Network Working Group
Request for Comments: 3127
Category: Informational

D. Mitton
Nortel Networks
M. St.Johns
Rainmaker Technologies
S. Barkley
UUNET
D. Nelson
Enterasys Networks
B. Patil
Nokia
M. Stevens
Ellacoya Networks
B. Wolff
Databus Inc.
June 2001

Authentication, Authorization, and Accounting: Protocol Evaluation

Status of this Memo

Copyright Notice

Abstract

This memo represents the process and findings of the Authentication, Authorization, and Accounting Working Group (AAA WG) panel evaluating protocols proposed against the AAA Network Access Requirements, RFC 2989. Due to time constraints of this report, this document is not as fully polished as it might have been desired. But it remains mostly in this state to document the results as presented.

Table of Contents

1. Process Description

Due to time constraints, the original draft of this document was rushed to meet the publication deadline of the June 2000 Pittsburgh meeting. Since the meeting has passed, we do not wish to substantially revise the findings within this document, so that we don't give the appearance of changing information after the presentation. Only additional descriptions of the process, formatting, layout editing and errors of fact have been corrected in subsequent revisions.

1.1. WG Co-Chair's Note:

After the AAA WG re-charter was approved, and the Network Access Requirements document passed AAA WG Last Call, a Solicitation of Protocol Submissions was issued on 4/13/2000. The Solicitation was sent to the AAA WG mailing list, as well as to other IETF WG mailing lists related to AAA, including NASREQ, Mobile IP, RAP, and SNMPv3.

Submissions were solicited effective immediately. Authors of candidate protocols were requested to notify the AAA WG chairs of their intent to submit a candidate protocol. It was suggested that this notification be sent by May 1, 2000.

Protocol submissions and compliance description documents were to be submitted in Internet Draft format by email to internet-drafts@ietf.org. The deadline for submissions was June 1, 2000. To be considered as a candidate, submissions needed to include an unqualified RFC 2026 statement, as described at: http://www.ietf.org/Sec10.txt

In order to assist the AAA WG in evaluating the protocol submissions and compliance description documents, the AAA WG chairs then formed an evaluation team, which was announced on May 20, 2000. The job of the team was be to put together an Internet Draft documenting their evaluation of the protocol submissions. The goal is to have a first draft available prior to the July 14, 2000 submission deadline for IETF 48.

In composing the evaluation draft, the evaluation team was asked to draw from the protocol specifications, the compliance descriptions, and other relevant documents, the Network Access Requirements document, RFC 2989.

Mike St. Johns was asked to chair the evaluation team. The chairs of WGs related to AAA were also invited to join the team. These included Dave Mitton, co-chair of NASREQ WG, Basavaraj Patil, co-chair of Mobile IP WG, and Mark Stevens, co-chair of the RAP WG.

Additional members of the evaluation team were chosen to represent the interests of network operators as well as developers of AAA client and server software.

As usual, the IESG advised the evaluation team. IESG advisors included Randy Bush and Bert Wijnen, Directors of the Operations and Management Area.

1.2. Chairman's Note:

This document is the result of 6 weeks of intense work by the panel listed below. Our mission was to evaluate the various AAA proposals and provide recommendations to the AAA working group and to the IESG on the viability of each of the proposals.

The evaluation process had three distinct phases. 1) Validate the AAA requirements document [AAAReqts] against the base requirements documents for NASREQ, MOBILEIP and ROAMOPS. 2) Evaluate each of the SNMP, Radius++, Diameter and COPS proposal claims against the validated requirements. 3) Provide final recommendations based on side by side comparison for each proposal on a requirement by requirement basis.

In general, the ONLY information the evaluators were allowed to use throughout the process was that provided in the source documents (the requirements document and the proposal) or documents referenced by the source documents. In other words, if it wasn't written down, it generally didn't exist. Our cutoff for acceptance of information was 1 June 2000 - any submissions after that time were not considered in the panel's deliberations.

1.3. Members Statements

The group was chaired by Michael St.Johns. David Mitton was the document editor. Following are the background statements and any conflicts of interest from them and the rest of the panel.

Michael St. Johns, Rainmaker Technologies

I have no known conflicts of interest with respect to the AAA process. I have neither advocated nor participated in the creation of any of the submissions. My company is a service company (ISP) and will not be involved in the manufacture or sale of AAA enabled products. Other than my participation as the chair of the AAA evaluation process, I have not had any contact with the AAA standards process.

David Mitton, Nortel Networks

I have been Nasreq WG co-chair and author of several Nasreq drafts. As well as, previously contributed to several RADIUS drafts.

I have been a RADIUS NAS implementor and Technical Prime on our Server products, so know it extremely well. In my current job role I am involved with Nortel's IP Mobility products, which support Diameter.

I have written a presentation on COPS vs NASreq Requirements for a Nasreq meeting, but have not implemented it, nor consider myself an through expert on the subject.

Stuart Barkley, UUNET

I've been working for 5 years at UUNET on various parts of our dialup network. I have extensive experience with designing, developing and operating our SNMP based usage data gathering system. I've also been involved in our radius based authentication and authorization systems in an advisory position.

I've participated in radius/roamops/nasreq/aaa groups for the past several years. I'm not an author or contributer on any of the requirements or protocol documents being presented although I have been peripherally involved in these working groups.

Dave Nelson, Enterasys Networks

Very active in the RADIUS WG, especially during the early years. No involvement in the AAA submission. Have not contributed to the development of Diameter.

No involvement with SNMPv3 or the AAA submission. David Harrington, a proponent, works in a different group within my company. We have not discussed the submission. No involvement with the COPS protocol.

Basavaraj Patil, Nokia

I am a contributor to the AAA requirements document (RFC 2977) submitted by the Mobile IP WG. I was a member of the team that was constituted to capture the Mobile IP requirements for AAA services.

As part of the co-chairing activity of the Mobile IP WG I have realized the need for AAA services by Mobile IP and hence closely followed the work done in the AAA WG, RADIUS, RoamOps and TR45.6.

My present work at Nokia does involve looking at AAA protocols (to some extent at least) for use in wireless networks. I have also done some work with AAA protocols such as Diameter in my previous job at Nortel Networks.

Mark Stevens, Ellacoya Networks

I am the co-chair of the IETF RAP working group which is the working group that has developed the COPS protocol. I have not contributed to the documents describing how COPS can satisfy AAA requirements.

I participated in early AAA working group meetings, but have not been an active participant since the group's rechartering. The company that currently employees me builds devices might benefit from being AAA enabled.

Barney Wolff, Databus Inc.

I have implemented RADIUS client, proxy and server software, under contract to AT&T. That software is owned by AT&T and I have no financial interest in it.

I have been a member of the RADIUS WG for several years, and consider myself an advocate for RADIUS against what I consider unjustified attacks on it.

I've never worked for any of the companies whose staff have produced any of the proposals, although I obviously might at some future time.

1.4. Requirements Validation Process

For each of the base requirements documents, the chair assigned a team member to re-validate the requirement. The process was fairly mechanical; the evaluator looked at what was said in [AAAReqts], and verified that the references and supporting text in the basis document supported the requirement in [AAAReqts] as stated. Where the reference was wrong, too general, missing or otherwise did not support the requirement, the evaluator either deleted or downgraded the requirement. The results of that process were sent to the AAA mailing list and are also included in this document in the appendixes. The group's used [AAAReqts] as modified by our validation findings to evaluate the AAA proposals.

1.5. Proposal Evaluation

For each of the four proposals, the chair assigned two panel members to write evaluation briefs. One member was assigned to write a 'PRO' brief and could take the most generous interpretation of the proposal; he could grant benefit of doubt. The other member was assigned to write a 'CON' brief and was required to use the strictest criteria when doing his evaluation.

