Diameter
next generation’s AAA protocol

Master thesis in Information theory
by
Håkan Ventura
LiTH-ISY-EX-3232-2002
2002-04-25
Diameter
next generation’s AAA protocol

Master thesis in Information theory
at Linköpings Tekniska Högskola
by

Håkan Ventura
LiTH-ISY-EX-3232-2002

Handledare: Miguel Garcia, Peter Cederstrand
Examinator: Viiveke Fäk
Linköping 2002-04-25
Sammanfattning
Abstract
The need for AAA protocols in the world are increasing and todays most common protocols RADIUS and TACACS+, cannot cope with the fast advances in fields benefiting from the use of AAA protocols. This is why IETF has developed the protocol Diameter as a next generations AAA protocol. The objective of this thesis is to account for the work conducted with Diameter as well as to determine if it is going to become the major AAA protocol of the next generation. In this thesis, I describe what Diameter is, its close integration with the Mobile IP protocol and its other uses. As Diameter is based on RADIUS an introduction to AAA and RADIUS is given in order to comprehend where we are today and where we are going as well as to why. I also compare today’s protocols (RADIUS, TACACS+, Kerberos and COPS) against the next generations AAA protocol Diameter. From this comparison, the Mobile IP integration capabilities and an analysis of the support of the Diameter protocol I have come to the conclusion that Diameter is going to become the major AAA protocol of the next generation.

Nyckelord
Keyword
Diameter, RADIUS, AAA protocol, AAA, Kerberos, TACACS+, COPS, Mobile IP, Diameter and Mobile IP integration, Mobile IP integration
Abstract

The need for AAA protocols in the world are increasing and today's most common protocols RADIUS and TACACS+, cannot cope with the fast advances in fields benefiting from the use of AAA protocols. This is why IETF has developed the protocol Diameter as a next generations AAA protocol. The objective of this thesis is to account for the work conducted with Diameter as well as to determine if it is going to become the major AAA protocol of the next generation. In this thesis, I describe what Diameter is, its close integration with the Mobile IP protocol and its other uses. As Diameter is based on RADIUS an introduction to AAA and RADIUS is given in order to comprehend where we are today and where we are going as well as to why. I also compare today’s protocols (RADIUS, TACACS+, Kerberos and COPS) against the next generations AAA protocol Diameter. From this comparison, the Mobile IP integration capabilities and an analysis of the support of the Diameter protocol I have come to the conclusion that Diameter is going to become the major AAA protocol of the next generation.
Acknowledgments

The work presented in this thesis would not be possible without the help and support from several people at Ki-Consulting. First, I would like to thank my supervisors Miguel Garcia and Peter Cederstrand who has given me the opportunity to work with such an exciting project. I would also like to thank the rest of the people at BU Bredband at Ki-Consulting, for their warm efforts to make me feel welcome.

Finally, I would like to thank my sweet girlfriend Camilla Johansson for her continuous support throughout the whole work with this thesis.
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contents</td>
<td>1</td>
</tr>
<tr>
<td>List of figures</td>
<td>2</td>
</tr>
<tr>
<td>List of tables</td>
<td>2</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>3</td>
</tr>
<tr>
<td>1.1 Background</td>
<td>3</td>
</tr>
<tr>
<td>1.2 Problem background</td>
<td>4</td>
</tr>
<tr>
<td>1.3 Problem specification</td>
<td>4</td>
</tr>
<tr>
<td>1.4 Objective</td>
<td>4</td>
</tr>
<tr>
<td>1.5 Method</td>
<td>4</td>
</tr>
<tr>
<td>1.6 Limitations</td>
<td>4</td>
</tr>
<tr>
<td>2 Frame of reference</td>
<td>4</td>
</tr>
<tr>
<td>2.1 AAA</td>
<td>4</td>
</tr>
<tr>
<td>2.1.1 Authentication</td>
<td>4</td>
</tr>
<tr>
<td>2.1.2 Authorization</td>
<td>4</td>
</tr>
<tr>
<td>2.1.3 Accounting</td>
<td>4</td>
</tr>
<tr>
<td>2.1.4 How does AAA work?</td>
<td>4</td>
</tr>
<tr>
<td>2.2 Today there is RADIUS, what is it?</td>
<td>4</td>
</tr>
<tr>
<td>2.2.1 RADIUS Funktion</td>
<td>4</td>
</tr>
<tr>
<td>2.2.2 RADIUS Architecture</td>
<td>4</td>
</tr>
<tr>
<td>3 DIAMETER</td>
<td>4</td>
</tr>
<tr>
<td>3.1 Diameter - An introduction</td>
<td>4</td>
</tr>
<tr>
<td>3.2 How is Diameter constructed?</td>
<td>4</td>
</tr>
<tr>
<td>3.2.1 Diameters Architecture</td>
<td>4</td>
</tr>
<tr>
<td>3.2.2 The Diameter message construction</td>
<td>4</td>
</tr>
<tr>
<td>3.2.3 Diameter base protocol</td>
<td>4</td>
</tr>
<tr>
<td>3.2.4 Does Diameter servers work with RADIUS?</td>
<td>4</td>
</tr>
<tr>
<td>3.2.5 Diameter API</td>
<td>4</td>
</tr>
<tr>
<td>3.3 What applications are there today</td>
<td>4</td>
</tr>
<tr>
<td>3.3.1 NASREQ</td>
<td>4</td>
</tr>
<tr>
<td>3.3.2 Mobile-IP</td>
<td>4</td>
</tr>
<tr>
<td>3.3.3 CMS security</td>
<td>4</td>
</tr>
<tr>
<td>3.3.4 ROAMOPS</td>
<td>4</td>
</tr>
<tr>
<td>3.3.5 Accounting</td>
<td>4</td>
</tr>
<tr>
<td>3.3.6 Resource management</td>
<td>4</td>
</tr>
<tr>
<td>4 Analysis</td>
<td>4</td>
</tr>
<tr>
<td>4.1 The need for a more powerful AAA protocol</td>
<td>4</td>
</tr>
<tr>
<td>4.2 Advantages/Disadvantages Radius compared to Diameter</td>
<td>4</td>
</tr>
<tr>
<td>4.2.1 Authentication</td>
<td>4</td>
</tr>
<tr>
<td>4.2.2 Authorization</td>
<td>4</td>
</tr>
<tr>
<td>4.2.3 Accounting</td>
<td>4</td>
</tr>
<tr>
<td>4.2.4 General differences between the RADIUS and Diameter protocol</td>
<td>4</td>
</tr>
<tr>
<td>4.3 Competition: Advantages/Disadvantages Diameter vs.</td>
<td>4</td>
</tr>
<tr>
<td>4.3.1 Kerberos</td>
<td>4</td>
</tr>
<tr>
<td>4.3.2 TACACS+</td>
<td>4</td>
</tr>
<tr>
<td>4.3.3 COPS</td>
<td>4</td>
</tr>
<tr>
<td>4.3.4 Evaluation Criteria</td>
<td>4</td>
</tr>
<tr>
<td>4.3.5 Evaluation of the protocols according to 4.3.4</td>
<td>4</td>
</tr>
</tbody>
</table>
4.4 Which vendors supports the Diameter protocol and how ........................................4
4.4.1 Diameter test suite ..................................................................................................4
4.5 How Diameter can be implemented in Mobile-IP networks ...................................4
4.5.1 The message flow of integrated Mobile IP/Diameter networks ..........................4
5 Conclusions ..............................................................................................................4
6 References ..................................................................................................................4

List of figures

Figure 2.1: AAA architecture .........................................................................................4
Figure 2.2: RADIUS Function ......................................................................................4
Figure 2.3: RADIUS Packet Format ............................................................................4
Figure 3.1: Diameter Protocol Architecture ...................................................................4
Figure 3.2: Diameter Header .........................................................................................4
Figure 3.3: AVP header .................................................................................................4
Figure 3.4: Proxy Chain .................................................................................................4
Figure 3.5: Mixed Diameter Security Models ...............................................................4
Figure 3.6: Roaming/mobile IP AAA with Diameter .....................................................4
Figure 3.7: Diameter Proxy Network ............................................................................4
Figure 3.8: Diameter Redirect service ..........................................................................4
Figure 4.1: How Kerberos work ....................................................................................4
Figure 4.2: PDP-PEP interaction Specified by the COPS protocol ...............................4
Figure 4.3: Mobile-IP Trust Model .............................................................................4
Figure 4.4: Wireless IP Architecture for an integrated .................................................4
Figure 4.5: Mobile IP/Diameter Message Exchange .....................................................4

List of tables

Table 4.1: The Mechanisms and Algorithms used with CMS objects .........................4
1 Introduction

1.1 Background

Since the number of new internet services have increased rapidly the last years the routers and Network Access Servers (NAS) have needed to be constantly upgraded in order to handle them. Most of these new services are in need of an Authentication, Authorization, and Accounting (AAA) protocol to facilitate off-loading of policy information to an external server.

Large ISPs don’t want to take on the big administrative burden of reconfiguring all their users with every NAS every time the NAS equipment is upgraded. In order to avoid this, ISPs very successfully have used different AAA protocols, like Kerberos, TACACS and RADIUS (Remote Access Dial-In User Service) which is the most widely used AAA-protocol in the market today.

Historically, the RADIUS protocol has been used to provide AAA services for dial-up PPP (Point-to-Point Protocol)\(^1\) and terminal server access. Over time, as routers and network access servers (NAS) have increased in complexity and density and with the arrival of new services, the RADIUS protocol have become increasingly unsuitable for use in such networks.

Some of the new services such as Voice over IP, Fax over IP, Mobile IP and RAP all require similar services in order to be able to authenticate, retrieve authorization information, and generate accounting records for billing purposes.

The current trend is for each IETF working group (Voice over IP, Fax over IP, Mobile IP and RAP) to define its own policy protocol for a specific service, each with their own nuances. This requires customers to deploy several policy servers, which increases the cost of administration and complicates the deployment of several services.

Recently, within the IETF considerable attention has been given to the need to better structure the information carried in protocols operating within the network access environment. The arguable benefits of structured information is consistency in the definitions and reuse of individual data elements and well defined means for extending existing structures to support new or proprietary features and capabilities.

Diameter offers a common solution to the above stated scenarios and needs by defining a base protocol, which defines the header formats, security extensions and requirements as well as a small number of mandatory commands and AVPs. All the new services then have the ability to extend Diameter by adding applications extending the base protocol to support new functionality. This allows for each Working Group within IETF to use Diameter just adding their new service specific requirements not already supported by Diameter in an application.

---

\(^1\) W. Simpson, "The Point-to-Point Protocol (PPP)", RFC 1661, July 1994
1.2 Problem background

Today the Radius protocol is the leading AAA protocol on the market. The main usage for RADIUS today is to take care of Authentication, Authorization and collect Accounting information in a distributed dial-in PPP environment. New services and usage areas that could benefit from the usage of an AAA protocol have increased almost exponentially the last couple of years. With the increased usage of today’s AAA protocols limitations in them have started to show. With some services who benefit from AAA support today’s protocols are directly unsuitable. The IETF is developing a new open standard called Diameter in order to cover new services and usage areas. The first intended AAA usage area in companies all over the world, today using RADIUS or its competitor protocols, is now just a small part of the areas in need of an AAA protocol and has changed with their adaptation to the new services on the market. So network managers in larger companies see the short comings in today’s protocols and have to decide if they want to upgrade to the next generations AAA protocol or just try to circumvent the shortcomings by clever implementations. Today everything indicates that we are heading toward a wireless community and with the introduction of Mobile IP and its increasing popularity more and more ISPs see the benefits of their AAA protocol being able to interact with the Mobile IP protocol.

The intention is to provide KI-Consulting and the readers of this thesis with a guide, to Diameter, to what problems a new AAA protocol can solve and to determine if Diameter is this new protocol. This provides the readers with a basic understanding to why a new protocol might be needed and helps in determining if an upgrade from RADIUS to the Diameter protocol should be conducted.

1.3 Problem specification

From the problem background (section 1.2 above) the following questions arise and they are going to be studied with the intention to provide KI-Consulting and the readers of this thesis with a guide to Diameter.

