INTERNET DRAFT
Category: Informational
Title: draft-calhoun-aaa-diameter-comp-00.txt
Date: April 2000

Pat R. Calhoun
Sun Microsystems, Inc.

Comparison of DIAMETER Against AAA Network Access Requirements

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Abstract

The AAA Working Group has completed a document that itemizes their requirements for Network Access Applications (NASREQ, Mobile IP, and ROAMOPS). This specification compares the DIAMETER protocol against the requirements, and is provided to the AAA Working Group as an official submission for an AAA protocol.

1.0 Introduction

The AAA Working Group has completed a document that itemizes their requirements for Network Access Applications (NASREQ, Mobile IP, and ROAMOPS). This specification compares the DIAMETER protocol against the requirements, and is provided to the AAA Working Group as an official submission for an AAA protocol.

1.1 Requirements language

In this document, the key words "MAY", "MUST, "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [1].

Please note that the requirements specified in this document are to be used in evaluating AAA protocol submissions. As such, the requirements language refers to capabilities of these protocols; the protocol documents will specify whether these features are required, recommended, or optional. For example, requiring that a protocol support confidentiality is NOT the same thing as requiring that all protocol traffic be encrypted.

A protocol submission is not compliant if it fails to satisfy one or more of the MUST or MUST NOT requirements for the capabilities that it implements. A protocol submission that satisfies all the MUST, MUST NOT, SHOULD and SHOULD NOT requirements for its capabilities is said to be "unconditionally compliant"; one that satisfies all the MUST and MUST NOT requirements but not all the SHOULD or SHOULD NOT requirements for its protocols is said to be "conditionally compliant."

2.0 Requirements Summary

This section contains the same four sections as found in the AAA Network Access requirements. Each section contains a new column, named DIAMETER. For each requirement, it is noted whether the DIAMETER protocol meets (T), Partially meets (P), or does not meet (F) the stated requirement. Furthermore, each requirement has a footnote, which contains additional justification.

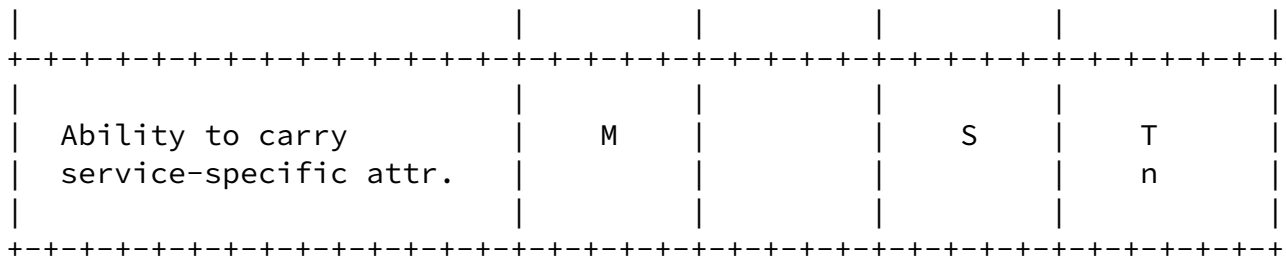
2.1 General requirements

These requirements apply to all aspects of AAA and thus are considered general requirements.

General Reqts.	NASREQ	ROAMOPS	MOBILE IP	DIAMETER
Scalability	M	M	M	Ta
Failover	M		M	Tb
Mutual auth AAA client/server	M		M	Tc
Transmission level security		M	S	Td
Data object Confidentiality	M	M	S	Te

Data object Integrity	M	M	M	T f
Certificate transport	M		S	T g

Reliable AAA transport mechanism	M		M	T h
Run Over IPv4	M	M	M	T i
Run Over IPv6	M		S	T j
Support Proxy and Routing Brokers	M		M	T k
Auditability	S			T l
Shared secret not required	S	O	O/M	T m



Ability to carry service-specific attr.	M		S	T n

Key
M = MUST
S = SHOULD
O = MAY
N = MUST NOT
B = SHOULD NOT

T = Meets Requirement
P = Partly Meets Requirement
F = Does Not Meet Requirement

Clarifications

[a] The DIAMETER Base Protocol [3] has learned from RADIUS' deficiencies and provides the following features that help scaling:

