International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-2 Issue-6, August 2013

Testing of Diameter- Based Protocol in the IP Multimedia Subsystem

Vinay Kumar.S.B, Mahendra Kumar M.D

Abstract*—The Diameter protocol was initially developed by the Internet Engineering Task Force (IETF) as an Authentication, Authorization, and Accounting (AAA) framework intended for applications such as remote network access and IP mobility. Diameter was further embraced by the Third Generation Partnership Project (3GPP) as the key protocol for AAA and mobility management in 3G networks [7]. The paper discusses the use of Diameter in the scope of the IP Multimedia Subsystem (IMS) as specified by 3GPP.In this paper, we present a solution for the problem of how to provide authentication, horization and accounting (AAA) for multi-domain interacting service and also the unit testing is used to test the AAA protocol Diameter.

We have studied the case of 'FoneFreez', a service that provides interaction between different basic services, like telephony and television. Because the involvement of several parties like television provider, telephony provider etc., secure interaction between multiple domains must be assured. A part of this security issue can be resolved using AAA [7].

***Index Terms*—Diameter protocol, IP Multimedia Subsystem, AAA,Testing.**

I. INTRODUCTION

In the present-day information society, the life has become unthinkable without the internet, mobile phones, and services provided through various networks. The availability of services and network resources is limited by institutions that provide such services, and it is very significant to keep track and check who can access a particular service, and for how long the service is used. The AAA protocols were created as a means to meet such specific demands. They enable us to identify the user, to recognize which service he is allowed to use, and for how long. In this paper, we will test AAA protocols operating in network environment: Diameter. These two protocols are standard AAA protocols for use in networks. The Diameter protocol was created by the IEEE organization in order to eliminate deficiencies of RADIUS, and to eventually replace RADIUS with the Diameter protocol.

Evolution of the 3rd generation network architecture is driven, among other factors, by the requirement to provide a rather fast, flexible and cost-efficient way of introducing new services for operators, as well as third-party service and content providers. The IP Multimedia Subsystem (IMS), as specified by the 3rd Generation Partnership project (3GPP), represents the key element for supporting ubiquitous service access to multimedia Internet services, with adequate support for Quality of Service as well as advanced, service-differentiated charging [1].

Initially specified by 3GPP/3GPP2, the IMS standards are now being adopted by other standards bodies including ETSI/TISPAN. For the purposes of Authentication, Authorization, and Accounting (AAA) and mobility management in 3G networks, 3GPP has adopted the Diameter protocol [2], developed by the Internet Engineering Task Force (IETF). This paper discusses the use of Diameter within the scope of the IMS and tesing of diameter using unit testing.

Diameter is a very flexible protocol. The adoption by 3GPP boosted the number of network products that implement Diameter. Diameter is mainly used for end-user authentication, authorization and accounting, and is specifically designed for roaming situations.

II. ROLE OF DIAMETER IN IMS

The IMS is based on a horizontally layered architecture, consisting of three layers, namely, Service Layer, Control Layer, and Connectivity Layer. Service Layer comprises application and content servers to execute value-added services for the user. Control layer comprises network control servers for managing call or session set-up, modification and release. The most important of these is the Call Session Control Function (CSCF). Connectivity Layer comprises of routers and switches, for both the backbone and the access network [7].

A. IMS function

A simplified IMS architecture is shown in Figure 1. As mentioned earlier, one of the key functions in the control layer is the CSCF. The HSS serves as the main data storage for user related information, such as IMS user profiles (including location), security and registration information, access parameters, and application server profiles.

The CSCF serve three different purposes, as the Proxy CSCF (P-CSCF), the Interrogating CSCF (I-CSCF) and the Serving CSCF (S-CSCF). The P-CSCF is a Session Initiation Protocol (SIP) proxy that acts as the first contact point between the IMS terminal and the IMS network. It is assigned to an IMS terminal during IMS registration. The I-CSCF is also a SIP proxy, usually located in the home network, at the edge of the administrative domain[5]. Main functions of the I-CSCF are to contact HSS in order to obtain the name of the S-CSCF that is serving the user, and to assign the S-CSCF to the user based on received information received from the HSS[1].