The questions the network managers and ISPs are faced with are:

1. What is Diameter? (section 3)
2. Why is a more powerful AAA protocol needed? (section 4.1)
3. What advantages does Diameter provide in comparison to RADIUS regarding:
   - Authentication (section 4.2.1)
   - Authorization (section 4.2.2)
   - Accounting (section 4.2.3)
4. What general advantage does Diameter provide compared to RADIUS? (section 4.2.4)
5. There are other AAA protocols than RADIUS that might be used today; how are they suited for future tasks in comparison to Diameter? (section 4.3)
6. How many and what vendors supports the Diameter protocol? (section 4.4)
7. How can Diameter be implemented in Mobile IP networks? (section 4.5)
1.4 Objective

The objective of this thesis is to account for the work conducted with Diameter as well as to determine if it is going to become the major AAA protocol of the next generation.

1.5 Method

Through extensive literature studies each one of the above problems stated in section 1.3 are going to be addressed. And through the study of the specified problems conclusions are going to be drawn and based on these final conclusions are stated so that the objective of the thesis is reached.

The intention to provide KI-Consulting and the readers of this thesis with a guide to Diameter is then obtained through sections 3 and 4. The comparison of Diameter to other protocols than RADIUS (section 4.3) is limited to the Evaluation criteria’s stated in section 4.3.4 and is supposed to provide some ideas of the competition the Diameter protocol has and when the different protocols best can be used.

1.6 Limitations

Since this thesis is about the work conducted with Diameter, I don’t go in too deeply on how the competitor protocols work, set aside Radius which gets a bit deeper examination since Diameter has adopted several parts from Radius.

When comparing the Diameter protocol against competitor protocols the scope of this thesis is limited to a comparison of the protocols against the evaluation criteria’s stated in section 4.2., which are constructed by KI-consulting.
2 Frame of reference

2.1 AAA

(This section is based on reference [13] when no other reference is stated)

The Internet is an insecure place [14]. Many of the protocols used in the Internet do not provide any security. Tools to “sniff” passwords off of the network are in common use by malicious hackers. Thus, applications, which send an unencrypted password over the network, are extremely vulnerable. Worse yet, some client/server applications rely on the client program to be “honest” about the identity of the user who is using it. Other applications rely on the client to restrict its activities to those, which it is allowed to do, with no other enforcement by the server.

This is why it is necessary to authenticate that the person or client you are communicating with are in fact who they say they are.

Once the requester is authenticated in one way or another, one has to determine what services to allow the requester. With the use of policy-based decisions the requester can be authorized to different services by evaluating the policies regarding those services.

In order to keep track of all the authorized users, accounting information is gathered for different purposes, like abuse handling of malicious users and billing purposes. To provide maximum coverage to the increasing roaming and mobile subscriber stock ISPs may (and seems to) choose to pool their NAS resources while keeping control over their subscribers access, usage and billing information. All these services require coordination between various administrative systems supported by the ISPs in partnership with each other.

The core of AAA Authentication, Authorization, and Accounting is to meet these challenges in a simplified and scalable manner. AAA essentially defines a framework for coordinating these individual disciplines across multiple network technologies and platforms. In practice, an AAA server with a database of user profiles and configuration data communicates with AAA clients residing on network components, such as NAS and routers, to provide distributed AAA services.

2.1.1 Authentication

“Authentication the act of verifying a claimed identity in the form of a pre-existing label from a mutually known name space, as the originator of a message (message authentication) or as the endpoint of a channel (entity authentication).” [12]

Authentication, the first “A” in AAA involves validating the end user’s identity prior to permitting them network access. This process keys on the notion that the end-user possesses a unique piece of information, a username-password combination, a secret key, or perhaps biometric data (fingerprints, for example); that serves as unambiguous identification credentials. The AAA server compares the user-supplied authentication data with the user-associated data stored in its database, and if the credentials match,
the user is granted network access. A mismatch results in an authentication failure and a denial of network access.

2.1.2 Authorization

“Authorization the act of determining if a particular right, such as access to some resource, can be granted to the presenter of a particular credential.” [12]

Authorization, the second “A” in AAA, defines what rights and services the end user is allowed once network access is granted. This might include providing an IP address, invoking a filter to determine which applications or protocols are supported, and so on. Authentication and authorization are usually performed together in an AAA-managed environment.

2.1.3 Accounting

“Accounting the act of collecting information on resource usage for the purpose of trend analysis, auditing, billing, or cost allocation.”[12]

Accounting, the third “A” in AAA, provides the methodology for collecting information about the end user’s resource consumption, which can then be processed for billing, auditing, capacity-planning purposes and also for abuse handling purposes in order to monitor and act against malicious users.

2.1.4 How does AAA work?

Figure 2.1 below illustrates the components of an AAA solution. The AAA server, multiple servers can be used for resiliency (see figure 3.7), is attached to the network and serves as a central storage place for storing and distributing AAA information. The device acting as the point of entry into the network is typically a NAS (although it could also be a router, a terminal server, or perhaps another host) that contains an AAA client function.

AAA processing can be summarized in the following steps:

- End user connects to the point-of-entry device and requests access to the network.
- NAS AAA client function collects and forwards the end user’s credentials to the AAA server.
- AAA server processes the data and returns an accept or a reject response and other relevant data to the AAA client.
- The AAA client on the NAS notifies the end user that access is granted or denied for the specified resources.

The NAS may also send an accounting message to the AAA server during connection setup and termination for record collection and storage.
An AAA client (NAS) at the POP (Point-of-presence) of the network communicates with the AAA server in order to provide AAA services.

One of this architecture’s benefits is that the AAA server can be housed on a general-purpose computing system, which can typically be found at a good price-to-performance ratio, offering high-volume disk storage and optimized database administration. This gives dial providers the horsepower needed to process bursts of AAA requests from the many port-dense NAS devices as well as the storage capacity needed to record accounting information on each of the many end-user connections. A single AAA server can act as a centralized administrative control point for multiple AAA clients contained within different vendor-sourced NAS and network components. Thus, AAA functions can be added to the server, and incrementally to the client, without disrupting existing network functions. There is no need to incur the operational burden of placing AAA information on the NAS itself.
2.2 Today there is RADIUS, what is it?

RADIUS (Remote Access Dial-IN User Service) is today the most widely used AAA protocol in the world, in competition with TACACS+ and Kerberos. One of the things that have made RADIUS greatest among the existing AAA protocols is that it is vendor independent, i.e. it isn’t controlled by a single vendor, contrary to TACACS+ (Cisco) and Kerberos (Merit).

2.2.1 RADIUS Funktion

RADIUS was developed in the mid nineties by Livingston Enterprises (later bought by Lucent Technologies) in order to provide their NAS Equipment with Authentication and Accounting services. IETF formalized Livingston’s work in 1996 by appointing RADIUS WG (Working Group) which resulted in that the basic functions and format got standardized in RFC 2138. RADIUS functionality can be summarized in:

- **Client-server-based operations.** A RADIUS client resides on the NAS and communicates over the network with a RADIUS server running on a host computer. Additionally, a RADIUS server may serve as a proxy client for another RADIUS or authentication server.
- **Network security.** All communications between a RADIUS client and server are authenticated by virtue of a shared secret key that is never sent over the network. In addition, user passwords contained in RADIUS messages are encrypted to prevent hackers from reading them by snooping the network.
- **Flexible authentication.** RADIUS can support multiple authentication mechanisms, including PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol) and EAP (Extended Authentication Protocol).
- **Attribute/value pairs.** RADIUS messages carry AAA information encoded in type-length-value fields, called attributes (or attribute/value pairs). Common examples of attributes include User-Name, User-Password, Framed-Protocol (such as PPP), Framed-IP-Address (IP address for end user), and so on. RFC 2138 and vendor-specific documentation contain more complete lists of RADIUS attributes supported by servers and clients.
Figure 2.2: RADIUS Function

The RADIUS client on the NAS forwards the end user’s credentials in an Access-Request message to the RADIUS server. After validating the end user’s credentials, the RADIUS server returns an Access-Accept message to the client.

An end-user dials into a NAS that supports a RADIUS client. Using a prompt, or perhaps PPP frames, the NAS collects the username and password from the end user. It then uses UDP/IP to forward an encrypted Access-Request message over the network to the RADIUS server. The message may also contain attributes such as the NAS port ID and IP address.

The RADIUS server then checks the User-Name attribute for a matching entry stored in its database. If there is no match, then the server returns an Access-Reject message to the NAS along with an optional text message indicating the reason for the failure. The NAS, in turn, notifies the end user of the authentication failure. If a match is found and the password is correct, then the RADIUS server returns an Access-Accept message to the NAS along with any additional configuration information required to complete the connection, such as an IP address for the end user or a filter that limits them to a specific protocol type, like Telnet or HTTP.

2.2.2 RADIUS Architecture

RADIUS information is sent in RADIUS packages and these consist of a header (see figure 2.3) together with different RADIUS objects. The objects are called AVPs (Attribute-Value-Pair) and to consist of a header and data-payload.

![Figure 2.3: RADIUS Packet Format](image)
The header in a RADIUS package consists of four different data fields:

- One 8 bits code field (Code) which determines what kind of package it is.
- One 8 bits identifier field (Identifier) which helps to match requests with responses.
- One 16 bits length field (Length) containing the package length including all AVPs.
- One 32 bits Authentication field (Authenticator) which is used to Authenticate the response from the RADIUS server and is also used as a part of the algorithm to conceal the client password at requests.

The RADIUS AVPs contains the specific Authentication, Authorization and Accounting information and configuration details concerning the requests/responses. The AVPs consists of three fields (see figure 2.4 below).

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Length</th>
<th>Value</th>
</tr>
</thead>
</table>

Figure 2.4: AVP format
3 DIAMETER

3.1 Diameter - An introduction

The RADIUS protocol has since a time back been used with AAA services for dial-in PPP(Point to Point Protocol) and terminal server access. But at the same rate as routers and network access servers (NASs) have increased in numbers and size the RADIUS protocol has become less useful in such large networks. The Diameter protocol wasn’t created out of nothing but the creators rather have retained the basic RADIUS format and have tried to fix all the known different RADIUS deficiencies. Diameter doesn’t use the same Protocol-Data-Unit (PDU) as RADIUS but still borrows sufficiently from RADIUS in order to be backwards compatible. The idea with Diameter is to create a base protocol which easily can be extended in order to allow new access methods. Currently the developers are limiting the scope of the Diameter protocol to Internet access, through common PPP and through the criteria’s stated by the ROAMOPS and Mobile-IP models (see section 3.3.4 and 3.3.2 respectively).

3.2 How is Diameter constructed?

3.2.1 Diameters Architecture

Diameter consists of a Base protocol [4] and different extensions and applications like CMS Security [5], NASREQ [7] and Mobile-IP [6] (see fig 3.1). All basic functionality common to all applications and services is implemented in the base protocol while all application specific functionality exists within the different applications.

The Diameter base protocol [4] concerns itself with capabilities negotiation, how messages are sent and how peers may eventually be abandoned. The base protocol also defines certain rules which apply to all exchanges of messages between Diameter nodes. The Diameter base protocol is intended to provide an AAA framework for Mobile-IP, NASREQ (Network Access Server REQuirements) and ROAMOPS (ROAMing OPerationS). The Base protocol also specifies message format, transport, error reporting and security services to be used by all diameter application and must be supported by all Diameter implementations.

In order to use the Diameter protocol for different services the different implementations of the protocol has to support the applications providing the functions connected with the services.
Figure 3.1 shows a schematic picture over the architecture of the Diameter protocol, with the base protocol as the base closely connected to the CMS Security application in order to provide security to all applications and how the other applications though having different functions all must support the base protocol.

3.2.2 The Diameter message construction

The Diameter messages, like the RADIUS messages, consists of a header followed by a selection of AVPs.

![Diameter Header](image)

Figure 3.2: Diameter Header
The AVPs consist of an AVP header followed by the data connected to the selected AVP.