[1] Supports 2^32 pending requests

[2] reduces the number of servers necessary in a proxy environment, while increasing the robustness of the proxy chain

[3] does not require end-to-end application level acknowledgement

[4] support for message forwarding and redirect servers

[b] All DIAMETER messages are routed based on the realm portion of the Network Access Identifier (NAI) [10]. The DIAMETER Base Protocol [3] states that when a node receives a disconnect indication from a peer, all unacknowledged messages (at the transport layer) MUST be forwarded to an alternative server that is capable of handling the realm in question. Unlike the RADIUS protocol, the Destination-NAI AVP allows a DIAMETER response to fol-

low a path that differs from the requests, which allows for a more resilient service.

[c] The DIAMETER Base Protocol [3] defines three different authentication mechanisms:

[1] None - Used when an underlying security service is used, such as IP Security.

[2] Hop-by-Hop - The DIAMETER Base Protocol [3] defines message authentication, using symmetric transforms, which is used to provide mutual authentication between two DIAMETER nodes.

[3] End-to-End - Although not necessarily intended to provide message authentication, the Strong Security extension [6] provides object level authentication, which could cover all AVPs in a DIAMETER message. Given the fairly intensive computations necessary to generate an end-to-end objects, use of this authentication mechanisms to should be restricted to cases where strong authentication (e.g. Digital Signatures) are necessary (e.g. Internet-Domain).

[d] The DIAMETER Base Protocol [3] provides message authentication, integrity and confidentiality using hop-by-hop security.

[e] The DIAMETER Strong Security extension [6] defines the CMS-Data AVP, which is used to carry Cryptographic Message Syntax (CMS) [11] objects. The objects, as defined in [11], MAY be encrypted using asymmetric encryption, where only the target host would be able to retrieve the plaintext.

[f] The DIAMETER Strong Security extension defines the CMS-Data AVP, which is used to carry Cryptographic Message Syntax (CMS) [11] objects. The objects, as defined in [11], MAY be authenticated using different levels of authentication transforms, including asymmetric.

[g] The DIAMETER Strong Security extension defines the CMS-Data AVP, which is used to carry Cryptographic Message Syntax (CMS) [11] objects. The objects, as defined in [11], MAY be used to carry

X.509 certificates.

[h] The DIAMETER Base Protocol [3] is run over the Simple Control Transport Protocol (SCTP) [12], which provides reliability, quick failure detection, and addresses the AAA requirements.

[i] The DIAMETER Base Protocol [3] has no reliance on the underlying IP version, and is capable of including IP version 4 addresses.

[j] The DIAMETER Base Protocol [3] has no reliance on the underlying IP version, and is capable of including IP version 6 addresses.

[k] The DIAMETER Base Protocol [3] supports proxies and brokers in both transparent forwarding, as well as in the redirect mode. The former allows a server to simply forward a DIAMETER message to a downstream server. The latter allows a server to provide NAI-to-Address services, by returning information necessary for a server to directly communicate with another DIAMETER server handling a particular domain.

[l] The CMS-Data AVP [6] allows each DIAMETER entity in a proxy chain to add its identity, and signature in a serial fashion, which MAY be used to trace a DIAMETER message's path.

[m] The DIAMETER Base Protocol [3] does provide for no message authentication, which is normally used when an underlying security service is used, such as IP Security.

[n] The DIAMETER Base Protocol [3] is extensible, and allows third parties to create service-specific extensions, such as the Mobile IP [5] and NASREQ [8] extensions. Future extensions could be added, by allocating an Extension Identifier [3], and the AVP Values necessary for the objects needed, by IANA.

2.2 Authentication Requirements

Authentication Reqts.	NASREQ	ROAMOPS	MOBILE IP	DIAMETER

NAI Support	M	M	S	Ta
CHAP Support	M	M	O	Tb
EAP Support	M	S	O	Tc
PAP/Clear-Text Support	M	B	O	Td
Re-authentication on demand	M		S	Te
Authorization Only without Authentication	M		O	Tf

Key
M = MUST
S = SHOULD
O = MAY
N = MUST NOT
B = SHOULD NOT

T = Meets Requirement
P = Partly Meets Requirement

F = Does Not Meet Requirement

Clarifications

[a] The DIAMETER Base Protocol [3] defines an AVP that is used to carry a User-Name, which SHOULD be in an NAI format. Furthermore, [3] defines how DIAMETER message forwarding is performed using the realm portion of the NAI.

