Diameter

Term Paper	Seminar in Communication Systems
Author:	Christian Schulze
Student ID:	2611745
Date:	February 4, 2003
Tutor:	Martin Gutbrod

Table of Contents

Introduction

Diameter is a network protocol that provides AAA services for roaming users [1]. It has been designed by Pat Calhoun of *Black Storm Networks* in 1996 as a replacement for the outdated RADIUS protocol. Its open base protocol provides transport, message delivery and error handling services to applications that need them to function in broader, multi-domain environments [2].

With Diameter's "last call" having been issued by the *Internet Engineering Task Force* (IETF) on October 22, 2002 [3], it has become a proposed standard on January 27, 2003 [12]. It will now serve as an alternative to older protocols like RADIUS and Kerberos [4] or the proprietary TACACS+ [5]. Replacing these older protocols has become necessary with the ever growing number of users in network environments on the one hand and with new applications like Mobile IPv4 on the other.

Since the most widely used AAA protocol is RADIUS [6] and it can be seen as Diameter's predecessor, this paper will concentrate on the limitations of RADIUS and the innovations introduced by Diameter. After a broad overview of AAA services, I will introduce various scenarios where AAA is used and show, how recent developments call for a functionality. While this includes a short introduction to RADIUS as well, I will then explain the Diameter protocol and its advantages in more detail. To sum up this paper, Diameter's current applications, such as CMS Security, Mobile IPv4 and NASREQ will be mentioned. I will then close with a short evaluation and outlook as well as with a list of references for in-depth information.

AAA

Authentication, Authorization and Accounting make up for the three A's that define the main use of the Diameter protocol. They provide protection of investments and businesses against malicious users, but also offer auditing and session information or support for billable services by allowing and tracking network access, gateway services, high bandwidth or low latency or jitter paths [6]. In general, the three A's are defined as:

Authentication

The act of verifying the claimed identity of an entity (user or device) [7].

Authorization

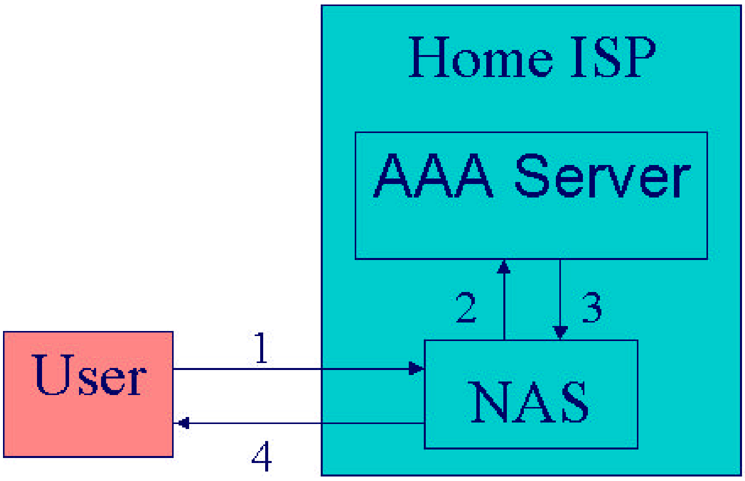
The act of determining if a requester can be granted a right (e.g. network access, high bandwidth service, etc.) [7].

Accounting

The act of collecting information on resource usage for the purpose of trend analysis, auditing, billing or cost allocation [7].