![AVP header](image)

**Figure 3.3: AVP header**

### 3.2.3 Diameter base protocol

As stated earlier the base protocol must be supported by all implementations of Diameter as well as all applications. The base protocol [29] defines the PDU (Protocol-Data Unit) format for Diameter, as well as a couple of primitives and the basic security in Diameter which is extended with the use of the close connection to the CMS security application.

Contrary to RADIUS, the base protocol defines Diameter to run over Stream-Control-Transmission-Protocol (SCTP)\(^1\) which supplies Diameter with reliable and thorough retransmission capabilities.

Since SCTP allows windowing the AAA servers can limit the number of incoming packages, which allows the Diameter clients to distribute the traffic load to different servers.

The transport layer’s retransmission and timeout timers allow clients and servers to detect the reachability state of peers, allowing for quick transition to back-up servers.

The Base Protocol assumes a peer-to-peer communication model, as opposed to a client-server model. The following goals have motivated the design of the base protocol:

- lightweight and simple to implement protocol
- Large AVP space
- Efficient encoding of attributes, similar to RADIUS
- Support for vendor specific AVPs and Commands
- Support for large number of simultaneous pending requests
- Reliability provided by underlying SCTP
- Well-defined fail-over scheme
- Ability to quickly detect unreachable peers
- No silent message discards
- Support of unsolicited messages to “clients”

---

\(^1\) Stream-Control-Transmission-Protocol, RFC
- integrity and confidentiality at the AVP level
- Hop-by-Hop security
- One session per authentication/authorization flow
- Provide redirect (referral) services, to allow bypassing of broker

The Diameter base protocol is intended to simply provide a secure transport for the messages defined in the various application-specific extensions. It is therefore imperative that the base be lightweight and simple to implement. In the Diameter protocol, data objects are encapsulated within the Attribute Value Pair (AVP). An AVP consists of three parts: the Identifier, the Length and the Data. A unique AVP Identifier is assigned to all data objects in order to be able to distinguish the data contained. The AVP Identifier namespace must be sufficiently large to ensure that future protocol extensibility is not limited by the size of the namespace, as in the RADIUS protocol. Furthermore, vendors wishing to add “proprietary” extensions must be allowed to do so by using a vendor-specific namespace, managed by IANA.

For many years the question as to whether RADIUS should operate over UDP or TCP has led to heated discussion. It must be determined whether the benefits that UDP provides are worth the implementation complexities. Over time, according to RFC 2865 [1], it has become clear that these benefits are well worth the cost. The issue with TCP is that an AAA protocol requires a quick retransmission and fail-over scheme, which TCP cannot provide.

The Diameter protocol must be able to operate over a transport that has an aggressive retransmission strategy in order to efficiently switch to an alternate host when the peer in question is no longer reachable. Contrary to RADIUS, the Diameter protocol requires that each node in a proxy chain acknowledge a request, or response, at the “transport” layer. Since Diameter operates over SCTP, which provides a reliable transport, each node in a proxy chain is responsible for retransmission of unacknowledged messages.

The SCTP transport provides retransmission detection, which greatly simplifies server implementations, and consequently allows a given server to support a much larger number of transactions per second. SCTP also provides windowing, which allows the flow of packets to a specific server to be controlled. Clever implementations can then decide to send the packets to an alternate server that can handle the load.

With the exception of a few security related errors, the Diameter base protocol requires that all messages be acknowledged, either with a successful response or one that contains an error code.

Where the RADIUS protocol is client-server, the Diameter protocol is peer-to-peer, allowing unsolicited messages to be sent to NASes. There are many benefits to peer-to-peer AAA protocols. One example is the on-demand retrieval of accounting data; another, server-initiated session termination.

The Base Diameter protocol provides for hop-by-hop security, similar to the scheme employed by RADIUS today. However, the Diameter protocol also provides for replay protection through a timestamp mechanism. This security scheme requires a long lived security association to be established by peers, or can make use of keying material negotiated out of band. The Base Protocol also allows the built-in security
measure to be turned off which is good if you want to use IPSec to provide integrity and confidentiality between two Diameter peers.

The Diameter protocol is a session-oriented protocol, meaning that for each user being authenticated, there exists a session between the initiator of the authentication/authorization request and the home Diameter server. Sessions are identified through a session identifier, which is globally unique at any given time. All subsequent Diameter transactions (e.g., accounting) must include the session identifier to reference the session. A Session termination message exists in order to end a Diameter session, and all sessions have a timeout value in order to ensure that they can be cleaned up properly.

Since today's processors work more efficiently when objects are aligned on a 32-bit boundary, the Diameter protocol requires 32-bit alignment of all headers and the data. This has recently become a common requirement for many new protocols at the IETF.

### 3.2.4 Does Diameter servers work with RADIUS?

The Diameter protocol was designed with RADIUS compatibility in mind. The RADIUS protocol defines a one octet attribute space, and the Diameter protocol reserves the first 255 attribute identifiers to be the same as those defined in RADIUS. This allows Diameter servers to easily perform protocol conversion, since in order to map a RADIUS attribute to a Diameter AVP an additional dictionary lookup isn’t necessary.

A Diameter server can easily read a typical RADIUS \[ 10 \] profile without any additional conversions by reusing the RADIUS attribute space, which reduces the need for duplicate user profiles for both protocols and makes database conversion unnecessary.

### 3.2.5 Diameter API

A standardized API (Application Interface) is not strictly necessary for protocol interoperability (see \[ 11 \]), but it does help a great deal to promote the use and deployment of the Diameter protocol by reducing the amount of work necessary to develop and access applications that use the protocol.

### 3.3 What applications are there today

Even though all implementations of the Diameter protocol has to support the base protocol it is never used on its own. The base protocol according to \[ 21 \] is always extended with at least one application in order to support a particular service. Although Diameter can be used to solve a wide set of AAA problems, and that is one of the reasons why a replacement/complement to RADIUS is developed, the AAA workgroup at the IETF are currently limiting the scope of the protocol to three Diameter applications, which are defined in companion documents to the base
protocol: NASREQ, Mobile-IP and CMS Security, in order to ensure that the effort remains focused on satisfying the requirements of network access.

Within IETF other workgroups like the Mobile-IP workgroup and the NASREQ workgroup are defining sets of specifications for the Diameter protocol in order to support their workings which have resulted in the AAA workgroups Mobile-IP and NASREQ applications. The Roaming Operations Workgroup (ROAMOPS) has published a set of specifications that define how a PPP user can gain access to the Internet without having to dial into his/her home service providers modem pool. This is achieved by allowing service providers to cross-authenticate their users. These specifications makes it possible for an user to dial into any service providers point of presence (POP) which has a roaming agreement with the users home Internet Service Provider (ISP), the benefits are obvious, the user doesn’t have to incur an expensive long distance charge while travelling. In early drafts of the Diameter protocol these specifications were to be formed in a Diameter application but lately the AAA Workgroup has integrated the roaming functionality into the Diameter base protocol.

With the AAA Workgroup currently concentrating on network access several larger companies and members of the AAA workgroup are writing their own drafts on other applications like Resource management and Mobile-IPv6. The main ideas of the network access applications and the other mentioned applications are presented and described below.

### 3.3.1 NASREQ

The Diameter NASREQ Extension defines a set of authentication/authorization commands, which can be used for CHAP, PAP and EAP. Diameters support for larger AVPs and the SCTP transport properties have made the use of EAP much more palatable, allowing for end-to-end user authentication, which reduces many of authentication replay attacks known to exist with CHAP and PAP.

Unlike PPP, Mobile-IP hosts do not have a long-lived “nailed-up” connection to a PPP server, but rather get service from routers that provide service in a particular cell. In the Mobile-IP world, the router is known as a Foreign Agent, while the moving hosts are known as Mobile Nodes. The mobile nodes home network has a host that forwards all messages destined to the mobile node through the Foreign Agent. This router is commonly referred to as the Home Agent.

The Diameter NASREQ application describes a Diameter application that is used in order to provide AAA functions in a PPP/SLIP Dial-Up and Terminal Server Access environment. The NASREQ application, combined with the base protocol [4], satisfies the requirements defined in the NASREQ AAA criteria specification [17] and the ROAMOPS AAA Criteria specification [36].

The NASREQ Application contains three main sections. The first section defines the Diameter Command-Codes and AVPs that are needed to support the RADIUS legacy authentication protocols, authentication protocols that are typically supported by RADIUS servers. The second section defines the Command-Codes and AVPs necessary for a Diameter node to support PPP's Extensible Authentication Protocol.
(EAP) [25]. The Authorization AVPs for various services offered by a NAS, such as PPP dial-in, terminal server and tunnelling applications, such as L2TP (Layer two Tunnelling Protocol) are described in the third part of the application.

Given that it is expected that initial deployments of the Diameter protocol in a dial-up environment will include legacy systems, this application was carefully designed to ease the burden of servers that must perform protocol conversion between RADIUS and Diameter. This is achieved as stated in section 3.2.4 by re-using the RADIUS address space, eliminating the need to perform attribute lookups. The NASREQ extension makes use of the attributes defined in the RADIUS protocol to carry the data objects. This is intended to ease migration of existing RADIUS servers to Diameter since they could share a single dictionary and user profile. Furthermore, this reduces the amount of processing required for an inter-working system that acts as a RADIUS/Diameter bridge.

3.3.2 Mobile-IP

Mobile-IP as described in RFC 2002 [27] defines a method that allows a Mobile Node to change its point of attachment to the Internet, i.e. move from one cell (subnet) to another while retaining the same IP-address, minimising the impact on applications, which allows for minimal service disruption. Mobile-IP in itself doesn’t provide any specific support for mobility across different administrative domains (roaming), and this limits the use of Mobile-IP in a large-scale commercial networks. Since the use of Mobile-IP is desirable in large networks too the Mobile-IP protocol [27] needs to be extended.

In order to give a Mobile Node (MN) access to networks resources, the Mobile Node needs to be authenticated and authorized according to Le [32], and the already existing AAA infrastructure can suitably be used. Besides supporting Mobile Node authentication and authorization, the AAA infrastructure can also be used for distributing the security keys needed to support the Mobile Node roaming. The AAA infrastructure can be used to support mobility procedures and to optimize authentication, authorization and mobility in a common procedure. AAA protocols such as Diameter precisely enable mobile users to roam and obtain service in networks that may not necessarily be owned by their home service provider. The AAA functions provided by Diameter, thus combined with Mobile IP, allow a inter-domain development of Mobile IP. This allows Diameter to be used in large-scale commercial networks such as future cellular networks.

The Diameter Mobile-IP application [31] extends the Diameter Base protocol to allow a Diameter server to authenticate, authorize and collect accounting information for Mobile IPv4 services rendered to a mobile node. Combined with the Inter-Realm capability of the base protocol, this application allows Mobile Nodes to receive service from Foreign Service providers. The Mobile IP application defines how the Foreign and Home agents can use the Diameter Accounting messages to transfer usage information to the Diameter servers.

In order to follow the security model specified in the Mobile IP protocol [27] the mobile nodes and home agents are required to share a pre-existing security association, which leads to scaling and configuration issues (see section 4.5). The
Diameter Mobile-IP application solves this through defining Diameter functions that allow the AAA server to act as a Key Distribution Centre (KDC), whereby dynamic registration keys are created and distributed to the mobility entities for the purposes of securing Mobile IP Registration messages.

In consistency with the roaming model defined by the ROAMOPS Working Group the AAA servers implementing the Mobile IP application uses the users’ identities supplied in the Network Access Identifiers (NAI), which is used by the base protocol for the message routing services, and this allows the Mobile Node not to have a static mobile home address or static home agent. A dynamic home address and agent helps the Mobile IP networks to be scalable since every agent doesn’t have to assign IP-addresses.

The Mobile-IP application also defines how the Mobile–IP and Diameter messages flow when a Mobile Node requests service in a Foreign Network, see section 4.5.

3.3.3 CMS security

The Diameter base protocol allows Diameter servers to communicate securely, using hop-by-hop authentication. Hop-by-hop authentication means that the requesting server has secure communication with a proxy or redirect server, and the proxy has secure communication with the home server. The hop-by-hop security is provided by the fact that the Diameter base protocol relies on either IPsec (IP Security) or TLS (Transport Layer Security) for integrity and confidentiality between two Diameter nodes. The base protocol also defines a Diameter proxy server that forwards requests to other servers when it detects that a given request cannot be satisfied locally. In such proxy environments security information is lost at each Diameter agent.