Each brief looked at each individual requirement and evaluated how close the proposal came in meeting that requirement. Each item was scored as one of an 'F' for failed to meet the requirement, 'P' for partially meeting the requirement, or 'T' for totally meeting the requirement. The proposals were scored only on the information presented. This means that a particular protocol might actually meet the specifics of a requirement, but if the proposal did not state, describe or reference how that requirement was met, in might be scored lower.

The panel met by teleconference to discuss each proposal and the PRO and CON briefs. Each of the briefers discussed the high points of the brief and gave his summary findings for the proposal. We then discussed each individual requirement line-by-line as a group. At the conclusion, the members provided their own line-by-line evaluations which were used to determine the consensus evaluation for the specific requirement relative to that proposal. The meeting notes from those teleconferences as well as the individual briefs are included in the appendixes.

1.6. Final Recommendations Process

The panel met for one last time to compare the results for the four proposals and to ensure we'd used consistent evaluation criteria. We did a requirement by requirement discussion, then a discussion of each of the protocols.

The final phase was for each member to provide his final summary evaluation for each of the protocols. Each proposal was scored as either Not Acceptable, Acceptable Only For Accounting, Acceptable with Engineering and Fully Acceptable. Where a proposal was acceptable with engineering, the member indicated whether it would be a small, medium or large amount.

It should be noted that score indicated the opinion of the team member. And they may have taken into consideration background knowledge or additional issues not captured in the minutes presented here.

Each member's scores were used within the group to develop the group's consensus.

2. Protocol Proposals

The following proposal documents were submitted to the AAA WG for consideration by the deadline.

- SNMP:

  [SNMPComp] "Comparison of SNMPv3 Against AAA Network Access Requirements", Work in Progress.

- RADIUS Enhancements:

  [RADComp] "Comparison of RADIUS Against AAA Network Access Requirements", Work in Progress.

  [RADExt] "Framework for the extension of the RADIUS(v2) protocol", Work in Progress.

- Diameter

  [DIAComp] "Comparison of Diameter Against AAA Network Access Requirements", Work in Progress.

- COPS for AAA:

  [COPSComp] "Comparison of COPS Against the AAA NA Requirements", Work in Progress.

  [COPSAAA] "COPS Usage for AAA", Work in Progress.

3. Item Level Compliance Evaluation

For each requirement item, the group reviewed the proposal's level of compliance. Where the proposal was lacking, the evaluators may have made supposition on how hard it would be to resolve the problem. The following shows the consensus results for each requirement item.

Key:
T = Total Compliance, Meets all requirements fully
P = Partial Compliance, Meets some requirements
F = Failed Compliance, Does not meet requirements acceptably

Where two are shown eg: P/T, there was a tie.

The sub-section numbering corresponds to the requirements document section and item numbers. This relative numbering was also used in the Protocol Position presentations, here in the appendices.

3.1 General Requirements

3.1.1 Scalability - SNMP:P, RADIUS:P, Diameter:T, COPS:T

SNMP was downgraded due to a lack of detail of how the current agent model would be adapted to a client request based transaction. The RADIUS proposal did not address the problem adequately. There are open issues in all proposals with respect to webs of proxies.

3.1.2 Fail-over - SNMP:P, RADIUS:P, Diameter:P, COPS:T/P

The group particularly noted that it didn't think any protocol did well in this requirement. Insufficient work has been done to specify link failure detection and primary server recovery in most submissions. COPS has some mechanisms but not all. How these mechanisms would work in a web of proxies has not been addressed.

3.1.3 Mutual Authentication - SNMP:T, RADIUS:T/P, Diameter:T, COPS:T

Many of the submissions missed the point of the requirement. There should be a way for the peers to authenticate each other, end-to-end, or user-to-server. However, the group questions who really needs this feature, and if it could be done at a different level.

Mutual authentication in RADIUS is only between hops.

3.1.4 Transmission Level Security - SNMP:T, RADIUS:P, Diameter:T, COPS:T

All protocols have methods of securing the message data.

3.1.5 Data Object Confidentiality - SNMP:P, RADIUS:P, Diameter:T, COPS:T

This requirement usually comes from third-party situations, such as access outsourcing.

Diameter and COPS both use CMS formats to secure data objects. The group is concerned if this method and it's support is perhaps too heavy weight for NAS and some types of edge systems.

3.1.6 Data Object Integrity - SNMP:F, RADIUS:P, Diameter:T, COPS:T

How to guard the data object from changes was not adequately described in the SNMP proposal. The RADIUS solution was not very strong either.

3.1.7 Certificate Transport - SNMP:T, RADIUS:T, Diameter:T, COPS:T

All protocols can figure out some way to transport a certificate.

3.1.8 Reliable AAA Transport - SNMP:P, RADIUS:P, Diameter:T, COPS:T

The requirement does not give a definition of "how reliable" it must be.

The SNMP and RADIUS proposals lacked in providing solutions to message retransmission and recovery.

3.1.9 Run over IPv4 - SNMP:T, RADIUS:T, Diameter:T, COPS:T

3.1.10 Run over IPv6 - SNMP:P, RADIUS:T, Diameter:T, COPS:T

The SNMP proposal indicated that this area is still in the experimental stages.

3.1.11 Support Proxy and Routing Brokers - SNMP:F, RADIUS:P, Diameter:T, COPS:P

The SNMP proposal did not address this requirement. COPS claims support, but does not work through some of the issues. Diameter was the only protocol that attempted to address this area to a fair extent.

3.1.12 Auditability - SNMP:F, RADIUS:F, Diameter:T, COPS:P

We treated this requirement as something like "non-repudiation". There is a concern that digital signatures may be too computationally expensive for some equipment, and not well deployed on those platforms.

The SNMP and RADIUS proposals did not attempt to work this requirement. COPS suggests that a History PIB will help solve this problem but gives no description.

3.1.13 Shared Secret Not Required - SNMP:P/T, RADIUS:T, Diameter:T, COPS:T

The requirement is interpreted to mean that any application level security can be turned off in the presence of transport level security.

Pretty much every protocol can use an enveloping secure transport that would allow them not to use an internal secret.

3.1.14 Ability to Carry Service Specific Attributes - SNMP:T, RADIUS:T, Diameter:T, COPS:T

3.2 Authentication Requirements

3.2.1 NAI Support - SNMP:T, RADIUS:T, Diameter:T, COPS:T

3.2.2 CHAP Support - SNMP:T, RADIUS:T, Diameter:T, COPS:T

3.2.3 EAP Support - SNMP:T, RADIUS:T, Diameter:T, COPS:T

3.2.4 PAP/Clear-text Passwords - SNMP:T, RADIUS:T, Diameter:T, COPS:T

The requirement for clear-text passwords comes from one-time-password systems and hard-token (SecurID) systems.

3.2.5 Reauthentication on demand - SNMP:T, RADIUS:P, Diameter:P, COPS:T

To supply this, the proposal must have asynchronous peer-to-peer capabilities, and there must defined operation for such state changes.

We also distinguished event-driven Reauthentication from timer-driven (or lifetime-driven). Also concerned about how this would work in a proxy environment.

3.2.6 Authorization w/o Authentication - SNMP:P, RADIUS:T/P, Diameter:T, COPS:T

This requirement really means authorization with trivial authentications (e.g. by assertion or knowledge).

3.3 Authorization Requirements

3.3.1 Static and Dynamic IP Addr Assignment - SNMP:P/F, RADIUS:T, Diameter:T, COPS:T

There is difficulty in interpreting what is static or dynamic with respect to the viewpoint of the client, server, administrator or user.

3.3.2 RADIUS Gateway Capability - SNMP:P, RADIUS:P, Diameter:T/P, COPS:P

It was noted that any new capability in a new AAA protocol would not be able to map directly back to RADIUS. But this is already a problem within a RADIUS environment.