Scenarios

I) Remote dial-in



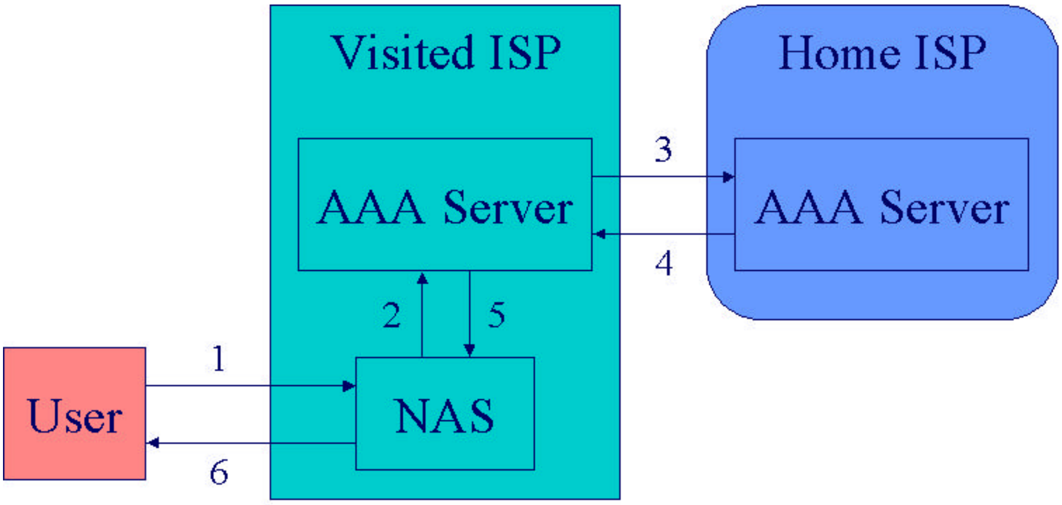
Graphic from [6]

In the above graphic, an end-user dials up a Network Access Server (NAS) that supports a **RADIUS** client. The NAS collects username and password information from the end-user and then forwards it to a RADIUS server. This access-request message containing the user's credentials is encrypted and sent over the network via UDP/IP.

Upon reception, the RADIUS server searches for information on the user in its database and in the case of a positive match returns an access-accept message along with additional information to the NAS or an access-reject message otherwise. The additional information serves to complete the connection and includes an IP address for the end-user and maybe a filter that limits his access to certain areas or protocol types, such as telnet or HTTP [8].

This kind of remote dial-in access is what the RADIUS protocol has been originally designed for. When it was created in 1995 [1] by Livingstone Enterprises [8], it provided AAA services to dial-in users [1] and centralized these functions to one server [6]. Its limitations, however, already show in the following, more complex scenario.

II) Mobile dial-in

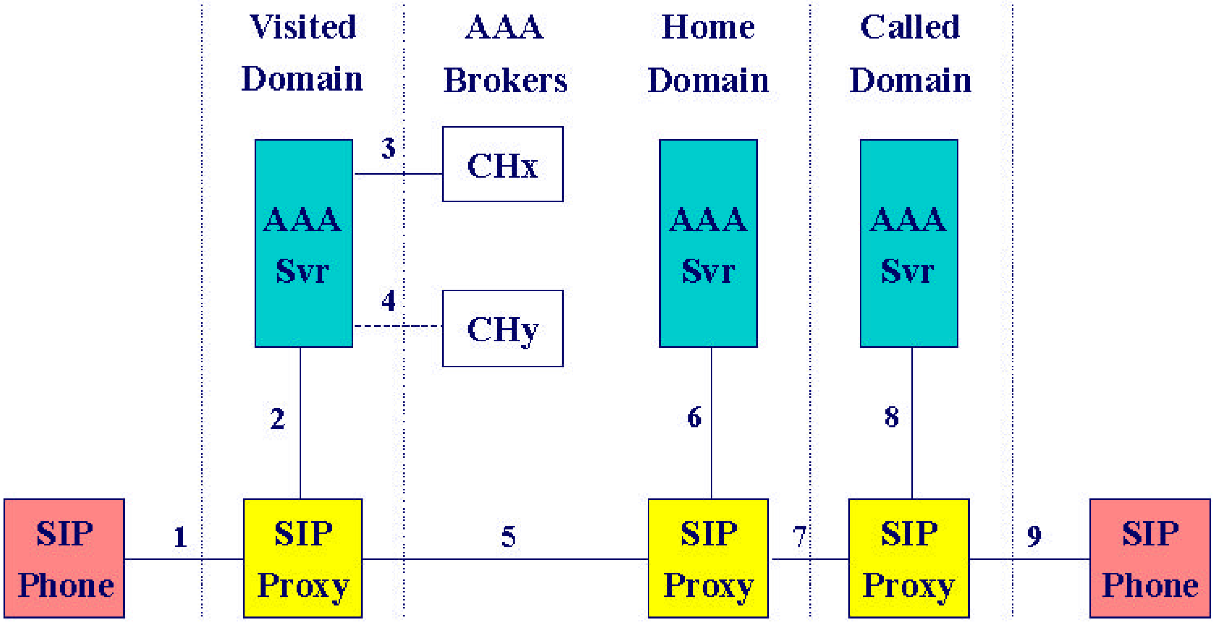


Graphic from [6]