Manuscript published on 30 August 2013.
* Correspondence Author (s)
Vinay Kumar.S.B*, Department of Electronics and Communication, School of Engineering and Technology, Jain University, Bangalore, India.
Mahendra Kumar M.D, Department of Electronics and Communication, School of Engineering and Technology, Jain University, Bangalore, India.

The S-CSCF is the central node of the signaling plane, the "brain" of the IMS[3][4]. The S-CSCF is located in the home network and it uses the Diameter-based Cx and Dx interfaces (reference points) towards the HSS to download and upload the user profiles.

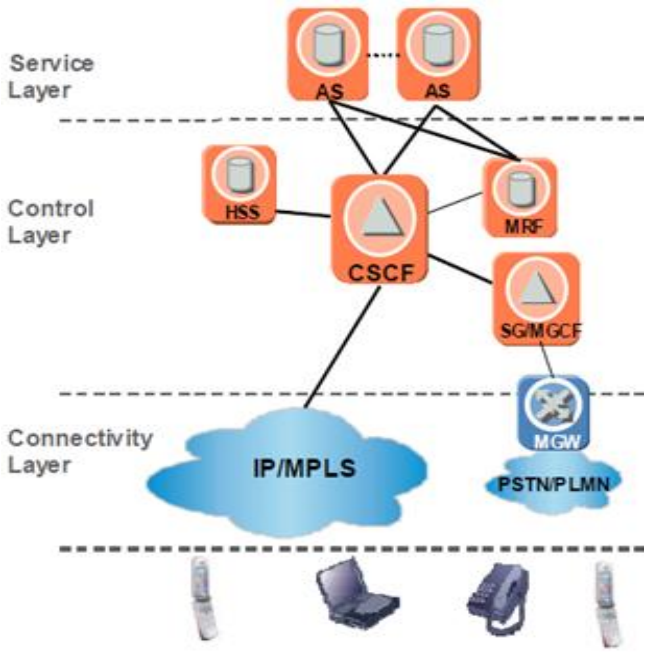

Figure1. The IMS architecture

B. Overview of AAA Protocol

AAA stands for Authentication, Authorization and Accounting. This section looks into the meaning of AAA, and the models used for authentication, authorization and accounting.

Authentication is the verification of the identity of the entity. An entity can be a user or the device a user has, like a computer or the SIM of his mobile phone. With authentication one can prove that it is really the person or device or it claims to be. This prevents from impersonations from other parties. Authentication consists of three sorts: user authentication, message authentication and device authentication.

Authorization is the determination whether the requesting entity is allowed access to a particular resource [1,7]. Authorization is the process of determining if the user has the right to access the network or use services, like the print server from that network. Furthermore, authorization is needed for resource reservation and quality of service support.

Accounting is the collecting of information about resource usage for the purpose of capacity planning, auditing, billing or cost allocation. For example, records are kept
about the duration a user surfs the Internet.

Re-Authentication is the renewal of the authentication by the client upon request of the server. When a session lifetime has expired, or when an error has occurred in the path, re-authentication can be necessary to ensure trust.

C. Diameter Protocol

Diameter is an authentication, authorization and accounting (AAA) protocol developed by the Internet Engineering Task Force (IETF). It is based on an earlier IETF's AAA protocol called RADIUS (Remote Authentication Dial-In User Service), widely used for dial-up PPP (Point-to-Point Protocol) and terminal server access. Extending the functionality of RADIUS, Diameter is designed to provide AAA services for a range of access technologies, including wireless and Mobile IP. The Diameter specifications consist of the Diameter Base Protocol [3], Transport Profile, and applications such as Mobile IPv4, network access server, credit-control, and Extensible Authentication Protocol (EAP). The Diameter Base protocol is utilized for negotiating capabilities, delivering Diameter data units, handling errors, and providing for extensibility. On the other hand, the Diameter application defines application-specific functions and data units. Diameter is an application layer protocol. Transport protocols to carry Diameter messages include Transmission Control Protocol (TCP) and Stream Control Transmission Protocol (SCTP). For securing the connection, Internet Protocol Security (IPSec) and Transport Layer Security (TLS) are applied. Diameter is a peer-to-peer protocol, meaning that any Diameter *node* may initiate a request. The three types of nodes are *clients*, *servers*, and *agents*. Clients are generally the edge devices of a network which perform access control. A Diameter agent provides relay, proxy, redirect, and translation services[8,9], while Diameter server handles the AAA requests for a particular domain, or realm. Message routing is based on the network access identifier of a particular user. In each Diameter node there is a peer table, which contains a list of known peers and their corresponding properties. Each peer table entry is associated with an identity and can be either statically or dynamically assigned. It includes a relative priority setting, which specifies the role of the peer as primary, secondary, or alternative. The status of the peer relates to a specific configuration of the finite state machine of the peer connection, called the Diameter Peer State Machine. As a part of message-routing process, Diameter realm-routing table references the Diameter peer entries.

