*
7.6.1 The Application-Id *166*
7.7 Lessons Learned *167*
7.8 Vendor-specific Extensions *169*
7.8.1 AVPs *169*
7.8.2 Command Codes *170*
7.8.3 Diameter Applications *170*
7.9 Prototyping with `freeDiameter` *170*
References *170*

Appendix A `freeDiameter` Tutorial *173*
A.1 Introduction to Virtual Machines *173*
A.2 Installing the Virtualization Software *174*

A.3 Creating Your Own Environment *174*
A.4 Downloading the VM Image *174*
A.5 Installing and Starting the Master VM `freeDiameter` *174*
A.6 Creating a Connection Between Two Diameter Peers *175*
A.6.1 Building client.example.net *176*
A.6.2 Building server.example.net *177*
A.6.3 Creating the Diameter Connection *178*

Appendix B `freeDiameter` from Sources *183*
B.1 Introduction *183*
B.2 Tools and Dependencies *183*
B.2.1 Runtime Dependencies *184*
B.2.1.1 SCTP *184*
B.2.1.2 TLS *184*
B.2.1.3 Internationalized Domain Names *185*
B.3 Obtaining `freeDiameter` Source Code *185*
B.4 Configuring the Build *186*
B.5 Compiling `freeDiameter` *188*
B.6 Installing `freeDiameter` *189*
B.7 `freeDiameter` Configuration File *189*
B.8 Running and Debugging `freeDiameter` *190*
B.9 Extensions for Debug Support *192*
B.9.1 Extended Trace *192*
B.9.2 Logging Diameter Messages: *dbg_msg_dumps.fdx* *193*
B.9.3 Measuring Processing Time: *dbg_msg_timings.fdx* *195*
B.9.4 Viewing Queue Statistics: *dbg_monitor.fdx* *196*
B.9.5 Understanding Routing Decisions: *dbg_rt.fdx* *197*
B.9.6 The Interactive Python Shell Extension: *dbg_interactive.fdx* *198*
B.10 Further Reading *199*
Reference *199*

Appendix C The `freeDiameter` Framework *201*
C.1 Introduction *201*
C.2 Framework Modules *201*
C.3 `freeDiameter` API Overview *202*
C.3.1 *libfdproto.h* *203*
C.3.2 *libfdcore.h* *205*
C.3.3 *extension.h* *207*
C.4 `freeDiameter` Architectures *207*
Reference *208*

Glossary *209*

Index *213*

Disclaimer

This book is based on the authors' personal experiences in the technical field and public standards documents created by the 3rd Generation Partnership Project (3GPP), the Internet Engineering Task Force (IETF), and other standards development organizations. The opinions and views of the authors are solely those of the authors and do not necessarily represent the views of organizations where the authors work. Throughout this book the authors have attempted to make it clear when something is an opinion or a view of the authors. Some of the examples, feature lists, and identified ambiguities may not apply universally to all deployments and products.

The publisher and the authors make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the authors shall be liable for damages arising herefrom. The fact that an organization or website is referred to in this work as a citation and/or a potential source of further information does not mean that the authors or the publisher endorses the information that the organization or website may provide or recommendations it may make. Further, readers should be aware that Internet websites listed in this work may have changed or disappeared between when this work was written and when it is read.

About the Authors

This book is a collaborative effort of the following four persons (in alphabetical order):