When the remote user from the first scenario decides to dial into the network from a different location and does not directly access the NAS, but comes from a foreign (visited) Internet Service Provider (ISP), the procedures become a little more complicated and complex. The end-user provides the visited NAS with his credentials, who asks his AAA server for an access-accept message. The visited AAA ISP however does not know the end-user and needs to contact the user's home ISP or its home AAA server respectively and asks him for an access-accept

message. The reply then is forwarded from the foreign AAA server to the foreign NAS, which in consequence either grants access or declines.
Obviously, this process involves more entities than in the first scenario. And when these systems become larger and even involve Quality of Service (QoS) services, RADIUS must back down and performs very bad or not at all [6]. Additional problems are posed by the lack of congestion control in RADIUS [6] and its requirement for a shared secret key, which makes access from a foreign ISP even more difficult [8].
Here, Diameters **NASREQ** application, which will be explained in a little more detail later on, is the product of choice, since it has been designed to not only meet the simple requirements of the above scenario, but also the more advance in a mobile dial-in setting.

III) IP-Telephony

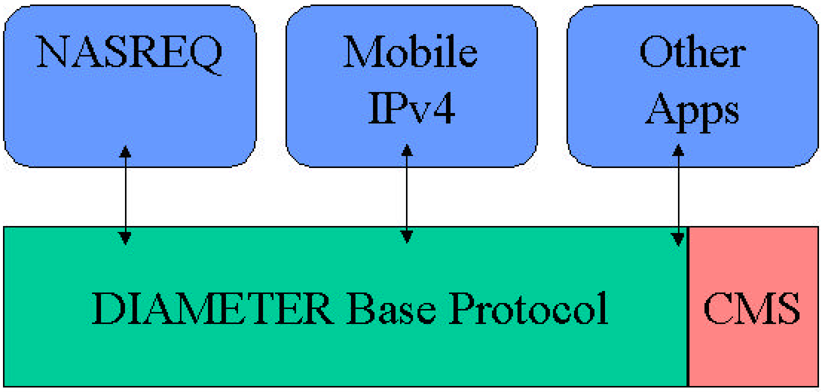


Graphic from [6]

A scenario that RADIUS does not support at all is one that involves the application of the Mobile IPv4 protocol. In the above setup, several AAA servers communicate for several reasons, such as authentication (is the caller really Mr. X and the callee really Mrs. Y), authorization (is he allowed to make a call from Germany to New Zealand) and accounting (10 seconds cost € 3). At the same time, Mr. X might be driving in his car and changing the domain, but needs to keep his IP address so the call is not interrupted.

Without wanting to go into further detail on the use of Mobile IPv4, Diameter provides all the AAA services that make this scenario happen and works in this environment through the use of the **MobileIPv4** application. However, this example introduces another novelty brought along by Diameter: the Broker. Since it is practically impossible for all (home) domains to have contact and contracts with all other (foreign) domains, especially in the huge mobile world, the broker has been instituted. It serves the function of a mediator between two domains that do not know each other but need to work together in a certain setting. In consequence, the relationship between domains can be established, if both parties have at least one broker in common. This allows for unlimited scalability, compared to other concepts of direct relationships that are always confined to less partners.

Design of Diameter



The Diameter protocol consists of two main components, the Diameter Base Protocol and the CMS (Cryptographic Message Syntax) Security Module. The base protocol, as the name suggests, offers all basic functionality needed to provide full AAA services. The CMS Module, which had been a separate entity in earlier versions of the protocol but has been tightly implemented later on, adds the necessary safety features such as encryption and digital signatures. The structure of the base protocol will be examined more closely later on. The advantages of the additional CMS Module will become clearer in the following paragraph "Features of Diameter", as end-to-end security is mentioned.

While these two parts make up for the protocol in itself, it is useless without an application, e.g. in a MobileIPv4 (MIP) or remote dial-in environment. These applications need to be designed specifically to fit with the diameter protocol. As an example, the MIP application provides the transport protocol for the submission of data between two computers. The Diameter protocol makes sure that the computer "calling" really is the one it claims to be, has the right to call and even can collect information on the resources it consumed to fulfil the task. It does not account for accuracy of data, which is left to the application protocol.