All realm-based routing lookups are performed against a realm-routing table. The realm-routing table lists the supported realms, with each route entry containing certain routing information. Each route entry is either statically or dynamically discovered. Dynamic entries are associated with an expiry time. The route entry is associated with an application identifier, which enables route entries to have a different destination depending on the Diameter application.

Diameter messages contain a Diameter header followed by a number of Diameter attribute value pairs (AVP). The format of Diameter header is shown in figure 2. The Command-Code field identifies the intention of a message. The Application-ID field identifies the Diameter application that is sending the message, for instance 3GPP applications[6,7,9]. The actual data of Diameter message is carried by a set of following AVP. In the AVP header the AVP Code combines with the Vendor-ID field (if present), will uniquely identify the attribute.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

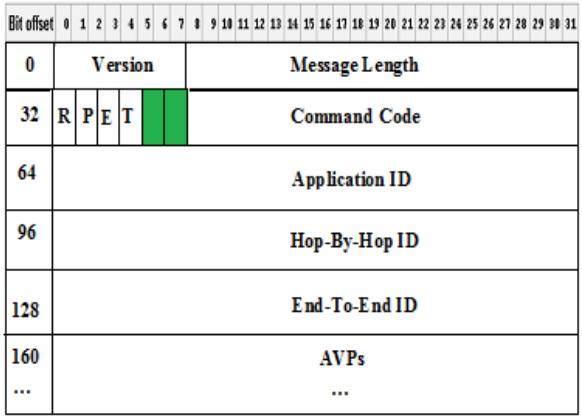

Figure. 2. Diameter package format

III. TESTING OF DIAMETER PROTOCOL

A. Testing

A test case in software engineering is a set of conditions or variables under which a tester will determine whether an application or software system is working correctly or not. The mechanism for determining whether a software program or system has passed or failed such a test is known as a test oracle. In some settings, an oracle could be a requirement or use case, while in others it could be a heuristic. It may take many test cases to determine that a software program or system is considered sufficiently scrutinized to be released. Test cases are often referred to as test scripts, particularly when written.

In order to fully test that all the requirements of an application are met, there must be at least two test cases for each requirement: one SUCCESS test and one FAILURE test. Keeping track of the link between the requirement and the test is frequently done using a traceability matrix. Written test cases should include a description of the functionality to be tested, and the preparation required to ensure that the test can be conducted. A formal written test-case is characterized by a known input and by an expected output, which is worked out before the test is executed. The known input should test a precondition and the expected output should test a post condition.

A1. Unit Testing

Unit testing is a method by which individual units of source code are tested to determine if they are fit for use. A unit is the smallest testable part of an application. In procedural programming a unit could be an entire module but is more commonly an individual function or procedure. Ideally, each test case is independent from the others.In our paper we have 729 test cases,each test cases is done for valid and invalid values to check the functionality of diameter protocol is shown in below figure.3 .