[b] The DIAMETER NASREQ extension [8] defines the AVPs necessary to request authentication of a PPP user using the CHAP authentication mechanism.

[c] The DIAMETER NASREQ extension [8] defines the AVPs necessary to carry Extensible Authentication Protocol (EAP) payloads, and defines a set of primitives to be used with the AVPs.

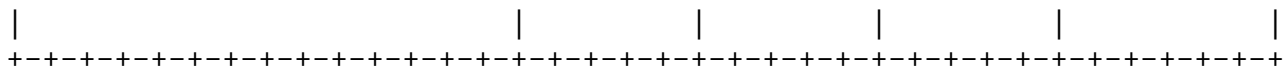
[d] The DIAMETER NASREQ extension [8] defines the AVPs necessary to request authentication of a PPP user using the PAP authentication mechanism.

[e] The DIAMETER Base Protocol [3] specifies that an authenticated user's session SHOULD expire in the number of seconds specified in the Session-Timeout AVP. In order to renew a session, a re-authentication MUST be submitted. Re-authentication MAY occur at any time before the timeout expires.

[f] The DIAMETER NASREQ extension [8] states "Unlike the RADIUS protocol the DIAMETER protocol does not require authentication information to be contained in a request from the client. Therefore, it is possible to send a request for authorization only. The type of service depends upon the Request-Type AVP. This difference MAY cause operational issues in environments that need RADIUS interoperability, and it MAY be necessary that protocol conversion gateways add some authentication information when transmitting to a RADIUS server."

2.2 Authorization Requirements

Authorization Reqts.	NASREQ	ROAMOPS	MOBILE IP	DIAMETER
Static and Dynamic IPv4/6 Address Assign.	M	M	M	T a
RADIUS gateway capability	M	M	O	T b
Reject capability	M	M	M	T c
Precludes layer 2 tunneling	N	N		T d
Re-Authorization on demand	M		S	T e
Support for Access Rules, Restrictions, Filters	M		O	T f
State Reconciliation	M			T g
Unsolicited Disconnect	M			T h



Key
M = MUST
S = SHOULD
O = MAY
N = MUST NOT
B = SHOULD NOT

T = Meets Requirement
P = Partly Meets Requirement
F = Does Not Meet Requirement

Clarifications

[a] The DIAMETER NASREQ [8] and Mobile IP [5] extensions allows for both static and dynamic address assignment. The DIAMETER Base Protocol [3] allows AVPs of format "Address" to carry either IP version 4 or 6 addresses.

[b] The DIAMETER protocol provides many features that makes the task simpler for an AAA protocol bridge function. First, the protocol reserves the first 256 Commands and AVPs to "Legacy" RADIUS. The RADIUS attributes are defined in the NASREQ extension [8]. Further, the Implementation Guideline [9] specification provides guidelines that MAY be followed when implementing a protocol bridge, which would ensure complete protocol compatibility.

[c] A forwarding agent, be it a Proxy or Broker, MAY reject a request by responding with a response, and the appropriate Result Code. The identity of the rejecting host is known through the Host-Name AVP [3].

[d] The DIAMETER NASREQ Extension [8] defines a set of AVPs that are used to create compulsory tunnels, including Layer 2 tunnels.

[e] The DIAMETER Base Protocol [3] specifies that an authorized user's session SHOULD expire in the number of seconds specified in the Session-Timeout AVP. In order to renew a session, a re-authorization MUST be submitted. Note that re-authorization MAY occur at any time before the timeout occurs.

[f] The NASREQ Extension [8] specifies two methods of supporting Filters and Access Rules. The first, is defined for Legacy RADIUS compatibility, and allows a Filter Identifier to be carried within an AVP. It is necessary for the NAS in question to recognize the Identifier provided, and map the appropriate filter rules to the user's access port. The second method is a much more scalable solution, and allows filters to be encoded in a standard AVP. Note that the RADIUS protocol has no equivalent

attribute, so use of this AVP SHOULD be reserved for networks that do not include RADIUS-only devices.