The ROAMOPS Working Group within the IETF has defined a requirement in [36] which requires that Diameter servers that are communicating through proxies must provide end-to-end AVP integrity and confidentiality, making it difficult for proxy agents to modify and see sensitive information within the message. The Mobile-IP and NASREQ Working Groups have stated in RFC 3169 [17] and RFC 2977 [19] that non-repudiation is a requirement for AAA data, such as accounting records.

When a chain of proxies use hop-by-hop security (e.g. TLS, IPsec), a proxy may modify information in a Diameter message. It is almost impossible for the rest of the nodes in the proxy chain to know that a message has been altered during delivery. Figure 3.4(below) shows an example of such a network, where Diameter node 3 (DIA3) modifies the contents of “foo” in both the request and the response.

![Figure 3.4: Proxy Chain](image-url)
The CMS Security application document [5] describes how strong authentication and encryption can be provided in the Diameter protocol, by encapsulating CMS (Cryptographic Message Syntax) objects [37] in AVPs. There are two main techniques to secure messages provided by the CMS Security application. Digital signatures (along with digital certificates) provide authentication, integrity and non-repudiation. Encryption provides confidentiality (using asymmetric techniques to encrypt a content encryption key, which then is used for bulk encryption). Both techniques can be used simultaneously to provide end-to-end authentication and confidentiality, thus providing end-to-end security.

In the case of Figure 3.4, the originator of the request and response can add a digital signature that covers a set of AVPs within the message. The protected AVPs can then not be changed by an intermediate proxy server (DIA2, DIA3) without detection since the signature validation performed by the end server would fail.

When redirect services are used, a network layer security protocol, such as IP Security, may be used to secure the traffic between the two Diameter servers. However, security at the application level may still be necessary in this network configuration, specifically the ability to authenticate a select set of AVPs. Brokers that operate in a redirect mode typically require that both Diameter servers sign the same set of AVPs, in accounting records. The accounting record, signed by both parties is then forwarded to the broker via the local Diameter server. This provides the broker with some assurances that both networks agreed on the accounting data, which the broker then can use for settlement purposes.

Given that asymmetric transform operations are expensive, Diameter servers may wish to use them only when dealing with inter-domain servers, as shown in Figure 3.5 (below). This configuration is normally desirable since Diameter entities within a given administrative domain may inherently trust each other. Further, it is desirable to move this functionality to the edges, since NASes do not necessarily have the CPU power to perform expensive cryptographic operations.

The Diameter CMS Security application [5] provides the confidentiality and different security features through the establishment of a security association between the end nodes. The application specifies two sets of messages which can be used in order to establish the security associations:
1. A set of messages DSR and DSA (Diameter Security Association Req/Ans) that allows a Diameter node to establish a security association, which is used to secure AVPs within a Diameter message, even though the message may traverse intermediate Diameter agents. A set of AVPs are also defined to sign and encrypt AVPs.

2. A set of messages, known as PDSR and PDSA, allows a Diameter client to request that an agent (third party) establish a Diameter security association with a server in a specific realm.

Once the security associations are established end-to-end security is provided to the messages. Through the close connection between the Diameter Base protocol and the CMS Security application when implemented, this application provides security to all other applications.

3.3.4 ROAMOPS

In the very first drafts of new AAA-protocol later to be called Diameter, according to the Diameter framework [20], the intention was to support roaming networks following the criteria’s established by ROAMOPS [36]. ROAMOPS, according to the Base protocol [21], realised that it would be an impossible task for each ISP to establish roaming agreements with every ISP (given the number of ISPs today). So ROAMOPS defined a “broker” whose only purpose is to establish these roaming agreements and a “Roaming consortium” which is the broker and a collection of connected ISPs.

While ROAMOPS only focused on roaming connected with PPP the Mobile-IP working group recently focused on inter administrative domain mobility and established criteria’s which are very similar to the ROAMOPS criteria’s but with Mobile-IP as the access protocol (figure 3.6 below shows how similar both criteria’s are).

---

Figure 3.6: Roaming/mobile IP AAA with Diameter

Roaming/mobile IP AAA with Diameter. A Diameter Broker, brokers AAA information between AAA servers on the visited and home networks.

---

Roaming networks, according to ROAMOPS, means that every node in the network is responsible for its own retransmissions, and that the protocol does allow each node to know a priori the reachable state of each peer. This allows for a flexible network, and efficient retransmission scheme. With the support of the ROAMOPS model the redirect, proxy and relay servers are supported and defined in the Diameter protocol. Diameter relay and redirect agents must transparently support the Diameter base protocol and all Diameter applications. The Diameter Proxy servers must support the base protocol and fully support every application which is needed to implement proxied services.

Figure 3.7 shows an example of a Diameter network that includes two proxy servers and alternate home servers in the local network for resilience. Once a message has been sent from the NAS to one of its local proxy servers, they are responsible for any retransmissions of the message to one of the home servers. Since SCTP provides quick peer failure detection, the local proxies can quickly transmit the message to the alternate peer in the home network upon failure notification as well as the NAS can switch to alternate proxy server upon failure notification.

The fact that each node in the proxy chain is responsible for its own retransmissions and fail-over detection provides the following benefits:

- The number of Diameter nodes in the network is greatly reduced.
- The time involved in switch-over to an alternate peer is greatly reduced.
- Reliability is increased.

The redirect servers provide simple Diameter message “routing” functions and are generally deployed in order to reduce the configuration information that would otherwise be necessary on all servers owned by members of a roaming consortium.
Through the message "routing" the redirect servers allow Diameter entities to communicate directly by providing NAI (Network Access Identifier) realm to home server translation services. When a request is received by a redirect server, a redirect response is returned to the initiator of the request with the information necessary to communicate directly with servers in the home domain (See figure 3.8).

![Figure 3.8: Diameter Redirect service](image)

Diameter Broker Returning Redirect Indication and the NAI information which allows the local Diameter server to communicate directly with the home Diameter server.

### 3.3.5 Accounting

As soon as a Diameter node receives a successful authentication and/or authorization messages from the Home AAA Server, according to the base protocol [4], it must collect accounting information about the session. The previous Accounting extension [30], now included as a part in the Diameter base protocol, provides usage collection to both the Mobile-IP and the NASREQ extensions.

The accounting requirements specifications (specified in RFC 2989) define that an accounting protocol must provide the following functionality:

- Negotiable transfer mechanism.
- Provide general purpose AVPs.
- Flexible to allow new extensions to use the accounting extension.
- Scalable to allow millions to users and thousands of sites.
- Secure accounting data transfer.

These functions are now provided by the base protocol and like the RADIUS protocol, Diameter includes accounting usage information in AVPs. The base protocol like the previous Accounting extension defines a set of accounting AVPs that are used

---

1 NAI example-user@realm
for all services, while each extension defines their own service specific accounting AVPs.

Diameter allows accounting information to be sent in real-time. Real-time accounting transfers are useful in environments where timely arrival of the information is required, such as when debit cards are used like mobile phone cards.

The base protocol accounting combined with the CMS Security application, provides strong authentication of accounting data, which may be used to omit repudiation of accounting data, for instance from dishonest foreign ISPs. The CMS Security application also allows multiple parties to sign the accounting information, which is beneficial in environments that include a referral broker. The foreign and home servers can both sequentially sign the accounting record, and submit the result to the broker. The broker can then use the signatures to ensure that both parties agreed to the contents of the accounting record.

### 3.3.6 Resource management

Many network access services requiring AAA support need servers to maintain session state information according to [22]. An example of the need for session state information is when using dial-up PPP as an access protocol, since the introduction of flat-rate internet access, there has been a surge in fraud where a user provides his username/password pair to other people. The end result is that a single username (account) can have simultaneous concurrent sessions. Hence the need for session state information in order to circumvent this fraud.

Earlier ISPs have had to implement proprietary extensions to RADIUS, in order to attempt to identify when such fraud occurs. Unfortunately, since RADIUS does not provide the necessary functionality required to maintain state information, these solutions have been largely unreliable and cunning criminals have found ways of using this.

According to the “NASREQ AAA requirements” RFC 3169 [17] AAA servers supporting the NASREQ application are required to maintain session state information. This is typically used to enforce a local policy decision, such as limiting the number of simultaneous sessions for a specific user and maintaining IP address pools.

The Diameter Base Protocol, together with the Mobile IP and NASREQ extensions provide some of the functionality that is required for servers to maintain state information, such as:

- Reliable Transport
- Indication of the termination of a session
- A Reboot message
- Interim Accounting
- Accounting On/Off message
- Ability to re-authorize an existing session

The above features allow servers to keep state information but it may also be necessary for Diameter nodes, to be able to query for the active sessions.
This extension (Resource Management [22]) describes an extension to the Diameter protocol that allows the server to query for active session state information from access servers. Usually done in order to rebuild state information should it be lost for any reason, which could occur after a device failure, or this may be done periodically in order to ensure that the state is current.

The state information is exchanged via the Resource-Token AVP specified in this extension, which is used to encapsulate a set of AVPs that describe the session and resources used. There is one Resource-Token AVP for each active session.
4 Analysis

4.1 The need for a more powerful AAA protocol

The AAA protocols of today were designed several years ago, in the beginning of the nineties, with the intention to provide AAA infrastructure to the requirements and environments of that age. The requirements put on AAA protocols have changed over the years, with the development of new technologies, with new demands and new services. The AAA protocol developers have tried to retain the existing RADIUS protocol and in order to support every change in the AAA protocol needs for the RADIUS protocol to still be usable have resulted in that numerous patches to the RADIUS protocol have been made. Since the RADIUS protocol isn’t scaleable in itself the need for new patches arises every time a new service is supposed to be supported. The amounts of patches have started to make it hard for implementers to support all different patches and at the same time maintain interoperability. Since the RADIUS protocol works over UDP (which doesn't provide any retransmission scheme) and the fact that the protocol doesn’t support a watchdog feature, users of the RADIUS protocol have no way of knowing a priori the reachable state of peers it is trying to communicate with. This has led to that the RADIUS protocol has weak proxy capabilities since a NAS for instance has to timeout before it recognises that a node in a proxy chain is down. This creates unnecessary long service disruptions in long proxy chains. All these reasons for wanting a new AAA protocol have to do with deficiencies in the RADIUS protocol. Many of the deficiencies with the RADIUS protocol comes from the fact that it was created to provide AAA infrastructure for traditional PPP networks, and with many of the newer services relying on mobility, support for Mobile IP and roaming is of essence to an AAA protocol. And with the need for roaming and mobility RADIUS doesn’t cope with the newer services and needs in the near future. With the extended terminal use in the world, RADIUS also have proved to show weaknesses in very large networks, one reason is that it requires a shared key between the RADIUS server and its clients (including possible proxy nodes) which doesn’t comply with roaming capabilities (see section 4.3). In order for an AAA protocol to provide mobility it has to have key distribution capabilities and the AAA protocols of today lack this capability. The amounts of shortages in the RADIUS protocol itself and its extensibility problems results in a need for a newer protocol.

4.2 Advantages/Disadvantages Radius compared to Diameter

A few of the reasons why the Diameter protocol was created was that the current AAA protocols weren’t scaleable, didn’t provide the ability to extend to the numerous of new AAA needs, and that there have been a growing number of protocols and applications which could benefit from the offloading that an AAA protocol can facilitate. One of the reasons for this thesis is to try and account for the differences between RADIUS the market leading AAA protocol of today with Diameter one of next generations AAA protocol. The findings of these investigations are presented below under 4 subsections, 4.2.1-4. The first three are addressing Authentication,
Authorization and Accounting issues and section 4.2.4 addresses other general/major differences between the RADIUS protocol and Diameter protocol. The criteria’s evaluated below are established by the writer together with the supervisor at Ki-Consulting, and are mainly brought to attention by the criteria’s established by IETF for evaluation of AAA protocols, “Criteria for Evaluating AAA Protocols for Network Access” RFC 2989 [12]

4.2.1 Authentication

- Authorization without Authentication

The Radius protocol does not support non-Authenticated Authorization, because the protocol does require some form of credentials in request messages. The Diameter protocol does not require Authentication information to be included in the request to the other peer. Authorization without Authentication is a requirement from the NASREQ Working Group to assert that dummy credentials doesn’t have to be filled in according to RFC 3169 [17], thus minimizing the processing burden on servers.