3.3.3 Reject Capability - SNMP:T/P/F, RADIUS:T, Diameter:T, COPS:P

3.3.4 Preclude Layer 2 Tunneling - SNMP:F, RADIUS:T, Diameter:T, COPS:T

3.3.5 Reauthorization on Demand - SNMP:P/F, RADIUS:P, Diameter:T/P, COPS:T

Some evaluators wondered how the server will know that re-authorization is supposed to be done? Will it interface to something external, or have sufficient internals?

3.3.6 Support for Access Rules & Filters - SNMP:P, RADIUS:P, Diameter:P, COPS:T/P

Only the Diameter proposal actually tackled this issue, but the group felt that the rules as designed were too weak to be useful. There was also concern about standardizing syntax without defining semantics.

3.3.7 State Reconciliation - SNMP:F, RADIUS:P/F, Diameter:P, COPS:T/P

All of the protocols were weak to non-existent on specifying how this would be done in a web of proxies situation.

3.3.8 Unsolicited Disconnect - SNMP:T, RADIUS:P, Diameter:T, COPS:T

3.4 Accounting Requirements

3.4.1 Real Time Accounting - SNMP:T, RADIUS:T, Diameter:T, COPS:T

3.4.2 Mandatory Compact Encoding - SNMP:T, RADIUS:T, Diameter:T, COPS:T

3.4.3 Accounting Record Extensibility - SNMP:T, RADIUS:T, Diameter:T, COPS:T

3.4.4 Batch Accounting - SNMP:T, RADIUS:F, Diameter:P, COPS:P

Some members of the group are not sure how this fits into the rest of the AAA protocol, which is primarily real-time and event driven. Would this be better met with FTP?

3.4.5 Guaranteed Delivery - SNMP:T, RADIUS:T, Diameter:T, COPS:T

3.4.6 Accounting Timestamps - SNMP:T, RADIUS:T, Diameter:T, COPS:T

3.4.7 Dynamic Accounting - SNMP:T, RADIUS:T, Diameter:T, COPS:T

3.5 MOBILE IP Requirements

3.5.1 Encoding of MOBILE IP Registration Messages - SNMP:T, RADIUS:T/P, Diameter:T, COPS:T

3.5.2 Firewall Friendly - SNMP:F, RADIUS:T, Diameter:P, COPS:P

There was considerable discussion about what it means to be "firewall friendly". It was suggested that not making the firewall look into packets much beyond the application port number. Protocols such as SNMP and COPS are at a disadvantage, as you must look far into the packet to understand the intended operation. Diameter will have the disadvantage of SCTP, which is not well deployed or recognized at the moment.

SNMP and COPS also have the problem that they are used for other types of operations than just AAA.

Should firewalls have AAA Proxy engines?

We didn’t look at "NAT friendly" issues either.

COPS:T

The group is not clear on how this requirement impacts the actual protocol. Raj explained it to us, but we mostly took it on faith.

4. Protocol Evaluation Summaries

4.1. SNMP

SNMP is generally not acceptable as a general AAA protocol. There may be some utility in its use for accounting, but the amount of engineering to turn it into a viable A&A protocol argues against further consideration.

4.2. Radius++

Radius++ is not considered acceptable as an AAA protocol. There is a fairly substantial amount of engineering required to make it meet all requirements, and that engineering would most likely result in something close to the functionality of Diameter.

4.3. Diameter

Diameter is considered acceptable as an AAA protocol. There is some minor engineering required to bring it into complete compliance with the requirements but well within short term capabilities. Diameter might also benefit from the inclusion of a broader data model ala COPS.

4.4. COPS

COPS is considered acceptable as an AAA protocol. There is some minor to medium engineering required to bring it into complete compliance with the requirements.

4.5. Summary Recommendation

The panel expresses a slight preference for Diameter based on the perception that the work for Diameter is further along than for COPS. However, using SCTP as the transport mechanism for Diameter places SCTP on the critical path for Diameter. This may ultimately result in COPS being a faster approach if SCTP is delayed in any way.

5. Security Considerations

AAA protocols enforce the security of access to the Internet. The design of these protocols and this evaluation process took many security requirements as critical issues for evaluation. A candidate protocol must meet the security requirements as documented, and must be engineered and reviewed properly as developed and deployed.

6. References

[AAAReqts] Aboba, B., Clahoun, P., Glass, S., Hiller, T., McCann, P., Shiino, H., Walsh, P., Zorn, G., Dommety, G., Perkins, C., Patil, B., Mitton, D., Manning, S., Beadles, M., Chen, X., Sivalingham, S., Hameed, A., Munson, M., Jacobs, S., Lim, B., Hirschman, B., Hsu, R., Koo, H., Lipford, M., Campbell, E., Xu, Y., Baba, S. and E. Jaques, "Criteria for Evaluating AAA Protocols for Network Access", RFC 2989, April 2000.

[AAAComp] Ekstein, TJoens, Sales and Paridaens, "AAA Protocols: Comparison between RADIUS, Diameter and COPS", Work in Progress.

[SNMPComp] Natale, "Comparison of SNMPv3 Against AAA Network Access Requirements", Work in Progress.

[RADComp] TJoens and DeVries, "Comparison of RADIUS Against AAA Network Access Requirements", Work in Progress.

[RADExt] TJoens, Ekstein and DeVries, "Framework for the extension of the RADIUS (v2) protocol", Work in Progress,

[DIAComp] Calhoun, "Comparison of Diameter Against AAA Network Access Requirements", Work in Progress.

[COPSComp] Khosravi, Durham and Walker, "Comparison of COPS Against the AAA NA Requirements", Work in Progress.

[COPSAAA] Durham, Khosravi, Weiss and Filename, "COPS Usage for AAA", Work in Progress.

7. Authors' Addresses

David Mitton
Nortel Networks
880 Technology Park Drive
Billerica, MA 01821

Phone: 978-288-4570
EMail: dmitton@nortelnetworks.com

Michael StJohns
Rainmaker Technologies
19050 Pruneridge Ave, Suite 150
Cupertino, CA 95014

Phone: 408-861-9550 x5735
EMail: stjohns@rainmakertechnologies.com

Stuart Barkley
UUNET
F1-1-612
22001 Loudoun County Parkway
Ashburn, VA 20147 US

Phone: 703-886-5645
EMail: stuartb@uu.net

David B. Nelson
Enterasys Networks, Inc. (a Cabletron Systems company)
50 Minuteman Road
Andover, MA 01810-1008

Phone: 978-684-1330
EMail: dnelson@enterasys.com

Basavaraj Patil
Nokia
6000 Connection Dr.
Irving, TX 75039

Phone: +1 972-894-6709
EMail: Basavaraj.Patil@nokia.com

Mark Stevens
Ellacoya Networks
7 Henry Clay Drive
Merrimack, NH 03054

Phone: 603-577-5544 ext. 325
EMail: mstevens@ellacoya.com

Barney Wolff, Pres.
Databus Inc.
15 Victor Drive
Irvington, NY 10533-1919 USA

Phone: 914-591-5677
EMail: barney@databus.com

Appendix A - Summary Evaluations Consensus Results by Requirement and Protocol

Requirement Section	SNMP	Radius++	Diameter	COPS
1.1.1	P	P	T	T
1.1.2	P	P	P	T/P
1.1.3	T	T/P	T	T
1.1.4	T	P	T	T
1.1.5	P	P	T	T
1.1.6	F	P	T	T
1.1.7	T	T	T	T
1.1.8	P	P	T	T
1.1.9	T	T	T	T
1.1.10	P	T	T	T
1.1.11	F	P	T	P
1.1.12	F	F	T	P
1.1.13	P/T	T	T	T
1.1.14	T	T	T	T
1.2.1	T	T	T	T
1.2.2	T	T	T	T
1.2.3	T	T	T	T
1.2.4	T	T	T	T
1.2.5	T	P	P	T
1.2.6	P	T/P	T	T
1.3.1	P/F	T	T	T
1.3.2	P	T	T/P	P
1.3.3	T/P/F	T	T	P
1.3.4	F	T	T	T
1.3.5	P/F	P	T/P	T
1.3.6	P	P	P	T/P
1.3.7	F	P/F	P	T/P
1.3.8	T	P	T	T
1.4.1	T	T	T	T
1.4.2	T	T	T	T
1.4.3	T	T	T	T
1.4.4	T	F	P	P
1.4.5	T	T	T	T
1.4.6	T	T	T	T
1.4.7	T	T	T	T
1.5.1	T	T/P	T	T
1.5.2	F	T	P	P
1.5.3	F	P	T	T

Appendix B - Review of the Requirements

Comments from the Panel on then work in progress, "Criteria for Evaluating AAA Protocols for Network Access" now revised and published as RFC 2989. This became the group standard interpretation of the requirements at the time.