- **Sébastien Decugis** is the original author and maintainer of the `freeDiameter` implementation. He was involved in IETF activities related to Diameter from 2008 to 2010, and he met Hannes and Jouni working on Diameter at IETF. His work was supported by the National Institute of Information and Communications Technology (NICT) and the WIDE Project, a cross-company and cross-university research project in Japan. Sébastien is not working for those structures anymore, but maintaining and developing the `freeDiameter` implementation on his free time, while NICT and WIDE are kindly maintaining the server resources required by the project.
- **Jouni Korhonen**, PhD, is a Principal R&D Engineer with Nordic Semiconductor. Previously he was with Broadcom and was active in Ethernet-based base station architectures, Ethernet-based fronthaul networks, and time-sensitive networking. Prior to Broadcom Dr. Korhonen was with Nokia Siemens Networks and TeliaSonera where he was heavily involved in IPv6, DNS, mobility, and Diameter-based core network signaling matters in 3GPP and IETF. He has also held multiple leadership positions within IETF and IEEE during his career, including chairing both the Diameter Maintenance and Extensions (DIME) and RADEXT WGs. Dr. Korhonen is still an active contributor with 38 published Requests for Comments (RFCs) to date. His current focus is on cellular Internet of Things and 3GPP system architecture evolution.
- **Jean Mahoney** had wanted to work on an oceanographic research vessel ever since she was a child. Having achieved her life goal right out of college, she discovered that she did not like being in the middle of the ocean. Thus she started on her career in computer networking and technical communication, explaining complex software systems to other developers, system administrators, and users. Jean has more than a decade's worth of experience with IETF specifications and the servers and clients built on top of them. Jean is currently the co-chair of the IETF SIPCORE working group and Gen-ART Secretary.
- **Hannes Tschofenig** co-chaired the IETF DIME working group from March 2006 till March 2010, when he was elected to the Internet Architecture Board (IAB) of the IETF. He is co-author of over 80 RFCs, including several Diameter specifications. His work on Diameter in the IETF was sponsored by Siemens (from 2001 to 2007) and later by Nokia Siemens Networks (from 2007 to 2013), i.e., telecommunication equipment manufacturers selling Diameter-based products. Hannes is now employed by Arm Ltd., where his focus is on improving the security of Internet of Things devices.

Foreword

The Diameter effort started 20 years ago. Its roots were in the limitations of other technologies for user authentication in access networks.

The need for backend authentication servers to assist access networks had grown in the preceding era of modem pools and dial-in access servers. Tools for the simple authentication task existed, but mobile networks in particular needed tools that were capable of growing beyond this task.

The Diameter protocol was born in the IETF. It was designed to be a general-purpose Authentication, Authorization, and Accounting (AAA) protocol for many uses.

Like many other pieces of Internet technology, AAA is not really visible to the end user, but it is crucial for the functioning of the Internet, in particular for the various access networks that provide connectivity for users. When your phone connects to a mobile network, the mobile network's control functions that are needed in the background are built on Diameter.

Mobile networks are the prime area where Diameter is used; simpler other tools also continue their existence and are today equally broadly used, in wireless local area network authentication for instance. And the technology continues to evolve, with most recent designs starting to employ web-based protocols.

The authors, Jean, Jouni, Sébastien, and Hannes, have all worked tirelessly for many years – or even decades – on Diameter, AAA, and other critical Internet technologies. They have written and reviewed specifications, worked on improvements, chaired working groups, built open source implementations, and helped the industry use this technology.

I am happy to see this book on Diameter come out. It focuses on the protocol itself, of course, but also covers open source systems. This is important, as we need both specifications and code to achieve something. It is code that ultimately provides a function, while specifications are needed to ensure that different systems interoperate. The authors approach this book as they have approached their work at the IETF and open source communities, by meticulous attention to detail while keeping the big picture and practical use also up front. Thank you!

Jari Arkko
Senior Expert, Ericsson Research

Preface

Why Did We Write This Book?

"To make money," you will say. That was, however, not our motivation.

We all have been working on Diameter for several years in different roles and therefore we are regularly involved in discussions about Diameter specification questions, or questions about system design and implementation. Often, we go through the same discussions again and again – just with different people.

There was, however, no book to recommend to our co-workers and friends. While we were attending the IETF #86 meeting in Orlando, we sat together outside the conference venue and talked about how to address the common questions we receive. The idea to write a book was born. We reached out to Sébastien, who maintains the `freeDiameter` implementation, and asked him if he would be willing to help us by creating `freeDiameter` examples since we prefer hands-on examples in our technical books.

Since two of us had worked with Wiley before on other book projects, we reached out to Wiley again to socialize our idea. To keep it short, you are now holding a Diameter book in your hands.

We hope you enjoy our approach in making you a Diameter expert. We have set up a dedicated website with additional material for this book. If you have questions or feedback, please send us an email at (diameter.book@gmail.com) or visit our webpage at https://diameter-book.info.