- PAP/plaintext password support

Even though PAP is an ill-suited protocol in today’s networks, it is still in use in many applications. Therefore AAA protocols to be used in large scale roaming networks still need to securely transport plaintext passwords. And in order for an AAA protocol to securely transport plaintext passwords it has to provide confidentiality for the password and it also must protect the password against disclosure to proxies in forwarding paths. Since RADIUS only supports hop-by-hop security (see hop-by-hop section 4.2.4) it can’t prevent disclosure of the password to proxies, neither can it provide end-to-end confidentiality of the password (see DATA object confidentiality in section 4.2.4). The Diameter protocol can by its CMS security application both provide the confidentiality as well as keep proxies from getting hold of the password as needed.

- Replay attacks and denial of service attacks

Since RADIUS doesn’t contain end-to-end Authentication just hop-by-hop authentication, the protocol does not include any replay attack prevention. This means that a malfunctioning server or malicious user can replay old packets without detection. For example when Radius is used in a proxy chain this means that a malicious user or server through a proxy server can replay old access-request messages to an RADIUS server and get Access-Accept messages back and use this to get access to network resources. For servers that maintain state information, to limit the number of concurrent sessions for a user, this can be used against the RADIUS server to mount a denial of service attack simply by replaying old RADIUS messages. For servers not keeping state information another drawback with no replay prevention are that it can be used to send duplicate accounting messages, which might create economical disadvantages to the ISP. The Diameter protocol prevents replay protection through a timestamp mechanism and through the support of end-to-end Authentication.
The RADIUS protocol requires that a shared secret exists between two peers. That this can be a problem and the magnitude of it can be realised when thinking of Mobile nodes roaming through different administrative domains since all Foreign Agents need a shared secret with the home agent, which require all Agents to have database containing unlimited amounts of shared secrets. The Diameter protocol does not require shared secrets.

### 4.2.2 Authorization

- **RADIUS gateway capability**

Since RADIUS is the largest AAA protocol today, the next generations AAA protocols need to have RADIUS capabilities in order to ease migration and be able to interact with the major AAA agents today, which maybe neither needs nor wants to migrate to Next Generations AAA protocol. The Diameter protocol was engineered/created with RADIUS capabilities in mind, but with all the applications trying to comply with the different IETF Working Groups requirements on Next Generation AAA protocol and the changes of the RADIUS protocol, has resulted in that the Diameter protocol today doesn’t completely satisfy backward capability. Obviously the RADIUS protocol support RADIUS gateway capabilities but with all the different implementations from different vendors it isn’t certain that all RADIUS implementations are interoperable. It is safe to say though that the RADIUS protocol by nature is better at providing RADIUS gateway capability than Diameter.

- **State-Reconciliation**

If an AAA protocol has State-Reconciliation capabilities it allows the clients to use the AAA server to manage Resource allocation state. State-Reconciliation allows the server to assist the clients with:

- Simultaneous user login control
- Limitations on port usage
- IP-address pooling
- Tunnel limits
- Connection time

But in order for an AAA server to assist its clients with these tasks the AAA protocol must provide state recovery capabilities, in case data is lost due to fault of any reason, like at an AAA server reboot. And in order for AAA protocols to provide state recovery session/resource status and update and disconnect messages is needed. RADIUS doesn’t provide applicable commands for any of the above needed messages as well as it has the issues with unsolicited messages (see section 4.2.3). Diameter on the other hand through the former resource management application and now by the base protocol do support the messages needed for state recovery and therefore supports State-Reconciliation.
Unsolicited disconnect

The Diameter base protocol defines a set of termination messages that can be used for unsolicited disconnects. The Diameter server sends a Session Termination Request (STR) to the client which then acknowledges the termination of the session. In comparison RADIUS in the newer RFCs of the protocol also includes a set of disconnect messages but the ability of unsolicited disconnect fails as the protocol fails to support unsolicited messages. The ability for servers to initiate a disconnect is useful when changes in the different authorization polices occurs at the servers.

Re-Authorization on demand

“Re-Authorization on demand” refers to the ability for a server or client to trigger re-Authorization. RADIUS is according to the RADIUS RFC [ 1 ] stated to support this feature by the Session-Timeout and Terminate-Action AVPs, but these AVPs just provide the ability to Re-Authorize periodically, and that can’t be considered to be on demand. As stated below (see section 4.2.3) a RADIUS server doesn’t have the ability to send unsolicited messages to the client so even on this point the RADIUS protocol fails to support this feature. Diameter on the other hand supports this feature through its session-based peer-to-peer relation between the “server” and “client”.

4.2.3 Accounting

Support of unsolicited messages

Unsolicited messages are messages that are not a reply to an explicit request. The RADIUS protocol doesn’t allow a server to send unsolicited messages to its clients (the NASes). As network services have become more complex, this limitation has forced implementers to deviate from the RADIUS protocol, causing interoperability problems. Since Diameter is a session based protocol (peer-to-peer) it supports unsolicited messages from the Diameter “server” (any direction from peer to peer) in traditional “server to client” sense. In comparison RADIUS does not support unsolicited messages since it is a client/server protocol that requires a client to initiate a request. Support of Unsolicited messages is typically needed for accounting purposes, to request that a NAS terminate a specific user session and to support of services where session/configuration information have to be changed during a session, like with mobile phone cards which have a credit limit.

4.2.4 General differences between the RADIUS and Diameter protocol

Scaleable

RADIUS as protocol isn’t scaleable, because the RADIUS protocol states that the identifier field, found within the header, is used to identify transmissions. Since the identifier field only is one byte the number of requests that can be pending simultaneously is only 255. With the dense NASes today the 255 pending messages,
that was enough when RADIUS was created, has made the protocol nearly unusable, but to solve this the problem is being worked around by making use of multiple UDP ports to ensure that no more than 255 simultaneous requests are pending on each port. The Diameter Protocol is scalable since it has a four bytes identifier and can handle $2^{32}$ (one byte = 8 bits) pending request at the same time. This makes a Diameter peer use fewer ports. The RADIUS protocol also requires that retransmitted requests, which include changes to the packet, include a new value in the Identifier field. Since most retransmissions do include updated information, and therefore typically require a new Identifier field. This further reduces the number of sessions that can be supported by the Identifier field and creates further congestion problems. In Diameter the session identifier is always the same for every message sent in that session, retransmitted or not.

- **Data object confidentiality**

The RADIUS Protocol doesn’t provide the messages with End-to-End confidentiality, only hop-by-hop confidentiality and this allows proxies to manage the intended confidential information in plain text. Diameter does provide end-to-end confidentiality and therefore keeps objects confidential even when traversing in proxy-paths.

- **Data object integrity**

The RADIUS Protocol doesn’t provide the messages with End-to-End integrity, which Diameter is able to do with the CMS security application implemented and the hop-by-hop security feature.

- **Auditability**

When proxies are used in the message transfer the Diameter protocol creates a trail and this trail is used to provide auditability. RADIUS on the other hand does not support any similar ability and cannot used to audit the received data.

- **Extensibility**

  1. **Limitation of AVPs**

One of problems that RADIUS suffers from is its limitation on the length of attribute data. This limitation is imposed by the fact that the RADIUS protocols attribute header only reserves one byte for the length field, which allows for 256 different AVPs. This limitation makes each vendor limited to only 256 different attributes. Diameter resolves this limitation by defining four bytes to the AVP space, which in comparison to the 256 attributes per vendor for RADIUS allows for $2^{32}$ AVPs per vendor. This has rendered that RADIUS isn’t considered very extensible.

The RADIUS protocol also allows multiple attributes of the same type to be included within a message therefore; it is difficult for a RADIUS server, or client, to determine whether multiple identical attributes are in fact multiple independent attributes, or a single fragmented attribute.

  2. **Support for vendor-specific commands**
Although the RADIUS protocol does support vendor-specific attributes, it does not allow for vendor-specific commands. This has forced vendors to abuse the address space, creating interoperability problems in mixed (roaming) vendor environments. Diameter does allow for vendor specific commands through the ability to extend the base protocol with vendor defined applications specifying their specific commands. Since every implementation of Diameter supports the base protocol every communication with a Diameter agent also presents what kind of application is supported by the agent and this determines if the Diameter protocol it can get service through that agent.

- Hop-by-Hop security

The RADIUS protocol uses hop-by-hop security, which means that every hop in a RADIUS proxy network adds authentication data that is used by the next peer in the chain. Since every hop can edit the RADIUS message RADIUS doesn’t support end-to-end security and can therefore not secure the message the whole link between the NAS and the home server, which would have eliminated the ability for proxy servers to modify critical components in messages. This has caused opportunities for fraud in RADIUS networks, since intermediate nodes i.e. proxy nodes can easily modify information (accounting information), and such events are difficult to trace since as above stated the end-to-end integrity is missing. Diameter on the other hand does support end-to-end security and as above stated provide object integrity which does prevent any fraudulent editing to the message.

- Retransmission procedure

Given that the RADIUS protocol requires that the Identifier field be changed in retransmissions that have updated information, RADIUS server implementers have had to design clever tricks to identify retransmissions. The most commonly used method is to cache all packets received within a time window. When, with this method implemented, servers receive a packet, it compares the contents of certain attributes, which are know to be static across retransmissions, with corresponding attributes in all packets in the cache. When a match is found, a retransmission has been detected. This places a burden on RADIUS servers and adds additional latency. Since the Diameter protocol runs over SCTP, which provides retransmission detection the server implementation is greatly simplified. This also allows a given server to support a much larger number of transactions per second.

- Control of the flow to servers

RADIUS does not include any windowing support and given the rather bursty nature (comes in part from the fact that RADIUS operates over UDP) of the RADIUS protocol, servers today have no way of properly managing their receive buffers. Large bursts of requests directed at a server can burden that servers ability to respond in a timely manner. The most common problem is that a server can become unavailable and all requests must be sent to an alternate server. SCTP, which Diameter operates over, provides a windowing scheme, which allows the flow of packets to a specific server to be controlled. This can then be used, through clever
implementations, by the AAA clients to distribute the traffic load across multiple alternate servers that can handle the load.

- **Alignment requirements**

Most of today’s processors work more efficiently when objects are aligned on a 32-bit boundary; due to this fact almost every newer IETF protocol requires that all data to be processed are aligned with 32-bits alignment. In order to allow efficient processing of data the Diameter protocol requires 32-bit alignment of all headers and the data (AVPs). Contrary to Diameter the RADIUS protocol doesn’t require any alignment of data and this puts an unnecessary burden on most processors, as all fields within the header and attributes must be treated as byte aligned characters.

- **Silent discarding of packets**

The RADIUS protocol states that messages that doesn’t contain the expected information or messages that have errors are silently discarded i.e. ignored without response. Silently discarding messages causes the NAS to assume that the local RADIUS server is no longer reachable since it doesn’t get any response on its pending requests, resulting in that the NAS retransmits all pending requests to alternate servers (see Server failure detection). When the messages arrive at the alternate servers the messages again will be silently discarded whereupon the NAS has to retransmit to other alternate servers, and so on. This continues until the NAS abandons the request. Through the silent discarding of messages the RADIUS protocol puts unnecessary burden on the NASes, as they have to send their pending requests to several alternate servers. With the exception of a few security related errors, the Diameter protocol requires that all messages be acknowledged, either with a successful response or one that contains an error code explaining the error. Through this the NAS knows that an error has occurred and doesn’t have to assume the server to be down and can correct the request making use of the alternate servers unnecessary.
4.3 Competition: Advantages/Disadvantages Diameter vs.