Separating the AAA functionality from the respective application is a concept that allows for easy customization and extensibility. As of today, two applications have been developed and brought to an applicable state. The first is the so-called NASREQ (Network Access Server Requirement), which has been designed to supersede the old RADIUS protocol for mobile dial-in environments. The second is the MobileIPv4 application mentioned several times before, which allows for AAA in a mobile telephony environment with moving users.

Features of Diameter

- **SCTP replaced UDP**

  SCTP offers reliable transport, since each node now is responsible for the retransmission of unacknowledged messages [8]. This also avoids inappropriate retransmissions by the NAS [2].

  Also, SCTP is a connection-oriented transport protocol with flow control and congestion avoidance mechanisms [2]. As an alternative, TCP can still be used at the loss of the advantages introduced by SCTP.

- **Keep-alive messages implemented**
  With a connection-oriented transport layer and the Diameter keep-alive messages, a Diameter node can detect the local failure of a peer [2].
  This also offers a failover functionality, which avoids lenghty delay of services if an alternate server needs to be contacted [2].

- **Peer-to-Peer replaces Client/Server**
  While a RADIUS server was unable to terminate connections due to the client/server architecture of the system. Diameter "servers" and "clients" now act as peers [8], allowing every node to send unsolicited messages [2].

- **Timestamp implemented**
  The timestamp in Diameter prevents the system for replay attacks, since every message can be uniquely identified and is not answered twice.

- **Space for extensions**
  The Diameter protocol offers room for vendor-specific commands and attributes, allowing for customizing without threatening interoperability [2].

- **IPSec and TLS implemented**
  As opposed to RADIUS, security is no longer accomplished by a mandatory shared secret, but by IP Security or Transport Layer Security (TLS) [2].

- **CMS allows End-to-End Security**
  The CMS Security module does not only admit hop-by-hop security as in previous protocols, but now also allows end-to-end security through digital signatures, while encryption prevents unauthorized reading of the messages' content [1].