B.1 General Requirements

Scalability - In clarification [a], delete "and tens of thousands of simultaneous requests." This does not appear to be supported by any of the three base documents.

Transmission level security - [Table] Delete the ROAMOPS "M" and footnote "6". This appears to be an over generalization of the roaming protocol requirement not necessarily applicable to AAA.

Data object confidentiality - [Table] Delete the MOBILE IP "S" and footnote "33". The base document text does not appear to support this requirement.

Reliable AAA transport mechanism - In clarification [h] delete everything after the "...packet loss" and replace with a ".". The requirements listed here are not necessarily supported by the base document and could be mistakenly taken as requirements for the AAA protocol in their entirety.

Run over IPv4 - [Table] Replace the MOBILE IP footnote "17" with footnote "33". This appears to be a incorrect reference.

Run over IPv6 - [Table] Replace the MOBILE IP footnote "18" with a footnote pointing to section 8 of [8]. This appears to be an incorrect reference.

Auditability - Clarification [j] does not appear to coincide with the NASREQ meaning of Auditability. Given that NASREQ is the only protocol with an auditability requirement, this section should be aligned with that meaning.

Shared secret not required - [Table] General - This section is misleadingly labeled. Our team has chosen to interpret it as specified in clarification [k] rather than any of the possible interpretations of "shared secret not required". We recommend the tag in the table be replaced with "Dual App and Transport Security Not Required" or something at least somewhat descriptive of [k]. Delete the NASREQ "S" and footnote "28" as not supported by the NASREQ document. Delete the MOBILE IP "O" and footnotes "34" and 39" as not supported.

B.2 Authentication Requirements

NAI Support - [Table] Replace MOBILE IP footnote "38" with "39". This appears to be a more appropriate reference.

CHAP Support - [Table] Delete MOBILE IP "O" as unsupported.

EAP Support - [Table] Delete MOBILE IP "O" as unsupported.

PAP/Clear-Text Support - [Table] Replace NASREQ footnote "10" with "26" as being more appropriate. Replace ROAMOPS "B" with "O". The reference text appears to not explicitly ban this and specifically references clear text for OTP applications. Delete MOBILE IP "O" as unsupported.

Re-authentication on demand - Clarification [e] appears to go beyond the requirements in NASREQ and MOBILE IP. [Table] Delete MOBILE IP footnote "30" as inapplicable.

Authorization Only without Authentication - Clarification [f] does not include all NASREQ requirements, specifically that unneeded credentials MUST NOT be required to be filled in. Given that there are no other base requirements (after deleting the MOBILE IP requirement) we recommend that clarification [f] be brought in line with NASREQ. [Table] Delete MOBILE IP "O" and footnote "30". The referenced text does not appear to support the requirement.

B.3 Authorization Requirements

Static and Dynamic... - Clarification [a] appears to use a particularly strange definition of static and dynamic addressing. Recommend clarification here identifying who (e.g. client or server) thinks address is static/dynamic. [Table] ROAMOPS "M" appears to be a derived requirement instead of directly called out. The footnote "1" should be changed to "5" as being more appropriate. A text clarification should be added to this document identifying the derived requirement.

RADIUS Gateway capability - [Table] Delete the MOBILE IP "O" and footnote "30". The referenced text does not appear to support the requirement.

Reject capability - [Table] Delete the NASREQ "M" and footnote "12". The NASREQ document does not appear to require this capability.

Reauthorization on Demand - [Table] Delete the MOBILE IP "S" and footnotes "30,33" The referenced text does not support this requirement.

Support for Access Rules... - Clarification [e] has a overbroad list of requirements. NASREQ only requires 5-8 on the list, and as The MOBILE IP requirement is not supported by its references, this clarification should match NASREQ requirements. [Table] Delete the MOBILE IP "O" and footnotes "30,37" as not supported.

State Reconciliation - Clarification [f] should be brought in line with NASREQ requirements. The clarification imposes overbroad requirements not required by NASREQ and NASREQ is the only service with requirements in this area.

B.4 Accounting Requirements

Real-Time accounting - [Table] Replace MOBILE IP footnote [39] with a footnote pointing to section 3.1 of [3] as being more appropriate.

Mandatory Compact Encoding - [Table] Delete MOBILE IP "M" and footnote "33" as the reference does not support the requirement.

Accounting Record Extensibility - [Table] Delete NASREQ "M" and footnote "15" as the reference does not support the requirement.

Accounting Time Stamps - [Table] Delete MOBILE IP "S" and footnote "30" as they don’t support the requirement. Replace MOBILE IP footnote "40" with a footnote pointing to section 3.1 of [3] as being more appropriate.

Dynamic Accounting - [Table] Replace the NASREQ footnote "18" with a footnote pointing to section 8.4.1.5 of [3]. Delete the MOBILE IP "S" and footnote "30" as the reference does not support the requirement.

Footnote section.

[40] should be pointing to 6.1 of [4].
[41] should be pointing to 6.2.2 of [4].
[45] should be pointing to 6.4 of [4].
[46] should be pointing to 8 of [4].

Appendix C - Position Briefs

C.1 SNMP PRO Evaluation

Evaluation of SNMP AAA Requirements
PRO Evaluation
Evaluator - Stuart Barkley

Ref [1] is "Comparison of SNMPv3 Against AAA Network Access Requirements", aka 'the document'
Ref [2] is the aaa eval criteria as modified by us, aka 'the requirements'

The document uses T to indicate total compliance, P to indicate partial compliance and F to indicate no compliance. For each section I've indicated my grade for the section. If there is a change, I've indicated that and the grade given by the authors.

1 Per item discussion

1.1 General Requirements

1.1.1 Scalability - Grade T

The document indicates that SNMP can adequately handle that scale from the requirements document. Since most current uses are ppp connections and SNMP is already capable of handling the interface table and other per session tables it is clear that basic capacity exists. Additions to support other tables and variables scales in a simple linear fashion with the number of additional variables and protocol interactions. Regardless of the final selected protocol handling the scaling required is not a trivial undertaking. SNMP can draw upon existing network management practices to assist in this implementation.

1.1.2 Fail-over - Grade T

SNMP is of vital importance to the operation of most networks. Existing infrastructures can handle required failover or other redundant operations.

1.1.3 Mutual Authentication - Grade T

The use of shared secrets described in the document is a well understood method of integrity control. Although shared secrets don't necessarily provide full authentication since other parties may also have the same secrets, the level of authentication is sufficient for the task at hand. In many cases the SNMP infrastructure will

already exist and shared secrets should already be properly managed on an operational network. A failure of the SNMP shared secret approach regardless of the AAA protocol will likely leave equipment and systems open to substantial misuse bypassing any more elaborate AAA authentication.