[g] The AAA network access requirements describe State Reconciliation as requiring:

[1] Re-authorization capabilities - The DIAMETER Base Protocol [3] provides the Session-Timeout AVP, which is used to inform the NAS of the lifetime of a successful authorization. The protocol states that the NAS MUST send a re-authorization in order to extend the life of the session. Re-authorization is service-specific, and is defined in Mobile IP [5] and NASREQ [8].

[2] Session disconnect message - The DIAMETER Base Protocol [3] defines the Session-Termination-Request message, which is used by the NAS to inform the AAA server that an active session has been terminated.

[3] Transport and application-layer reliability - The DIAMETER Base Protocol [3] requires the use of SCTP [13] as the reliable transport. Furthermore, the DIAMETER base protocol [3] defines what a node does in the event of a peer failure, in order to provide application level reliability.

[4] An interim message - The DIAMETER Accounting extension [4] defines the Accounting-Interim-Interval AVP, which is used by DIAMETER nodes to inform their peer of the expected interval between interim Accounting messages.

[5] A mechanism for the AAA server to retrieve state information from the NAS. This mechanism will provide timely

information though a complete state dump may not be immediately available. - The DIAMETER Resource Management extension [15] provides a message set that allows a DIAMETER node to request active session state information from its peer.

[6] A NAS reboot message - The DIAMETER Base Protocol [3] defines the Device-Reboot-Ind, which is used to communicate to a peer of a reboot.

[7] Accounting On/Off messages - The DIAMETER Accounting extension [4] defines the Accounting-Status-Ind message, which is used to communicate to a peer whether accounting has been enabled or disabled.

[h] The DIAMETER Base Protocol [3] supports a set of Session

Termination messages. A client (NAS) uses the messages to inform its server that an active session is being terminated. A server uses the messages to request that the client terminate the session. A session is identified through the Session-Id, which is guaranteed to be globally unique.

2.3 Accounting Requirements

Accounting Reqts.	NASREQ	ROAMOPS	MOBILE IP	DIAMETER
Real-time accounting	M	M	M	Ta
Mandatory Compact Encoding		M	M	Tb

Accounting Record Extensibility	M	M	M	T c
Batch Accounting	S			T d
Guaranteed Delivery	M		M	T e
Accounting Time Stamps	M		S	T f
Dynamic Accounting	M		S	T g

Key
M = MUST
S = SHOULD
O = MAY

N = MUST NOT
B = SHOULD NOT

T = Meets Requirement
P = Partly Meets Requirement
F = Does Not Meet Requirement

Clarifications

[a] The DIAMETER Accounting extension [4] allows for both Real-Time and batched accounting record transfer. The default mode is

real-time.

[b] The DIAMETER Accounting extension [4] defines the ADIF-Record AVP, which is used to carry ADIF [13] records. The AAA Accounting Record and Attributes [14] specification states "[ROAM-ADIF] proposes a standard accounting record format, the Accounting Data Interchange Format (ADIF), which is designed to compactly represent accounting data in a protocol-independent manner."

[c] The ADIF [13] Accounting Data Format MAY be extended by assigning new keywords for new accounting data objects by IANA.

[d] The DIAMETER Accounting extension [4] allows for both Real-Time and batched accounting record transfer. When batched mode is desired, information on the frequency that records should be provided (both in terms of time and bandwidth) is provided in a set of defined AVPs.

[e] The DIAMETER server that is responsible for a specific realm MUST acknowledge, at the application level, all Accounting Requests. This allows the sender to have an acknowledgement, which MAY be signed, of receipt and acceptance of one or more Accounting Records.

[f] The DIAMETER Base Protocol [3] defines the Timestamp AVP, which MUST be present in all Accounting [4] messages.

[g] The DIAMETER Accounting extension [4] allows for "interim" accounting records, which MAY be sent periodically, and after a re-authentication and/or re-authorization.

2.4 Unique Mobile IP requirements

In addition Mobile IP also has the following requirements:

Unique Mobile IP requirements	NASREQ	ROAMOPS	MOBILE IP	DIAMETER
Encoding of Mobile IP registration messages			M	T a
Firewall friendly			M	T b
Allocation of local Home agent			S/M	T c

Key
M = MUST
S = SHOULD
O = MAY
N = MUST NOT
B = SHOULD NOT

T = Meets Requirement
P = Partly Meets Requirement
F = Does Not Meet Requirement

Clarifications

[a] The DIAMETER Mobile IP extension [5] defines the MIP-Registration-Req and the MIP-Registration-Reply AVPs, which are used to carry the Mobile IP Registration Requests as opaque data.