As mentioned in section two there are other AAA protocols used on the market today, other than RADIUS, like Kerberos and TACACS+, as well as other protocols considered possible to be used as AAA protocols in the future, like COPS, which Diameter has to compete with. In order to evaluate the different competitor protocols on the market the criteria’s stated in section 4.3.4 are going to be investigated. The criteria’s are constructed by Ki-Consulting to provide a comparison of the different protocols on the market. The protocols to be evaluated are:

- Kerberos
- TACACS+
- COPS
- Diameter

4.3.1 Kerberos

Kerberos is an authentication service developed as part of the ATHENA project at MIT. Kerberos is one of the earliest developed Authentication protocols and is also one of the most widely used Authentication protocol on the market today. Kerberos, named after the mythological three-headed dog that guards the gates of Hades, avoids sending passwords over a network where they may be sniffed by snoopers or captured by hackers, instead relying on encrypted messages from the user to a Kerberos security server. Once proper ID is established, Kerberos issues an encrypted ticket which the user can use to Authenticate himself to the server he wishes service from.
4.3.1.1 How Authentication is performed with Kerberos i.e. how it works

According to RFC1510 [16] the authentication process proceeds as follows: A client sends a request to the authentication server (AS) requesting “credentials” for a given server. The AS responds with these credentials, encrypted in the client's key. The credentials consist of:

- A “ticket” for the server and
- A temporary encryption key (often called a “session key”).

The client transmits the ticket (which contains the client's identity and a copy of the session key, all encrypted in the server's key) to the server. The session key (now shared by the client and server) is used to authenticate the client, and may optionally be used to authenticate the server (if mutual authentication is desired). The session key may also be used to encrypt further communication between the two parties or to exchange a separate sub-session key to be used to encrypt further communication.

4.3.2 TACACS+

TACACS (Terminal Access Controller Access Control System) is an industry standard protocol specification that forwards username and password information to a
centralized server. TACACS+ protocol is a new version of the TACACS protocol referenced by RFC 1492 [25]. TACACS+ is Cisco’s propriety security implementation of TACACS. It is a client/server protocol where a client (Network Access Server) sends a request, which is responded by the server (AAA server). The protocol is based on the TCP transport protocol. The overall design goal of TACACS+ has been to define a standard method for managing different Network Access Servers (NASes) from a single management server, such as a server in connection with a database.

TACACS+ improves on TACACS by separating the functions of Authentication, Authorization and Accounting and by encrypting all traffic between the NAS and the TACACS+ node. TACACS+ also allows for arbitrary length and content authentication exchanges which allow for any authentication mechanism to be used with TACACS+ clients. It is extensible to provide for site customization and future development features, and it uses TCP to ensure reliable delivery. The separation of authentication, authorization and accounting is a fundamental component of the design of TACACS+, but an implementation or configuration is not required to employ all three. TACACS+ overall function is similar to that of RADIUS but RADIUS has enjoyed a more widespread use since it is not a propriety of Cisco.

### 4.3.3 COPS

COPS (Common Open Policy Service) protocol is a query and response protocol stated in RFC 2748 and is a policy control protocol to be used as a link between a PDP (Policy Decision Point) and a PEP (Policy Enforcement Point) usually a NAS. Recently (read within the last two years) voices have been raised to propose the protocol AAA Working Group as a possible future AAA protocol.

The basic model of interaction between a policy server (PDP) and its clients (PEPs) is compatible with the policy framework document “Policy based admission control” RFC 2753.

![COPS Diagram](image-url)

**Figure 4.2: PDP-PEP interaction Specified by the COPS protocol.**
Figure 4.2 shows how COPS is used to transfer policy information between the PEP and a remote PDP, the figure also shows how a Local Policy Decision Point (LPDP) can be used by the PEP to make local policy decisions when the connection with the PDP is lost or absent for one reason or another.

4.3.4 Evaluation Criteria

In order to evaluate the different competitor protocols in the market the following criteria’s are going to be considered.

Functionality:

1. In which situations are the different protocols best used?
2. Do they work with firewalls?

Manageability:

3. Do keys need to be sent by mail or distributed in another trusted offline form?

Security:

4. Is just the Authentication info encrypted or is security for the entire message possible?
5. Is it simple to use this extra encryption?
6. What part of the protocol is “secure” in regards of usage?
7. What amount of effort is needed to “crack” the encryption?
8. What kind of encryption/security mechanism is supported?
9. What type of transport protocol is supported (UDP, TCP,…) and which ports are they working/supported on?

Market shares:

10. How / where do the protocols exist today?
11. Are they increasing or decreasing in market shares today?

Economy:

12. Is there any economical advantage or disadvantage to use the different protocols?
13. Do they support Real-time accounting?

4.3.5 Evaluation of the protocols according to 4.3.4

Functionality:

1. In which situations are the different protocols best used?
Kerberos: Kerberos v5 is today widely used as a plain Authentication protocol but it might be used in close connection with the other AAA protocols (TACACS+, RADIUS) as their Authentication mechanism.

RADIUS: RADIUS is best used as an AAA protocol in minor to medium size networks as it according to Ekstein [24] has congestion control problems. It doesn’t completely support the scalability requirements since only up to 256 outstanding requests can be handled at the same time, instead of tens of thousands simultaneous request between two communicating devices.

Diameter: Diameter is developed to be an AAA protocol used in anything from small to very large networks with the scalability in mind and $2^{32}$ different requests can be handled simultaneously. It also is backwards compatible with RADIUS which makes Diameter agents able to act as RADIUS gateways sending RADIUS messages through the network without any conversion needed.

COPS: COPS was developed to support different policy based services and is like Diameter made to be scaleable. The protocol was created for and is best used with general administration, configuration, and enforcement of policies, but with minor to medium work it can come into total compliance with the AAA requirements and is therefore suitable to perform AAA functions as well, all in accordance with RFC 2748 [18].

TACACS+: Like RADIUS TACACS+ is best used as an AAA protocol in minor to medium sized networks. The TACACS+ specifications says the protocol is scaleable to provision large networks but lately some complaints about this not being entirely true have been raised since the protocol in large networks have started to show degraded performance.

2. Do they work with firewalls?

A firewall friendly protocol is one which is designed to accommodate a firewall acting as a proxy according to RFC2989 [12]. This requirement, to be firewall friendly, stated by the Mobile-IP Working Group [19] for protocols to support Mobile-IP, permits a Home Agent AAA-server situated behind a firewall to be reachable from the Internet so it can provide AAA services to a Mobile-IP Foreign Agent. Another thing that could be accounted a firewall friendly protocol is that the protocol doesn’t make the firewall look into packet much beyond the application port number.

Kerberos: Since Kerberos runs on both UDP and TCP with fixed ports assigned by IANA and the Kerberos packets are easily recognised by a firewall (i.e. without thorough packet examination), Kerberos is considered to be firewall friendly.

RADIUS: RADIUS is according to Ekstein [24] known to be operational in environments where firewalls acting as proxies are active. RADIUS also runs
on a fixed port number assigned by IANA which helps the firewall and is on the market considered to be firewall friendly.

- **Diameter**: Diameter relies on SCTP, which is currently not supported on firewalls, and can therefore not be used with some firewalls. However a firewall could easily implement a Diameter proxy server, which would provide for firewall penetration, as an application proxy and it would probably be more secure than punching holes through the firewalls. In the future as SCTP gets more recognition on the market one can assume that firewall implementations will allow Streaming traffic to penetrate the firewalls. But with the ability for the Diameter protocol to accommodate firewalls acting as proxies and that Diameter packages are easily recognised and it could be considered firewall friendly [34].

- **COPS**: COPS runs over TCP and uses a fixed port number assigned by IANA, in addition, COPS proxy servers can easily be supported which is why it is considered firewall friendly. But on the other hand, depending on what it means to be firewall friendly, since COPS has other usage’s than AAA and uses the same port for every kind of message a firewall has to look deeply into the package to determine what kind of package it is, and this doesn’t comply to being firewall friendly [35].

- **TACACS+**: TACACS+ is known to be operational in environments where firewalls are acting as proxy. As RADIUS, TACACS+ also runs on a fixed port number assigned by IANA which helps the firewall and TACACS+ is, as RADIUS, therefore considered to be firewall friendly on the market.

**Manageability:**

3. Do keys need to be sent by mail or distributed in another trusted offline form?

- **Kerberos**: When using Kerberos to Authenticate a user against a server (any server) the user needs to have a shared secret with the TGS and this secret shouldn’t be passed over the Internet but instead be distributed in some trusted offline form. With a shared secret with the TGS the user never has to send a password over the Internet.

- **RADIUS**: The RADIUS protocol requires a shared secret to exist between the communicating client and server. This shared secret is required to pre-exist the communication attempt and thus needs to be transmitted in some secure offline form, so that it can’t be snoop off the Internet.

- **Diameter**: The Diameter protocol doesn’t require a shared secret between communicating peers and thus there is no need to distribute keys in any kind of offline form (for further explanation of reason se COPS below).

- **COPS**: The COPS protocol that, like Diameter, relies on CMS Objects to provide security doesn’t require a key to be distributed in any trusted offline form, since the use of CMS enables the communicating peers to exchange
secret keys through the Deffie-Hellman key exchange capabilities provided by the CMS support.

- **TACACS+:** The TACACS+ protocol requires that a shared secret exist in order to provide confidentiality. So in order to be able to provide any kind of confidentiality to the message a shared secret needs to exist between two peers. Without a shared secret no confidentiality can be provided so to achieve confidentiality one has to distribute keys in an offline secure form, to, like with RADIUS prevent key snooping on the Internet. But for messages that don’t require confidentiality, no offline key distribution is necessary.

**Security:**

4. **Is just the Authentication information encrypted or is security for the entire message possible?**

- **Kerberos:** The Kerberos protocol is usually just used to Authenticate a client/user to a network node. Kerberos is an Authentication protocol that doesn’t need to send the user password over the net, and through this the information sent to the Authentication server, in Kerberos case the TAGS (Ticket Granting Server), doesn’t encrypt the Authentication message to the TGS. Since the user password is never sent over the Ethernet every opportunity to sniff the net for passwords is removed.

- **RADIUS:** In the RADIUS protocol just the Authentication information is encrypted and the AVPs are in plain text according to RFC 2865 [1].

- **Diameter:** In Diameter all the AVPs can be protected through the use of the Cryptographic Message Syntax [37].

- **COPS:** In COPS all the objects can be protected through the use of the Cryptographic Message Syntax.

- **TACACS+:** According to Grant [28] the TACACS+ header (describes the remainder of the packet) of 12 bytes is always in plain text and the complete body of the packet may be encrypted.

5. **Is it simple to use this extra encryption?**

- **Kerberos:** While Kerberos is just an Authentication protocol there is no need for encryption beyond the Authentication part since there is no entire message other than the Authentication information.

- **RADIUS:** As stated above (see point 4) the RADIUS protocol only encrypts the authentication information with no possibility to encrypt the other AVPs, i.e. it is impossible to use any extra encryption.
- Diameter: In order for Diameter to be able to have end-to-end and hop-to-hop security the implementation of Diameter has to support the CMS Security application, if it does, it is easy to use the extra encryption otherwise you can not encrypt the AVPs or check integrity of the AVPs.

- COPS: The COPS protocol supports, according to Durham [35], the use of CMS objects and once the support is implemented it is easy to use the extra security CMS provides.

- TACACS+: In TACACS+ it is standard to use the encryption, i.e. it is simple, but it is still optional.

6. What part of the protocol is “secure” in regards of usage?

- Kerberos: As Kerberos is just an authentication protocol the only security it applies in usage is the encryption of the TGS ticket, encrypted with the receiver's key i.e. the requested service providers key, which the service provider receives from the requesting user.

- RADIUS: Just encryption of the Authentication information is possible.

- Diameter: Encryption of the entire message is possible.

- COPS: Encryption of the entire message is possible.

- TACACS+: Just encryption of the body of the message is possible.

7. What kind of encryption/security mechanism is supported?

- Kerberos: While the earlier version Kerberos v4 requires the use of DES (Data Encryption Standard) Kerberos v5 tags every cipher text with an encryption identifier so that any encryption technique may be used.