1.1.4 Transmission Level Security - Grade T

SNMPv3 provides many additional security options which were not available or were more controversial in previous SNMP versions.

1.1.5 Data Object Confidentiality - New Grade P (from T)

The document discusses SNMPv3 which can provide data confidentially for data passing over the wire. There is substantial implied AAA architecture (brokers and proxies) in the requirements that full conformance is difficult to determine. In particular, the evaluator has difficulty with the concept of "the target AAA entity for whom the data is ultimately destined", but will concede that the desired requirement is only partially met (most especially with the transfer of a PAP password).

1.1.6 Data Object Integrity - New Grade T (from P)

SNMP has full capabilities that allow the authentication of the data. Brokers, proxies or other intermediaries in the data chain can verify the source of the information and determine that the data has not been tampered with. The document downgrades the grade to P because of confusion over the integrity checking role of intermediaries.

1.1.7 Certificate Transport - Grade T

The requirements require the capability of transporting certificates but do not have any specific use for the certificates. The requirements make assumptions that the protocol selected will be dependent upon certificates, but this is not necessarily true. SNMP can transport arbitrary objects and can transport certificates if necessary. The document indicates some issues with size of certificates and current maximum practical data sizes, however if the compact encoding requirement extends to the internal certificate information this should be less of an issue.

1.1.8 Reliable AAA Transport - New Grade T (from P)

The requirements is stated rather strongly and makes substantial assumptions of AAA protocol architecture and based upon current protocols and their failings. SNMP allows for great flexibility in retransmission schemes depending upon the importance of the data.

1.1.9 Run over IPv4 - Grade T

SNMP has operated in this mode for many years.

1.1.10 Run over IPv6 - New Grade T (from P)

SNMP must support IPv6 for many other systems so support for this should be possible by the time the requirement becomes effective. The document indicates that experimental versions satisfying this requirement are already in existence.

1.1.11 Support Proxy and Routing Brokers - New Grade T (from P)

The requirements make significant assumptions about the final architecture. It is well within the capabilities of SNMP to provide intermediaries which channel data flows between multiple parties. The document downgrades SNMPs compliance with this requirement due to issues which are covered more specifically under "Data Object Confidentially" which the evaluator has downgraded to P.

1.1.12 Auditability - New Grade T (from F)

Data flows inside SNMP are easily auditable by having secondary data flows established which provide copies of all information to auxiliary servers. The document grades this as a failure, but this support is only minor additions within a more fully fleshed out set of data flows.

1.1.13 Shared Secret Not Required - Grade T

Shared secrets are not required by SNMP. They are desirable in many instances where a lower level does not provide the necessary capabilities. The document supplies pointers to various security modes available.

1.1.14 Ability to Carry Service Specific Attributes - Grade T

SNMP has long had the ability for other parties to create new unambiguous attributes.

1.2 Authentication Requirements

1.2.1 NAI Support - Grade T

SNMP easily supports this. NAIs were defined to be easily carried in existing protocols.

1.2.2 CHAP Support - Grade T

SNMP can easily provide objects to pass the necessary information for CHAP operation.

1.2.3 EAP Support - New Grade T (from P)

SNMP can easily provide objects to pass the necessary information for EAP operation. As with CHAP or PAP MIB objects can be created to control this operation thus the upgrade from the document grade.

1.2.4 PAP/Clear-text Passwords - New Grade P (from T)

SNMP can easily provide objects to pass the necessary information for PAP operation. The requirement about non-disclosure of clear text passwords make assumptions about the protocol implementation. The choice to use clear text passwords is inherently insecure and forced protocol architecture don't really cover this. This requirement grade is downgraded to P (partial) because the document does not really address the confidentially of the data at application proxies.

1.2.5 Reauthorization on demand - Grade T

SNMP can easily provide objects to control this operation.

1.2.6 Authorization w/o Authentication - New Grade T (from T)

The document makes an incorrect interpretation of this requirement. However, SNMP makes no restriction which prevents to desired requirements. No actual change of grade is necessary, since both the actual requirements and the incorrect interpretation are satisfied by SNMP.

1.3 Authorization Requirements

1.3.1 Static and Dynamic IP Addr Assignment - Grade T

SNMP can easily provide objects to control this operation.

1.3.2 RADIUS Gateway Capability - Grade T

As the document describes, with the addition of any necessary compatibility variables SNMP can be gatewayed to RADIUS applications.

1.3.3 Reject Capability - Grade T

Any of the active components in the SNMP based structure could decide to reject and authentication request for any reason. Due to mixing different levels of requirements the document doesn't attempt to directly address this, instead indicating that a higher level application can cause this operation.

1.3.4 Preclude Layer 2 Tunneling - New Grade T (from ?)

Nothing in SNMP explicitly interacts with the selection of any tunneling mechanisms the client may select. The document author was unclear about the needs here.

1.3.5 Reauth on Demand - Grade T

SNMP can easily provide objects to control this operation.

1.3.6 Support for ACLs - Grade T

The document indicates that should it be desired SNMP can provide objects to control these operations. In addition, active components can apply substantial further configurable access controls.

1.3.7 State Reconciliation - Grade T

The requirements describe an over broad set of required capabilities. The document indicates concern over incompatibilities in the requirements, however SNMP can provide methods to allow active components to reacquire lost state information. These capabilities directly interact with scalability concerns and care needs to be taken when expecting this requirement to be met at the same time as the scalability requirements.

1.3.8 Unsolicited Disconnect - Grade T

The document indicates that SNMP can easily provide objects to control this operation.

1.4 Accounting Requirements

1.4.1 Real Time Accounting - Grade T

SNMP can provide this mode of operation. The document outlines methods both fully within SNMP and using SNMP to interface with other transfer methods. Many providers already use SNMP for real time

notification of other network events. This capability can directly interact with scalability concerns and implementation care needs to be taken to make this properly interact is large scale environments.

1.4.2 Mandatory Compact Encoding - Grade T

The document indicates the possibility of controlling external protocols to handle data transmissions where the BER encoding of SNMP objects would be considered excessive. SNMP BER encoded protocol elements are generally in a fairly compact encoding form compared with text based forms (as used in some existing radius log file implementations). This interacts with the general requirement for carrying service specific attributes and the accounting requirement for extensibility. With careful MIB design and future work on SNMP payload compression the SNMP coding overhead can be comparable with other less extensible protocols.

1.4.3 Accounting Record Extensibility - Grade T

SNMP has a strong tradition of allowing vendor specific data objects to be transferred.

1.4.4 Batch Accounting - Grade T

There are many methods which a SNMP based system could use for batch accounting. The document discusses SNMP parameters to control the batching process and indicates that certain existing MIBs contain examples of implementation strategies. SNMP log tables can provide accounting information which can be obtained in many methods not directly related to real time capabilities. The underlying system buffering requirements are similar regardless of the protocol used to transport the information.

1.4.5 Guaranteed Delivery - Grade T

SNMP is very amenable to providing guaranteed delivery. Particularly in a pull model (versus the often assumed push model) the data gatherer can absolutely know that all data has been transfered. In the common push model the data receiver does not know if the originator of the data is having problems delivering the data.

1.4.6 Accounting Timestamps - Grade T

Timestamps are used for many SNMP based operations. The document points at the DateAndTime textual convention which is available for use. As with all environments the timestamps accuracy needs evaluation before the information should be relied upon.

1.4.7 Dynamic Accounting - Grade T

As long as there is some way to relate multiple records together there are no problems resolving multiple records for the same session. This interacts with the scalability requirement and care must be taken when implementing a system with both of these requirements.

1.5 MOBILE IP Requirements

1.5.1 Encoding of MOBILE IP Registration Messages - Grade T

SNMP can easily provide objects to transfer this information.