What Does This Book Provide?

This book provides the necessary material to understand Diameter, Diameter applications, and the interactions many applications have with the backend infrastructure.

This book provides a coherent picture of Diameter without regurgitating the specifications. It provides information necessary to understand Diameter. To provide you with a hands-on experience and to make your reading experience more interesting, we make use of an open source implementation of the Diameter protocol, called `freeDiameter`, to

- help you to understand how a Diameter implementation works, and
- illustrate a number of examples using `freeDiameter`.

It is not our goal to cover everything found in the Diameter specifications. We will, however, provide you with the necessary pointers for further reading.

Who is the Intended Audience?

This book assumes only basic familiarity with how Internet protocols work, such as the concept of IP addresses, the layered protocol stack, and the functions of the layers (particularly the "network layer", the "transport layer", and the "application layer").

We use `freeDiameter` for examples and to illustrate test setups. A basic understanding of Unix is required in order to set up the `freeDiameter` environment and to execute the protocol runs. An understanding of TCP/IP will make the examples easier to follow. Readers may skip the examples, but we do recommend engineers use the hands-on experience to gain a deeper understanding of the protocol.

While a technical background or interest in technical matters is a plus, familiarity with the standardization work in the IETF or 3GPP is not required to understand this book.

We believe the following groups will benefit:

- System architects and system designers who have to understand a range of technologies to solve specific use cases. The challenge for those people is to understand the big picture and enough details to glue different protocols together.
- Programmers who need to understand the bigger picture of the Diameter protocol.
- Standardization experts who are new to Diameter or need to define new Diameter extensions.
- Students and researchers who are interested in technology that is deployed by many network operators. Typically, Diameter is not widely known since it is not an end-user-facing technology.
- Technical marketing people who want to gain a better understanding of the technology they are dealing with.

Book Structure

Chapter 1 discusses the motivation for using Diameter, briefly talks about the predecessor to Diameter, RADIUS, and introduces the open source Diameter implementation, `freeDiameter`.

Chapter 2 describes Diameter via its building blocks. These building blocks are then used to illustrate the basic peer-to-peer communication between neighboring Diameter nodes in Chapter 3.

Chapter 4 extends Diameter communication from two nodes to an arbitrary number of nodes.

Following the chapters covering communication between Diameter nodes, Chapter 5 introduces security functionality. Diameter security is today mainly implemented and deployed at the level of peer-to-peer communication.

Chapter 6 describes selected Diameter applications in more detail. We have chosen applications that are deployed today and illustrate the flexibility and capabilities of Diameter well.

Chapter 7 is an advanced chapter that teaches you how to develop your own Diameter extensions, for example by defining new attribute–value pairs (AVPs), new commands, or even completely new Diameter applications.

We have added `freeDiameter` examples throughout the book as far as applicable. Not every standardized functionality is already available in `freeDiameter`.

Acknowledgements

This book effort took much longer than we had expected. A big thanks to Wiley for their continued support and patience. We (Jean, Sébastien, Jouni, and Hannes) had specific ideas in mind of what type of book we wanted to write. We are happy that we managed to implement our ideas in this book without taking shortcuts and came this far in our journey.

Needless to say, this book project would not have been possible without the efforts put forth by those working in the IETF DIME working group. We would also like to thank our peers working in other organizations on Diameter extensions, specifically in 3GPP. A tremendous amount of work has gone into Diameter's standardization and widespread deployment. It does not just happen by accident or luck.

Writing more than 200 pages was not easy, and we would like to thank our families for their patience. Without their support it would not have been possible to complete this project. Thank you, Verena, Elena, Robert, and Hanna. Jouni also sends special thanks to Dana Street Roasting Company for its excellent caffeine-rich products that helped him to stay focused as the writing of this book took place during hours when normal people sleep.

Finally, we would also like to thank our employers. They have enabled us to participate in various standards developing organizations for many years. Not only have we been able to work on exciting technical topics, and to travel around the world to participate in many face-to-face standardization meetings and interoperability events, but we also met many great people.

Hannes, Sébastien, Jean, Jouni