- Diameter: With the Diameter application CMS Security one can use several symmetric and asymmetric encryption algorithms to encrypt the Diameter AVPs. The mechanisms and algorithms supported when implementing Diameter with the CMS security application is presented in table 4.1 (below).
Table 4.1: The Mechanisms and Algorithms used with CMS objects

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hashing</td>
<td>Sha-1</td>
</tr>
<tr>
<td>Signature</td>
<td>Sha-1 in combination with RSA algorithm</td>
</tr>
<tr>
<td>Content Encryption</td>
<td>DES</td>
</tr>
<tr>
<td>Asymmetric Key Encryption</td>
<td>RSA algorithm</td>
</tr>
<tr>
<td>Symmetric Key Encryption</td>
<td>3DES</td>
</tr>
</tbody>
</table>

- **RADIUS**: According to RFC 2865 [1] and as stated above the RADIUS protocol just encrypts the authentication information. RADIUS does this by running the shared secret (between the NAS and the RADIUS server) followed by a Request Authenticator through a one way MD5\(^1\) hashing algorithm to create a 16 bytes digest value which is then XOR-ed byte-wise with the user-password. The encrypted password is then put in the user-password AVP which is sent with the Access-Request from the NAS to the RADIUS server in order to Authenticate the user.

- **COPS**: COPS like Diameter uses the Cryptographic Message Syntax [37] objects to provide Message integrity and confidentiality and the Encryption techniques used with the CMS is according to [35] the same as those with Diameter (see table 4.1 above).

- **TACACS+**: encrypts the body of a package with MD5, it does so by hashing the plain text in the packet header concatenated with a secret key to form a padding, which then is XOR-ed byte-wise with the packet body.

8. What amount of effort is needed to “crack” the encryption?

This section is mainly based on book Cryptography and Network Security by William Stallings [8], and below when referring to brute-force attacks one has to keep in mind that considerations only have been taken to today’s known methods.

- **Kerberos**: With the cipher text identifier used in the Kerberos protocol the effort to “crack” the encryption can be “unlimited” (i.e. computationally infeasible), depending on the chosen encryption technique. But Kerberos doesn’t specify how the user should choose his password and a password hack/attack is always possible, to prevent such (can’t be completely prevented

\(^1\)MD5 Message-Digest Algorithm RFC1321
but minimized) one has to be careful when choosing password. If a hacker gets hold of a user’s password he can gain access to tickets from the TGS arbitrary and can impersonate the user.

- **RADIUS**: Since RADIUS uses the MD5 algorithm to encrypt information the effort needed to “crack” the encryption is proportional to the strength of MD5. Rivest conjectures in the MD5 RFC that MD5 is as strong as a 128 bits hash can be, namely the difficulty of coming up with two messages having the same message digest is in the order of $2^{64}$ operations, where as the difficulty of finding a message with a given digest is on the order of $2^{128}$ operations. Lately though MD5 has been considered vulnerable to both cryptanalytic attacks as well as birthday (brute-force) attacks since it requires on the order of effort $2^{64}$ operations.

- **Diameter**: Since Diameter encrypts the information using the CMS security application it uses different encryption techniques and one of them is SHA-1 (Secure Hash Algorithm) which produces a 160 bits hash digest. Using brute-force technique, the difficulty of producing any message having a given message digest is on the order of $2^{160}$ operations for SHA-1 compared to $2^{128}$ for MD5, and the difficulty of producing two messages having the same message digest is on the order of $2^{80}$ for SHA-1 compared to $2^{64}$ for MD5. This makes SHA-1 a considerably stronger than MD5. SHA-1 is also as of today not vulnerable to cryptanalytic attacks which MD5 is.

- **COPS**: Since COPS, like Diameter (see Diameter above), uses the CMS format to encrypt the message it isn’t vulnerable to cryptanalytic attacks and thinking of brute-force attacks COPS also provides considerable stronger encryption compared to the protocols using MD5.

- **TACACS+**: Since TACACS+, like RADIUS (see RADIUS above), uses the MD5 as the encryption mechanism it is considered to be vulnerable to attacks and the effort to use Brute force attack needed to “crack” the encryption is of the order $2^{64}$ operations.

9. What type of transport protocol is supported (UDP, TCP, …) and which ports are they working/supported on?

The transport protocols and ports described below are all assigned and registered by IANA.

- **Kerberos**: Kerberos is according to RFC 1510 [16] supporting UDP as well as TCP on port 88 as transport protocols. Kerberos is also using port 464 with both TCP and UDP to change/set passwords.

- **RADIUS**: RADIUS supports UDP on port 1812 and RADIUS Accounting runs on port 1813 of UDP according to RFC 2865 [1].

- **Diameter**: The Diameter base protocol [4] is according to Calhoun [21] run on port TDB of both TCP and SCTP transport protocols. Today the protocol is
run in port 1812 in order to test interoperability until IANA assigns the Diameter protocol a port. The Diameter clients must support either of TCP and SCTP (might be mandated to use SCTP in the future) while agents and servers must support both.

- **COPS:** According to RFC 2748 [18] COPS uses a TCP connection between the PEP (responsible for initiating the connection) and a remote PDP, and at least one PDP implementation per server must listen on port 3288.

- **TACACS+:** According to RFC 1492 [25] TACACS+ runs on port 49 of TCP.

**Market shares:**

10. How / where do the protocols exist today?

- **Kerberos:** Kerberos is one of the earliest developed Authentication protocols and is also one of the most widely used Authentication protocols on the market today considered just as an Authentication protocol. Kerberos provides a centralised authentication server whose function is to authenticate users to servers and servers to users. Useful in cases the users and servers are just interested in knowing who they are dealing with, for instance in a company or a school the personnel/students once authenticated might be authorized to use whatever resources they want and no accounting or resource usage information is to be collected.

- **RADIUS:** Both RADIUS and TACACS+ are used by service providers all over the world. The protocols are today mainly used to support dial-in access and to handle access through other connection like xDSLs. But as new services like Voice over IP and QoS is used the need for new AAA protocols increases.

- **Diameter:** The Diameter protocol at the present just exists as a couple of drafts submitted to the AAA Work Group as to be proposed standard. There are also a couple of binary implementations of the protocol which can be found on the internet.

- **COPS:** The COPS protocol today exist as a policy provisioning protocol, but the use of COPS as a AAA protocol is nonexistent on the market today as it yet doesn’t provide full AAA functionality, and it to as Diameter above has been submitted as a proposed standard.

- **TACACS+:** Both RADIUS and TACACS+ are used by service providers all over the world. The protocols are today mainly used to support dial-in access and to handle access through other connection like xDSLs. But as new services like Voice over IP and QoS is used the need for new AAA protocols increases.
11. Are they increasing or decreasing in market shares today?

- **Kerberos:** As an Authentication protocol Kerberos is one of the most widely used protocols in the market today and as it looks today like it will continue as that. But with the introduction of the AAA protocols it has been losing weight in areas where more services than just Authentication is wanted, since they can provide a larger usage area.

- **RADIUS:** RADIUS is the largest and most widely used AAA protocol on the market today with the most users and developed implementations. For the most part its success depends on the easily managed implementations and that it has no propriety owner. As more and more service providers see the benefits of using an AAA protocol, RADIUS is increasing its market shares and usage around the world today. Almost every major remote-access vendor supports RADIUS today [23].

- **Diameter:** Since the Diameter protocol is still under development there aren’t any real fully working implementations out on the market but there exists a few free binary implementation which is downloadable on the Internet. Several major vendors do support the development and are implementing the Diameter protocol as it looks today (see section 4.4).

- **COPS:** As a policy provisioning protocol COPS is enjoying a wide spread recognition on the market and is rapidly increasing its market shares. As an AAA protocol COPS hasn’t received any real recognition yet but, it as Diameter, isn’t completely finished, and there are still fairly large amount of work to be done before it complies with the NASREQ requirements.

- **TACACS+:** The second most used AAA protocol today is TACACS+ and it, as RADIUS, benefits from the increasing AAA protocol usage on the market [33] and are increasing regarding usage around the world but TACACS+ is little by little losing market shares in favour of RADIUS. Mainly this is because many both larger and smaller companies are appealed by an open standard like RADIUS instead of having to rely on a single vendor with propriety rights to the protocol. Of major remote-access protocols only every third seems to support Cisco’s TACACS+, according to Networkcomputing [23].

**Economy:**

12. Is there any economical advantage or disadvantage to use the different protocols?

In order to evaluate if there is an economical advantage to use one protocols ahead of another different scenarios are to accounted for, like if you are using one of the protocols

- **Kerberos:** If one is just interested in Authentication Kerberos is probably in an economical advantage compared to the other protocols since it through its long existence and wide usage is well established and not too expensive compared
to the AAA implementations. The source code for several Kerberos implementations are free [14] but the possibility to buy a commercial Kerberos implementation so that you don’t have to build the source code and get help with configuration is also available at different prices but considerably cheaper than the other AAA protocols.

- **Diameter**: If one at the present aren’t using an AAA protocol and are using some kind of implementations that are providing AAA functions one might want to start using an AAA protocol in order to provide the AAA functions, and one might get an economical advantage by considering using Diameter straight away since it is extendible and the need for an upgrade can be avoided. If one is using one of the present ordinary AAA protocols, RADIUS or TACACS+, one has to think about what needs one has. If you aren’t in the need of an extendible protocol, or if the protocol you have works fine for the intended use and you don’t see any immediate change of ones usage areas of the protocol, like with the adaptation to Mobile IP or Voice over IP, it would be an economical disadvantage to upgrade to Diameter.

- **COPS**: Since COPS needs quite a bit of time and work to be done before it conforms to the NASREQ requirements, it’s an economical disaster to try to change to COPS from any other protocol now. But if you are in the need of an policy provisioning protocol and chooses to use COPS as provisioning protocol then it might be an economical advantage to use as AAA protocol when it complies to the NASREQ requirements, since you only need to have one protocol.

- **TACACS+**: One of the things that are positive with the use of TACACS+ is the ability to separate the different AAA functions. If one today uses TACACS+ and doesn’t need the functions of a Next generations AAA protocol, like Mobile IP functionality, it is an economical disadvantage to change to either RADIUS or Diameter. If one wants to be able to extend the uses of the AAA protocol Diameter might be the way to go.

13. **Do they support Real-time accounting?**

Real-time accounting involves the processing of information on resource usage within a defined time window; this time constraint is imposed in order to limit financial risks.

- **Kerberos**: No, according to RFC 1510 [16] (the Kerberos protocol isn’t supporting Accounting at all).

- **RADIUS**: Yes, according to the RADIUS accounting RFC 2866 [26].

- **Diameter**: Yes, according to the Diameter base protocol [21].

- **COPS**: Yes, according to RFC 2748 [18].

- **TACACS+**: Yes, according to the TACACS+ specification [28].
As the work with this thesis started and the lack of prior knowledge of the Diameter protocol and its competitor protocols the intention was to compare Diameter to Kerberos as well as the other above mentioned protocols but with the study of the different protocols the Kerberos protocol has shown not to be an generic AAA protocol but mainly just used as an Authentication protocol. Some implementations of the other protocols does allow for Kerberos to be used as authentication mechanism instead of the protocols built in Authentication mechanism.

4.4 Which vendors supports the Diameter protocol and how

Since the Diameter protocol has not yet reached standards status which would result in Diameter RFCs, no NAS are supporting the Diameter protocol. But several large companies do support the development of the Diameter protocol by funding several man years into the protocol development. By studying the different Diameter drafts the persons and companies working with the protocol can be identified. These vendors have people who are working with the DIAMETER protocol:

- Blackstorm Networks  Pat Calhoun
- Sun Microsystems       Eric Guttman
- Nortel Networks       Hasseb Aktar
- LM Ericsson            Jari Arkko
- Tut-systems            Allan C. Rubens
- Cisco systems          Glen Zorn
-               Jeff Haag
- Merit Network          William Bully
- Nokia Research Center  Charles E. Perkins
- Microsoft              Bernad Aboba

Aside from these companies another company called Interlink Networks are interested in the development of the Diameter protocol, and they have implemented the Diameter protocol according to the latest drafts in order to try to test it for interoperability.