1.5.2 Firewall Friendly - New Grade T (from P)

SNMP is already deployed in many operational networks. SNMPv3 addresses most concerns people had with the operation of previous versions. True SNMPv3 proxies (as opposed to AAA proxies) should become commonplace components in firewalls for those organizations which require firewalls.

1.5.3 Allocation of Local Home Agent - New Grade T (from ?)

SNMP is not concerned with the LHA. This can be under control of the Local network to meet its needs.

2. Summary Discussion

SNMP appears to meet most stated requirements. The areas where the SNMP proposal falls short are areas where specific AAA architectures are envisioned and requirements based upon that architecture are specified.

Scaling of the protocol family is vital to success of a AAA suite. The SNMP protocol has proved scalable in existing network management and other high volume data transfer operations. Care needs to be taken in the design of a large scale system to ensure meeting the desired level of service, but this is true of any large scale project.

3. General Requirements

SNMP is well understood and already supported in many ISP and other operational environments. Trust models already exist in many cases and can be adapted to provide the necessary access controls needed by the AAA protocols. Important issues with previous versions of SNMP have been corrected in the current SNMPv3 specification.

The SNMP proposal is silent on the specific data variables and message types to be implemented. This is largely due to the requirements not specifying the necessary data elements and the time constraints in extracting that information from the base document set. Such a data model is necessary regardless of the ultimate protocol selected.

4. Summary Recommendation

SNMP appears to fully meet all necessary requirements for the full AAA protocol family.

C.2 SNMP CON Evaluation

Evaluation of SNMP AAA Requirements
CON Evaluation
Evaluator - Michael StJohns

Ref [1] is "Comparison of SNMPv3 Against AAA Network Access Requirements", aka 'the document'
Ref [2] is the aaa eval criteria as modified by us.

The document uses T to indicate total compliance, P to indicate partial compliance and F to indicate no compliance. For each section I've indicated my grade for the section. If there is no change, I've indicated that and the grade given by the authors.

Section 1 - Per item discussion

1.1 General Requirements

1.1.1 Scalability - Although the document indicates compliance with the requirement, its unclear how SNMP actually meets those requirements. The document neither discusses how SNMP will scale, nor provides applicable references. The argument that there is an existence proof given the deployed SNMP systems appears to assume that one manager contacting many agents maps to many agents (running AAA) contacting one AAA server. A server driven system has substantially different scaling properties than a client driven system and SNMP is most definitely a server (manager) driven system. Eval - F

1.1.2 Fail-over - The document indicates the use of application level time outs to provide this mechanism, rather than the mechanism being a characteristic of the proposed protocol. The protocol provides only partial compliance with the requirement. Eval - P

1.1.3 Mutual Authentication - There is some slight handwaving here, but the protocol's USM mode should be able to support this requirement. Eval - No Change (T)

1.1.4 Transmission Level Security - The authors should elaborate on the specific use of the SNMPv3 modes to support these requirements, but the text is minimally acceptable. Eval - No Change (T)

1.1.5 Data Object Confidentiality - The authors describe a mechanism which does not appear to completely meet the requirement. VACM is a mechanism for an end system (agent) to control access to its data based on manager characteristics. This mechanism does not appear to map well to this requirement. Eval - P

1.1.6 Data Object Integrity - There appears to be some handwaving going on here. Again, SNMP does not appear to be a good match to this requirement due to at least in part a lack of a proxy intermediary concept within SNMP. Eval - F

1.1.7 Certificate Transport - The document does indicate compliance, but notes that optimization might argue for use of specialized protocols. Eval - No Change (T)

1.1.8 Reliable AAA Transport - The document indicates some confusion with the exact extent of this requirement. Given the modifications suggested by the eval group to the explanatory text in [2] for the related annotation, the point by point explanatory text is not required. The document does indicate that the use of SNMP is irrespective of the underlying transport and the support of this requirement is related at least partially to the choice of transport. However, SNMP over UDP - the most common mode for SNMP - does not meet this requirement. Eval - No Change (P)

1.1.9 Run over IPv4 - While the evaluator agrees that SNMPv3 runs over V4, the authors need to point to some sort of reference. Eval - No Change (T)

1.1.10 Run over IPv6 - The document indicates both experimental implementations and future standardization of SNMPv3 over IPv6. Eval - No Change (P)

1.1.11 Support Proxy and Routing Brokers - The section of the document (5.5.3) that, by title, should have the discussion of SNMP proxy is marked as TBD. The section notes that the inability to completely comply with the data object confidentiality and integrity requirements might affect the compliance of this section and the evaluator agrees. Eval - F

1.1.12 Auditability - The document indicates no compliance with this requirement. Eval - No Change (F)

1.1.13 Shared Secret Not Required - Slight handwaving here, but SNMPv3 does not necessarily require use of its security services if other security services are available. However, the interaction with VACM in the absence of USM is not fully described and may not have good characteristics related to this requirement. Eval - P

1.1.14 Ability to Carry Service Specific Attributes - SNMP complies via the use of MIBs. Eval - No Change (T)

1.2 Authentication Requirements

1.2.1 NAI Support - The document indicates that MIB objects can be created to meet this requirement, but gives no further information. Eval - P

1.2.2 CHAP Support - The document indicates that MIB objects can be created to meet this requirement, but gives no further information. Given the normal CHAP model, its unclear exactly how this would work. Eval - F

1.2.3 EAP Support - The document notes that EAP payloads can be carried as specific MIB objects, but also notes that further design work would be needed to fully incorporate EAP. Eval - No Change (P)

1.2.4 PAP/Clear-text Passwords - The document notes the use of MIB objects to carry the clear text passwords and the protection of those objects under normal SNMPv3 security mechanisms. Eval - No Change (T)

1.2.5 Reauthorization on demand - While there’s some handwaving here, its clear that the specific applications can generate the signals to trigger reauthorization under SNMP. Eval - No Change (T)

1.2.6 Authorization w/o Authentication - The author appears to be confusing the AAA protocol authorization with the AAA user authorization and seems to be over generalizing the ability of SNMP to deal with general AAA user authorization. Eval - F

1.3 Authorization Requirements

1.3.1 Static and Dynamic IP Addr Assignment - The reference to MIB objects without more definite references or descriptions continues to be a negative. While the evaluator agrees that MIB objects can represent addresses, the document needs to at least lead the reader in the proper direction. Eval - F

1.3.2 RADIUS Gateway Capability - The transport and manipulation of Radius objects appears to be only a part of what is required. Eval - P

1.3.3 Reject Capability - Again, a clarification of how SNMP might accomplish this requirement would be helpful. The overall document lacks a theory of operation for SNMP in an AAA role that might have clarified the various approaches. Eval - F

1.3.4 Preclude Layer 2 Tunneling - Document indicates lack of understanding of this requirement. Eval - F

1.3.5 Reauth on Demand - See response in 1.3.3 above. None of the text responding to this requirement, nor any other text in the document, nor any of the references describes the appropriate framework and theory. Eval - F

1.3.6 Support for ACLs - The response text again references MIB objects that can be defined to do this job. There is additional engineering and design needed before this is a done deal. Eval - P

1.3.7 State Reconciliation - The text fails to address the basic question of how to get the various parts of the AAA system back in sync. Eval - F

1.3.8 Unsolicited Disconnect - Assuming that the NAS is an SNMP agent for an AAA server acting as an SNMP manager the evaluator concurs. Eval - No Change (T).

1.4 Accounting Requirements

1.4.1 Real Time Accounting - SNMP Informs could accomplish the requirements. Eval - No Change (T)

1.4.2 Mandatory Compact Encoding - This is a good and reasonable response. SNMP can vary the style and type of reported objects to meet specific needs. Eval - No Change (T).