[b] The DIAMETER Base Protocol [3] relies on SCTP, which is currently not supported on firewalls, and therefore could not be used with some firewalls. Furthermore, most NAT implementations DO NOT support SCTP either. However, a firewall could easily

implement a DIAMETER proxy server, which would provide for firewall penetration, as an application proxy and would probably be more secure than punching holes through firewalls. It is assumed that future firewall implementations will recognize the SCTP protocol, and will allow such traffic to penetrate the firewall.

[c] The DIAMETER Mobile IP extension [5] specifies how a Home Agent within a foreign network could be allocated, and defines the message flow as well as how the Key Distribution Center (KDC) session keys are used in such a network.

3.0 Conclusion

The DIAMETER Base Protocol [3], and associated extensions [4, 5, 6, 8, 15] is unconditionally compliant with the AAA Network Access requirements [2].

4.0 References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] Aboba et al, "Network Access AAA Evaluation Criteria", IETF work in progress, draft-ietf-aaa-na-reqts-02.txt, March 2000.

[3] P. Calhoun, A. Rubens, H. Akhtar, E. Guttman, "DIAMETER Base Protocol", draft-calhoun-diameter-14.txt, IETF work in progress, April 2000.

[4] J. Arkko, P. Calhoun, P. Patel, G. Zorn, "DIAMETER Accounting Extension", draft-calhoun-diameter-accounting-05.txt, IETF work in progress, April 2000.

[5] P. Calhoun, C. Perkins, "DIAMETER Mobile IP Extensions", draft-calhoun-diameter-mobileip-07.txt, IETF work in progress, April 2000.

[6] P. Calhoun, W. Bulley, S. Farrell, "DIAMETER Strong Security Extension", draft-calhoun-diameter-strong-crypto-03.txt, IETF work in progress, April 2000.

[7] P. Calhoun, G. Zorn, P. Pan, H. Akhtar, "DIAMETER Framework", draft-calhoun-diameter-framework-07.txt, IETF work in progress, April 2000

[8] P. Calhoun, W. Bulley, "DIAMETER NASREQ Extension", draft-calhoun-diameter-nasreq-03.txt, IETF work in progress, April 2000.

[9] P. Calhoun, A. Rubens, H. Akhtar, E. Guttman, W. Bulley, J. Haag, "DIAMETER Implementation Guidelines", draft-calhoun-diameter-impl-guide-02.txt, IETF work in progress, April 2000

[10] B. Aboba, M. Beadles "The Network Access Identifier." RFC 2486. January 1999.

[11] R. Housley, "Cryptographic Message Syntax", RFC 2630, June 1999.

[12] R. Stewart et al., "Simple Control Transmission Protocol", draft-ietf-sigtran-sctp-08.txt, IETF Work in Progress, April 2000.

[13] B. Aboba, D. Lidyard, "The Accounting Data Interchange Format (ADIF)", IETF Work in Progress, draft-ietf-roamops-actng-07.txt, September 1999.

[14] N. Brownlee, A. Blount, "Accounting Attributes and Record Formats", IETF Work in Progress, draft-ietf-aaa-accounting-attributes-02.txt, March 2000.

[15] P. Calhoun, N. Greene, "DIAMETER Resource Management", draft-calhoun-diameter-res-mgmt-03.txt, IETF Work in Progress, April 2000.

5.0 Security Considerations

This document, being a protocol evaluation document, does not have any security concerns. The security requirements on protocols to be evaluated using this document are described in the referenced documents.

6.0 IANA Considerations

This draft does not create any new number spaces for IANA administration.

7.0 Acknowledgements

Thanks to the various co-authors of the DIAMETER documents, which have been very helpful in getting the protocol in the state that it

is today. The author would also like to thank the active DIAMETER mailing list members, and some IESG members, for their valuable input.

8.0 Authors Addresses

Pat R. Calhoun
Network and Security Research Center, Sun Labs
Sun Microsystems, Inc.
15 Network Circle
Menlo Park, CA 94025

Phone: +1 650 786-7733
EMail: pcalhoun@eng.sun.com

9.0 Full Copyright Statement