4.4.1 Diameter test suite

Recently there was a third DIAMETER bakeoff, this time, hosted by LM Ericsson. The bakeoff was held in order for the different vendors to test their implementations of DIAMETER for interoperability and to test the different implementations support of the base protocol and the three applications NASREQ, Mobile IP and CMS Security.

There were five vendors attending the bakeoff out of 11 registered (probably because the September 11th incident in New York; the bakeoff was held shortly after) and the names of the companies other than LM Ericsson that attended the bakeoff has according to the LM Ericsson information centre been classified in order to protect the companies that still attended. The results of these interoperability tests showed that different vendors have come far in the implementation of the Diameter protocol and it also gave the developers of the Diameter protocol new tasks to work with in order to ensure that interoperability and functionality was working.
4.5 How Diameter can be implemented in Mobile-IP networks

As previously stated in section 3.3.3 the Mobile IP protocol works well when all mobile nodes belong to and are traversing within the same administrative domain. But if the Mobile IP protocol is used, according to its specification, in roaming networks it leads to scalability problems since the mobile IP protocol requires strong authentication (i.e. share a pre-existing security association) between the mobile node and its home agent. In roaming networks this requirement translates into the need for a security association between the Mobile Node and the foreign Agent and between the foreign agent and the home agent and between the Mobile Node and the Home agent (see figure 3.6). That scalability problems arise is obvious since this requires the Mobile Node to have a shared secret with every foreign agent it wants service from. The Mobile IP protocol specification also requires the mobile node to have a static home agent, in order to at least minimize the number of security associations (otherwise everyone of the numerous Foreign agents have to have multiple security associations with the home realm of the Mobile Node). With the use of Diameter the above problems are solved.

In order to allow the scaling of wireless data access across administrative domains, it is necessary to minimize the security associations required. By applying the Diameter AAA services to this Mobile IP model the number of security associations needed by each Mobile Node (previously unlimited) is reduced to only one, by requiring the Mobile Node just to have a security association with its home AAA server (this also allows for the home agent to be dynamically assigned by the home Diameter server since there is no pre-existing shared secret between the home agent and the mobile node. Then by using the roaming capabilities of the Diameter protocol, the home Diameter server(AAAH) can communicate with foreign(in another administrative
domain) Diameter servers (AAAFs). Through the required security association between the AAAH and the Mobile Node, keys for each security association (associations according to figure 3.6) can be created. The keys destined for the foreign and home agent are propagated to their nodes via the Diameter protocol, while the key destined for the Mobile Node is sent via the Mobile-IP protocol, and this result in the integrated Mobile IP/Diameter architecture shown in figure 3.7(below).

![Diagram of Mobile IP/Diameter architecture]

Figure 4.4: Wireless IP Architecture for an integrated Mobile-IP/Diameter Network

In an integrated Mobile-IP/Diameter Network (see Figure 4.4), it is assumed that each Foreign Agent (FA) shares a security association between itself and its local Diameter server (AAAF). Further, the Home and Local Diameter servers both share a security association with the broker's Diameter server. All this allows the Mobile Node to roam throughout different administrative domains and still have strong Authentication with the home agent, which is required in order for the Mobile Node to use the Mobile IP protocol. Once the session keys have been established and propagated, the mobility devices can exchange registration information directly without the need of the Diameter infrastructure. However the session keys have a lifetime, after which the Diameter infrastructure again must be used in order to acquire new session keys.

The interaction between Mobile IP and Diameter/AAA provides:

- better scaling of security associations
- mobility across administrative domain boundaries (roaming)
- dynamic home agent assignment (now it’s optional)
4.5.1 The message flow of integrated Mobile IP/Diameter networks

(when a Mobile Node get access to network resources through Mobile IP)

This section describes how the Diameter protocol is used in order for a Mobile Node to get access to network resources through the Mobile IP protocol all according to figure 3.7.

When a Mobile Node appears within a local network it issues a registration request to the Foreign Agent. Since the Foreign Agent does not share any security association with the Mobile Node’s Home Agent, it sends a Diameter AA-Mobile-Node-Request (AMR) to its local Diameter server, and includes the authentication information (MN-AA) and the Mobile-IP registration request. There are two reasons why the Mobile Node has to send a request to the Foreign Agent and not directly to the home Diameter server:

1. It doesn’t have access to the network. The registration request is sent by the Mobile Node to request access to the network.
2. The Mobile Node may not have an IP address, and may be requesting that one be assigned to it by its home provider.

The Local Diameter Server determines whether the request can be satisfied locally through the use of the Network Access Identifier (NAI) an example: user@realm provided by the Mobile Node, the Diameter Server uses the realm portion of the NAI to identify the Mobile Node’s home Diameter Server and forwards the message if unable to process it locally.

When the home Diameter Server receives the AMR, it authenticates the user and begins the authorization phase. The authorization phase includes the generation of session keys to be distributed to the AAAF, FA, HA and Mobile Node. The keys destined for the foreign and home agent are propagated to the mobility nodes via the Diameter protocol, while the keys destined for the Mobile Node are sent via the Mobile-IP protocol.

Once authorization is complete, the home Diameter Server issues an unsolicited Diameter request a Home-Agent-MIP-Request (HAR), to the Home Agent, which includes the information in the original Diameter request as well as the authorization information generated by the home Diameter server (including the security association keys). For new sessions, the AAAH must create an accounting session identifier, which is added to the Accounting-Multi-Session-Id AVP in the HAR message sent to the home agent. During the creation of the HAR, the AAAH uses a different session identifier than the one used in the AMR/AMA (see figure 3.8).
Figure 4.5: Mobile IP/Diameter Message Exchange

The AAAH uses the same session identifier for all HARs initiated on behalf of a given mobile node’s session. A mobile node's session is identified via its identity in the User-Name AVP, the MIP-Mobile-Node-Address and MIP-Home-Agent-Address AVPs.

The Home Agent retrieves the Registration Request from the Diameter request and processes it (assigns an IP address), then generates a Registration Reply that is sent back to the home Diameter server in a Diameter Home-Agent-MIP-ANSWER (HAA). The Accounting-Multi-Session-Id AVP in the HAR must be included in the HAA, which is then forwarded to the AAAH.

Upon receipt of the HAA, the AAAH creates the AA-Mobile-Node-Answer (AMA) message, includes the Accounting-Multi-Session-Id that was present in the HAA, and the MIP-Home-Agent-Address, MIP-Mobile-Node-Address AVPs in the AMA message. The message is sent to the Local Server, through the proxy if one was used, and finally to the Foreign Agent (see figure 3.7)
5 Conclusions

In this section of the thesis conclusions are going to be drawn from every section in chapter four thus answering the questions stated in the problem specification (section 1.3). Then final conclusions are going to be formulated based on conclusions from every chapter and the insight the writer of this thesis have gained.

That RADIUS today by far is the largest AAA protocol on the market tells us that in order for easy migration, the Next Generations AAA protocol needs to have RADIUS capabilities, which Diameter does. Also since RADIUS is the most widely used AAA protocol, Diameter extends the Authorization capabilities through its peer-to-peer connection as the server can send unsolicited requests, as an example requesting a private key-code in order to allow different services. Diameter also enhances the previously limited proxy capabilities of RADIUS thus allowing secure roaming. The users finding RADIUS unable to cope with their mobile work habits will thrive at the ease Diameter solves this. Through the 32-bit AVP address space and the more powerful attribute value pairs Diameter is able to serve mobile non-dialup users.

There is no way to say for sure that Diameter is going to be the next Generation AAA protocol from the comparison to COPS in section 4.3 but with everything stated above together with the fact that the Diameter protocol is further developed than COPS gives it an advantage over COPS.

It is my opinion that COPS will be completely developed though but not usually used as an AAA protocol but rather coexist with Diameter since they are developed for different purposes and at COPS original intended use as an policy protocol it is superior to Diameter. This and the fact that COPS doesn’t provide any direct RADIUS backwards capabilities which makes it hard for it to take market shares since people using the today domination RADIUS protocol cannot migrate in any easy way speaks in favour of the Diameter protocol as being the Next Generations AAA protocol.

The Kerberos protocol isn’t a likely competitor to the Diameter protocol as it is generally just used to provide Authentication and not fulfilling the consensus of AAA. Since the Kerberos protocol is widely used today and quite successful as an Authentication protocol I believe that Diameter probably, in the near future, will be able to integrate Kerberos as one of its possible Authentication methods.

As TACACS+ suffers from congestion problems in larger environments, as it requires a shared secret existing between TACACS+ servers and clients, the Diameter protocol gets a huge leap ahead of it. A couple of other things that I think is speaking for the Diameter protocol as a successor protocol to TACACS+, is that compared to Diameter it provides poor security and that TACACS+ still is a propriety protocol of Cisco, keeping in mind that people using AAA protocol has shown to head towards open standards. Lastly the lack of RADIUS capabilities within the TACACS+ protocol also speaks for Diameter as next generation AAA protocol as RADIUS today is by far the most used protocol and is increasing its market shares.

Since the large numbers of vendors of great size are supporting the development of Diameter, I think it is safe to draw the conclusions that Diameter is going to get broad acceptance on the market as the Next Generations AAA protocol. And since the large
vendors have been testing the interoperability of their implementations according to the Diameter drafts. Diameter is well on the right track to be finished as drafts and becoming a standard.

Another thing Diameter has going for it is that it can be closely integrated with the Mobile IP protocol extending the Mobile IP protocol to allow it to be used in roaming networks which is a must in the near wireless future.

Final conclusion:

From the above conclusions together with my intuition gained from literature studies of the papers in the reference list I draw the conclusion that the Diameter protocol is going to be most widely used AAA protocol of the Next Generation on the market. Although I believe the Diameter protocol going to be the greatest AAA protocol on the market I think it will start out slowly with just really large ISPs and smaller companies specialising in new Internet services, being in need of the services Diameter can provide that today’s AAA protocol cannot. This since companies satisfied with their solutions today not striving forward in the Internet development, will not take on the administrative burden and expenses that come with a new protocol but rather just keep going on with their solutions of today as long as they can before time and demands catch up with them.
6 References


[26] C. Rigney, "RADIUS Accounting" RFC 2866, June 2000,


[33] URL:http://ing.ctit.utwente.nl/WU5/D5.1/Technology/tacacs+/ (2001-08-08)


På svenska

Detta dokument hålls tillgängligt på Internet – eller dess framtida ersättare – under en längre tid från publiceringsdatum under förutsättning att inga extra-ordinära omständigheter uppstår.

Tillgång till dokumentet innebär tillstånd för var och en att läsa, ladda ner, skriva ut enstaka kopior för enskilt bruk och att använda det oförändrat för ickekommersiell forskning och för undervisning. Överföring av upphovsrätten vid en senare tidpunkt kan inte upphäva detta tillstånd. All annan användning av dokumentet kräver upphovsmannens medgivande. För att garantera äktheten, säkerheten och tillgängligheten finns det lösningar av teknisk och administrativ art.

Upphovsmannens ideella rätt innefattar rätt att bli nämnd som upphovsman i den omfattning som god sed kräver vid användning av dokumentet på ovan beskrivna sätt samt skydd mot att dokumentet ändras eller presenteras i sådan form eller i sådant sammanhang som är kränkande för upphovsmannens litterära eller konstnärliga anseende eller egenart.

För ytterligare information om Linköping University Electronic Press se förlagets hemsida http://www.ep.liu.se/

In English

The publishers will keep this document online on the Internet - or its possible replacement - for a considerable time from the date of publication barring exceptional circumstances.

The online availability of the document implies a permanent permission for anyone to read, to download, to print out single copies for your own use and to use it unchanged for any non-commercial research and educational purpose. Subsequent transfers of copyright cannot revoke this permission. All other uses of the document are conditional on the consent of the copyright owner. The publisher has taken technical and administrative measures to assure authenticity, security and accessibility.

According to intellectual property law the author has the right to be mentioned when his/her work is accessed as described above and to be protected against infringement.

For additional information about the Linköping University Electronic Press and its procedures for publication and for assurance of document integrity, please refer to its WWW home page: http://www.ep.liu.se/

© Håkan Ventura