1.4.3 Accounting Record Extensibility - MIBs are extensible. Eval - No Change (T)

1.4.4 Batch Accounting - MIBs provide data collection at various times. Eval - No Change (T)

1.4.5 Guaranteed Delivery - There’s some weasel wording here with respect to what guaranteed means, but the description of mechanisms does appear to meet the requirements. Eval - No Change (T)

1.4.6 Accounting Timestamps - Accounting records can use the DateAndTime Textual Convention to mark their times. Eval - No Change (T)

1.4.7 Dynamic Accounting - The author may have partially missed the point on this requirement. While the number of records per session is not of great interest, the delivery may be. The author should go a little more into depth on this requirement. Eval - No Change (T)

1.5 MOBILE IP Requirements

1.5.1 Encoding of MOBILE IP Registration Messages - Registration messages can probably be encoded as SNMP messages. Eval - No Change (T)

1.5.2 Firewall Friendly - There’s a chicken and egg problem with the response to the requirement in that the author hopes that SNMP as an AAA protocol will encourage Firewall vendors to make SNMP a firewall friendly protocol. Eval - F

1.5.3 Allocation of Local Home Agent - The author disclaims an understanding of this requirement. Eval - F

2. Summary Discussion

The documents evaluation score was substantially affected by a lack of any document, reference or text which described a theory of operation for SNMP in AAA mode. Of substantial concern are the items relating to the AAA server to server modes and AAA client to server modes and the lack of a map to the SNMP protocol for those modes.

The evaluator also notes that the scaling issues of SNMP in SNMP agent/manager mode are in no way indicative of SNMP in AAA client/server mode. This has a possibility to substantially impair SNMPs use in an AAA role.

However, SNMP may have a reasonable role in the Accounting space. SNMP appears to map well with existing technology, and with the requirements.

3. General Requirements

SNMP appears to meet the general requirements of an IP capable protocol, but may not have a proper field of use for all specific requirements.

4. Summary Recommendation

Recommended in Part. SNMP is NOT RECOMMENDED for use as either an authentication or authorization protocol, but IS RECOMMENDED for use as an accounting protocol.

C.3 RADIUS+ PRO Evaluation

Evaluation of RADIUS AAA Requirements PRO Evaluation

Evaluator - Mark Stevens

Ref [1] is "Comparison of RADIUS Against AAA Network Access Requirements"
Ref [2] is "Framework for the extension of the RADIUS(v2) protocol"
Ref [3] is the aaa eval criteria as modified by us.

The documents uses T to indicate total compliance, P to indicate partial compliance and F to indicate no compliance.

For each section I've indicated my grade for the section. I have indicated whether or not my evaluation differs from the statements made with respect to RADIUS++. The evaluation ratings as given below may differ from the evaluations codified in the document referred to as, "Comparison of RADIUS Against AAA Network Access Requirements" without any indication.

1.1 General Requirements

1.1.1 [a] Scalability - In as much as a protocol's scalability can be measured, the protocol seems to transmit information in a fairly efficient manner.So, in that the protocol appears not to consume an inordinate amount of bandwidth relative to the data it is transmitting, this protocol could be considered scalable. However, the protocol has a limit in the number of concurrent sessions it can support between endpoints. Work arounds exist and are in use. Eval - P (no change)

1.1.2 [b] Fail-over - The document indicates the use of application level time outs to provide this mechanism, rather than the mechanism being a characteristic of the proposed protocol. The fail-over requirement indicates that the protocol must provide the mechanism rather than the application. The implication is that the application need not be aware that the fail-over and subsequent correction when it happens. The application using the RADIUS++ protocol will be involved in fail-over recovery activities. The protocol layer of the software does not appear to have the capability built-in. Given the wording of the requirement: Eval - P (changed from T)

1.1.3 [c] Mutual Authentication - The RADIUS++ protocol provides shared-secret as a built-in facility for mutual authentication. The authors of the document suggest the use of IPSec to obtain mutual authentication functions. The RADIUS++ protocol provides no road blocks to obtaining mutual authentication between instances of AAA applications, however the protocol provides no facilities for doing so.

1.1.4 [d] Transmission Level Security - The RADIUS++ protocol provides no transmission level security features, nor does it preclude the use of IPSec to obtain transmission level security. Eval - P (no change)

1.1.5 [e] Data Object Confidentiality - The document describes a RAIDUS++ message designed to server as an envelope in which encrypted RADIUS messages (attributes) may be enclosed. Eval - T (no change)

1.1.6 [f] Data Object Integrity - Using visible signatures, the RADIUS++ protocol appears to meet this requirement. Eval - T (no change)

1.1.7 [g] Certificate Transport - The document indicates compliance through the use of the CMS-Data Radius Attribute (message). Eval - T (no change)

1.1.8 [h] Reliable AAA Transport - The document points out that RADIUS++ can be considered a reliable transport when augmented with Layer 2 Tunneling Protocol. The protocol itself does not provide reliability features. Reliability remains the responsibility of the application or a augmenting protocol. Eval - P (no change)

1.1.9 [i] Run over IPv4 - Eval - T (no change)

1.1.10 [j] Run over IPv6 - an IPv6 Address data type must be defined. Eval - T (no change)

1.1.11 [k] Support Proxy and Routing Brokers - There is no mechanism for rerouting requests, but an extension can be made to do so. Eval - T (no change)

1.1.12 [l] Auditability - The document indicates no compliance with this requirement. Eval - F (no change)

1.1.13 [m] Shared Secret Not Required - RADIUS++ can be configured to run with empty shared secret values. Eval - T (no change)

1.1.14 [n] Ability to Carry Service Specific Attributes - Vendor escape mechanism can be used for this purpose.. Eval - T (no change)

1.2 Authentication Requirements

1.2.1 [a] NAI Support - Eval - T (no change)

1.2.2 [b] CHAP Support - Subject to dictionary attacks. Eval - P (changed from T)

1.2.3 [c] EAP Support - Eval - T (no change)

1.2.4 [d] PAP/Clear-text Passwords - No end-to-end security, but potential for encapsulation exists within current paradigm of the protocol. - Eval -T (no change)

1.2.5 [e] Reauthentication on demand - The RADIUS protocol supports re-authentication. In case re-authentication is initiated by the user or AAA client, the AAA client can send a new authentication request. Re-authentication can be initiated from the visited or home AAA server by sending a challenge message to the AAA client. Eval - T (no change)

1.2.6 [f] Authorization w/o Authentication - A new message type can be created to enable RADIUS++ to support Aw/oA . Eval - T (no change)

1.3 Authorization Requirements

1.3.1[a] Static and Dynamic IP Addr Assignment - Both supported. IPv6 would require the definition of a new address data type. Eval - P (no change)

1.3.2 [b] RADIUS Gateway Capability - The transport and manipulation of RADIUS objects appears to be only a part of what is required. Requirement seems to be worded to preclude RADIUS. Eval - P (changed from T)

1.3.3 [c] Reject Capability - Eval -T

1.3.4 [d] Preclude Layer 2 Tunneling - I do not see a definition in the AAA eval criteria document. Eval - ?