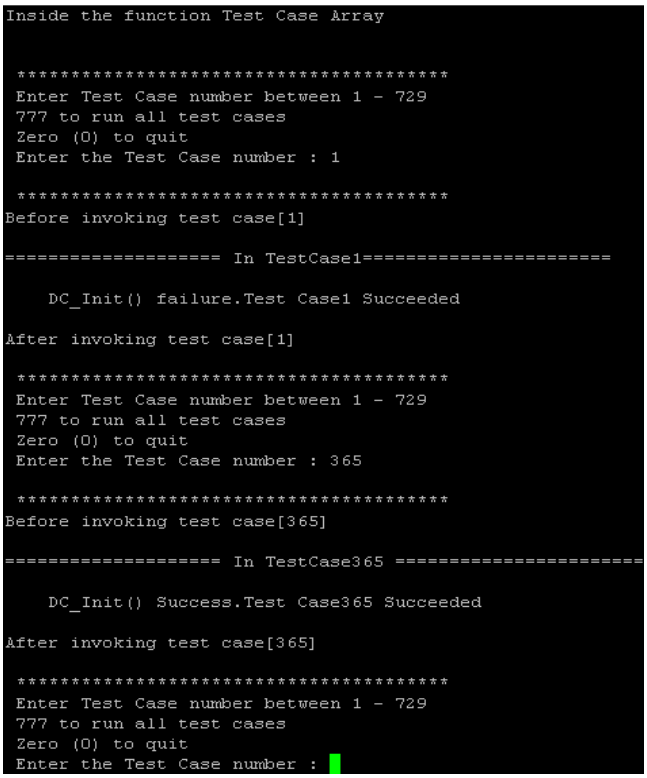

Figure 3.Unit testing

III. CONCLUSION

With the emergence of new wireless access technologies and new applications envisioned in new generation networks, the need for AAA becomes more pressing. The AAA solution adopted by the 3GPP and 3GPP2 for use in the IMS is based on the Diameter protocol. In this paper, we have studied the Testing of Diameter protocol using unit testing.

Therefore that the Diameter protocol can be reused in its existing form, to provide AAA for multi-domain interacting services. It is recommended that further research is done into the exchange of identities for our problem. Furthermore the provisioning of quality of service by Diameter for multi-domain interacting services should be explored.

REFERENCES

1. Vinay Kumar.S.B,Manjula N harihar, *Diameter-based Protocol in the IP Multimedia Subsystem:IJSCE,2012*
2. G. Camarillo, M. A. García-Martín, *The 3G IP Multimedia Subsystem: Merging the Internet and the Cellular Worlds*, John Wiley and Sons, Ltd., England, UK, 2004.
3. P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, *Diameter Base Protocol*, IETF RFC 3588, September 2003.
4. *IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signaling flows and message contents*, The 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; TS 29.228, 2005.
5. *Cx and Dx interfaces based on the Diameter protocol; Protocol details*, The 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; TS 29.229, 2005.
6. J. Loughney, *Diameter Command Codes for Third Generation Partnership Project (3GPP) Release 5*, IETF RFC 3589, September 2003.
7. http://www.fer.unizg.hr/images/50010415/Mipro_2006.pdf
8. http://en.wikipedia.org/wiki/Diameter(protocol).
9. http://en.wikipedia.org/wiki/IP_Multimedia_Subsystem.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Vinay Kumar S.B. is an Assistant Professor in the Department of Electronics and Communication Engineering, School of Engineering and Technology, Jain University, Bangalore. He obtained his Bachelor degree in Electronics and Communication Engineering from Coorg Institute of Technology, ponnampet in 2009, Visvesvaraya Technological University, Belgaum and Master degree (M.tech) in Signal processing and VLSI, Jain University, Bangalore. He is pursuing Ph.D. in Electronics and Communication Engineering, Jain University, Bangalore. My research interest includes VLSI, Reverse logic, DSP and Embedded Systems. He has altogether 3 international journals to his credit and also he presented 8 technical papers in national conference.

Mahendra kumar M.D is a student in the Department of Electronics and Communication Engineering, School of Engineering and Technology, Jain University, Bangalore. He obtained his Bachelor degree in Telecommunication Engineering from AMC Engineering college, Bangalore in 2011 , Visvesvaraya Technological University, Belgaum and He is pursuing M.tech(SP and VLSI) in Electronics and Communication Engineering, Jain University, Bangalore. My research interest includes VLSI, DSP, Micro-Controller.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)