Diameter Protocol Layout

Header

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Ver      |                 Message Length                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|R P E T r r r r|                  Command-Code                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Application-ID                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Hop-by-Hop Identifier                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      End-to-End Identifier                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  AVPs ...
+-+-+-+-+-+-+-+-+-+-+-+-+-
```

The above layout represents the layout of the Diameter header. The "Ver"-field notes the current version of the protocol, which is 1 at present. The Command-Code can be extended for future uses, numbers 1-128 have been reserved for downward-compatibility with the RADIUS protocol. A request of a mobile node in a MIP setting would contain a 260 with the R attribute set for request in the box on the left to it. The application ID will allow for more (proprietary) applications in the future. Noticeable are also the fields for hop-by-hop and end-to-end security mentioned above, where the latter also prevents doubles [9] as a security measure. After this general header format, a various number of Attribute Value Pairs (AVPs) follow, which can contain specific information for AAA purposes.

Attribute Value Pairs

The following shows the format of a diameter Attribute Value Pair (AVP), which allows for backward compatibility with RADIUS and the vendor-specific commands mentioned earlier on [9], but more than that is not so limited in size as to prevent extensions in the future.
An AVP is a pair consisting of two pieces of information. The first contains the description of the attribute (its "name") and the other its value or content. For example, the request of the mobile node with the R-flag set and the 260 command

code will contain among others AVP declaring the mobile nodes home address, the address of the home agent it is trying to connect to, its user name and the also a request for the generation of a secure key for future communication.
The home servers reply (Command Code 262) will the include the desired information (again packaged in AVPs) or an request-rejection message. A detailed description of the long list of AVPs for MIP can be found at [13].

Applications for Diameter

NASREQ

As mentioned in the first scenario with the remote dial-in access of an end-user to his home network, RADIUS has been designed for exactly that task. Since Diameter is meant as a replacement for the RADIUS protocol, it is also build to provide AAA services for dial-in PPP users. For this task, the Diameter Network Access Server Requirement (NASREQ) application has been developed. As often as possible, it uses existing RADIUS attributes to carry the data objects to ease migration from existing systems and reduce protocol conversion for Diameter/RADIUS gateway servers.
The NASREQ application satisfies the requirements of both, RFC 2477 and RFC 3169 and is able to work with the Extensible Authentication Protocol (EAP), Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). The Network Access Server Requirement (NASREQ) might therefore help to eliminate the problems of RADIUS' scalability, resource management and limited extensibility for future technologies [2].

Mobile IPv4

As the scenario for Mobile IPv4 has already been drawn above, I will only summarize the major accomplishments of the Diameter protocol in this area. However, it is important to mention that this application cannot be used with the Mobile IPv6 protocol so far [2].

The advantages of Diameter combined with the Mobile IPv4 protocol are

- Better scaling of security associations
- Mobility across administrative domain boundaries
- Dynamic home agent assignment

Also, the Mobile IPv4 application allows Diameter AAA servers to act as Key Distribution Centers (KDC). This allows the home AAA server to produce a key on the base of a shared secret without requiring the foreign AAA server to know this secret but at the same time allowing him to profit from a secure session key [2].

EAP

The Extensible Authentication Protocol (EAP) is a an authentication method in a Point-to-Point Protocol (PPP) environment. It can be used for a number of authentication schemes and has been suggested as an additional application to the diameter protocol. It will allow for EAP information to be encapsulated in Diameter's AVPs. In this specific case, the command code needs to be set to 268 and the original EAP information is found in a AVP called "eap payload".

This application serves as a very good example how extensible the Diameter protocol is to current needs and future developments.

IPFIX

The Internet Protocol Flow Information eXport has been developed to standardize the collection and submission of information on data flow. This is especially useful for purposes of statistics, but also for accounting and billing information (e.g. AOL charges its users less if their network is congested). While this would be a useful additional feature to the Diameter protocol, the design of a proposed application still has to overcome major difficulties according to [15]. Also, the official Diameter website [16] does not mention IPFIX as a current project yet.

Outlook

Today's AAA protocols have been designed a few years ago and often do not match current requirements as far as scalability, flexibility or extendibility are concerned. Mobile IP, Quality of Service and millions of users with thousands of hosts pose problems that call for a new protocol. Diameter seems to be the answer to it, at least as far as the state at the beginning of 2003 is concerned.

The declaration as a standard by the IETF will only be helpful in spreading this protocol throughout the world, so that it can do what it has been designed for: secure worldwide interoperability.

Current projects like the Moby-Dick-Project [10] already try to implement Diameter and let older RADIUS systems evolve into the new architecture. As soon as the first implementations have reached a certain level of stability, the market will hopefully be keen to put the new protocol into practice - especially taking into account, that major companies such as Nokia, Sun, Cisco and Ericson helped building and fine-tuning this protocol. Last, but not least an open-source project has been started to produce a Diameter reference implementation [14].

Still, especially the NASREQ application might take a little longer to actually replace the old RADIUS protocols that have been in practice for some time and proven to be working. Especially since Diameter is more complex and its security options are harder to implement [11], moving to the new protocol is a major investment - and might not pay off for everybody as of today.

Bibliography

[1] http://www.cs.columbia.edu/~hgs/teaching/ ais/slides/2000/diameter.ppt

[2] Interlink Networks - An introduction to Diameter; http://www.interlinknetworks.com/images/resource/ Introduction_to_Diameter.pdf

[3] http://www1.ietf.org/mail-archive/ietf-announce/Current/msg20836.html

[4] http://web.mit.edu/kerberos/www/

[5] http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Internetworking: Tacacs_plus

[6] Gerhard Gross, http://www.imtc.org/forums/fforum01/presentations/ gerhard_gross_aaa_slides.ppt

[7] Ulf Gustavson, http://www.ce.chalmers.se/undergraduate/IMP/ EDA435/pictures/F6_3_6perpage.pdf

[8] Hakan Ventura, http://www.ep.liu.se/exjobb/isy/2001/3232/

[9] http://www.ietf.org/internet-drafts/draft-ietf-aaa-diameter-15.txt

[10] http://www.interlinknetworks.com/images/ resource/Moby_Dick_Project.pdf

[11] http://www.interlinknetworks.com/images/resource/Diameter_NASreq_App.pdf

[12] http://www1.ietf.org/mail-archive/ietf-announce/Current/msg22328.html

[13] http://www.ietf.org/internet-drafts/draft-ietf-aaa-diameter-mobileip-13.txt

[14] http://www.opendiameter.org/

[15] http://ipfix.doit.wisc.edu/eval/draft-zander-ipfix-diameter-eval-00.txt

[16] http://www.diameter.org