1.3.5 [e] Reauthorization on Demand - Implementation in the field demonstrate that extensions to RADIUS can support the desired behavior. Re-authentication is currently coupled to re-authorization. Eval - P (no change)

1.3.6 [f] Support for ACLs - Currently done in the applications behind the RADIUS end points, not the within the protocol. RADIUS++ could define additional message types to deal with expanded access control within new service areas. Eval - P (no change)

1.3.7 [g] State Reconciliation - Eval - F (no change)

1.3.8 [h] Unsolicited Disconnect - RADIUS++ extensions to support. Eval - T. (no change)

1.4 Accounting Requirements

1.4.1 [a] Real Time Accounting - Eval - T (no change)

1.4.2 [b] Mandatory Compact Encoding - Eval - T (no change)

1.4.3 [c] Accounting Record Extensibility - Eval - T (no change)

1.4.4 [d] Batch Accounting - RADIUS++ offers no new features to support batch accounting. Eval - F No change)

1.4.5 [e] Guaranteed Delivery - Retransmission algorithm employed. Eval - T (no change)

1.4.6 [f] Accounting Timestamps - RADIUS++ extensions support timestamps. Eval - T (no change)

1.4.7 [g] Dynamic Accounting - RADIUS++ extensions to support. Eval - T (no change)

1.5 MOBILE IP Requirements

1.5.1 [a] Encoding of MOBILE IP Registration Messages - RADIUS++ extensions can be made to include registration messages as an opaque payload. Eval - T (no change)

1.5.2 [b] Firewall Friendly - RADIUS is known to be operational in environments where firewalls acting as a proxy are active. Eval - T (no change)

1.5.3 [c] Allocation of Local Home Agent -Requirement statement needs some clarification and refinement. Eval - F (no change)

2. Summary Discussion

The RADIUS protocol, and its associated extensions, is presently not fully compliant with the AAA Network Access requirements. However, it is possible with a small effort to extend present procedures to meet the requirements as listed in, while maintaining a high level of interoperability with the wide deployment and installed base of RADIUS clients and servers.

3. General Requirements

RADIUS++ the protocol and the application meet the majority of the requirements and can be extended to meet the requirements where necessary.

4. Summary Recommendation

RADIUS++ as it could be developed would provide a level of backward compatibility that other protocols cannot achieve. By extending RADIUS in the simple ways described in the documents listed above, the transition from existing RADIUS-based installations to RADIUS++ installations would be easier. Although accounting continues to be weaker than other approaches, the protocol remains a strong contender for continued use in the areas of Authorization and Authentication.

C.4 RADIUS+ CON Evaluation

Evaluation of RADIUS++ (sic) AAA Requirements CON Evaluation
Evaluator - David Nelson

Ref [1] is "Comparison of RADIUS Against AAA Network Access Requirements", a.k.a. 'the document'
Ref [2] is "Framework for the extension of the RADIUS(v2) protocol", a.k.a. 'the protocol'
Ref [3] is the AAA evaluation criteria as modified by us.
Ref [4] is RFC 2869.
Ref [5] is an expired work in progress "RADIUS X.509 Certificate Extensions".
Ref [6] is RFC 2868

The document uses T to indicate total compliance, P to indicate partial compliance and F to indicate no compliance. Evaluator's Note: The document [1] pre-dates the protocol [2]. It is clear from reading [2], that some of the issues identified as short comings in [1] are now addressed in [2]. The evaluator has attempted to take note of these exceptions, where they occur.

Section 1 - Per item discussion

1.1 General Requirements

1.1.1 Scalability - The document [1] indicates partial compliance, largely in deference to the "tens of thousands of simultaneous requests" language in [3], that has been deprecated. The issue of simultaneous requests from a single AAA client is addressed in [1], indicating that the apparent limitation of 256 uniquely identifiable outstanding request can be worked around using well known techniques, such as the source UDP port number of the request. The document claims "P", and the evaluator concurs.

1.1.2 Fail-over - The document [1] indicates the use of application level time outs to provide the fail-over mechanism. Since the AAA protocol is indeed an application-layer protocol, this seems appropriate. There are significant issues of how to handle fail-over in a proxy-chain environment that have not been well addressed, however. The document claims "T", and the evaluator awards "P".

1.1.3 Mutual Authentication - The document [1] indicates that mutual authentication exists in the presence of a User-Password or CHAP-Password attribute in an Access-Request packet or the Message-Authenticator [4] in any packet. Once again, this addresses hop-by-hop authentication of RADIUS "peers", but does not fully address proxy-chain environments, in which trust models would need to be established. The document further indicates that strong mutual authentication could be achieved using the facilities of IPsec. This claim would apply equally to all potential AAA protocols, and cannot be fairly said to be a property of the protocol itself. The document claims "T", and the evaluator awards "F".

1.1.4 Transmission Level Security - The document [1] indicates that transmission layer security, as defined in [3], is provided in the protocol, using the mechanisms described in section 1.1.3. It should be noted that this requirement is now a SHOULD in [3]. The document claims "P", and the evaluator concurs.

1.1.5 Data Object Confidentiality - The document [1] indicates that end-to-end confidentiality is not available in RADIUS, but goes on to say that it could be added. The protocol [2] actually makes an attempt to specify how this is to be done, in section 4.3.2.2 of [2], using a CMS-data attribute, based in large part upon RFC 2630. The evaluator has not, at this time, investigated the applicability of RFC 2630 to the AAA work. The document claims "F", but in light of the specifics of the protocol [2], the evaluator awards "P".

1.1.6 Data Object Integrity - The document [1] indicates that end-to-end integrity is not available in RADIUS, but goes on to say that it could be added. The protocol [2] actually makes an attempt to specify how this is to be done, in section 4.3.2.1 of [2], using a CMS-data attribute, based in large part upon RFC 2630. The evaluator has not, at this time, investigated the applicability of RFC 2630 to the AAA work. The document claims "F", but in light of the specifics of the protocol [2], the evaluator awards "P".

1.1.7 Certificate Transport - The document [1] indicates that certificate transport is not available in RADIUS, but goes on to say that it could be added. The protocol [2] actually makes an attempt to specify how this is to be done, in section 4.3.2.3 of [2], using a CMS-data attribute, based in large part upon RFC 2630. The evaluator has not, at this time, investigated the applicability of RFC 2630 to the AAA work. Other relevant work in the area of certificate support in RADIUS may be found in an expired work in progress, "RADIUS X.509 Certificate Extensions" [5]. The document claims "F", but in light of the specifics of the protocol [2], the evaluator awards "P".

1.1.8 Reliable AAA Transport - The document [1] indicates that RADIUS provides partial compliance with the requirements of the original AAA requirements document. However, in [3], the requirement has been simplified to "resilience against packet loss". Once again, the evaluator finds that the protocol [2] meets this criteria on a hop-by-hop basis, but fails to effectively address these issues in a proxy-chain environment. The document claims "P", and the evaluator awards "F".

1.1.9 Run over IPv4 - RADIUS is widely deployed over IPv4. The document claims "T", and the evaluator concurs.

1.1.10 Run over IPv6 - The document [1] indicates that adoption of a limited number of new RADIUS attributes to support IPv6 is straightforward. Such discussion has transpired on the RADIUS WG mailing list, although that WG is in the process of shutting down. The document claims "P", and the evaluator concurs.

1.1.11 Support Proxy and Routing Brokers - The document [1] indicates that RADIUS is widely deployed in proxy-chains of RADIUS servers. This is equivalent to the Proxy Broker case, but the Routing Broker case is a different requirement. The protocol [2] does not describe any detail of how a Routing Broker might be accommodated, although it opens the door by indicating that the RADIUS++ protocol is peer-to-peer, rather than client/server. The document claims "P", and the evaluator awards "F".

1.1.12 Auditability - The document [1] indicates no compliance with this requirement. The document claims "F", and the evaluator concurs.

1.1.13 Shared Secret Not Required - The document [1] indicates that RADIUS may effectively skirt the requirement of application-layer security by using a value of "zero" for the pre-shared secret. While this is a bit creative, it does seem to meet the requirement. The document claims "T" and the evaluator concurs.

1.1.14 Ability to Carry Service Specific Attributes - RADIUS has a well defined Vendor-Specific Attribute, which, when properly used, does indeed provide for the ability to transport service-specific attributes. The document claims "T", and the evaluator concurs.

1.2 Authentication Requirements

1.2.1 NAI Support - The document [1] indicates that RADIUS specifies the NAI as one of the suggested formats for the User-Name attribute. The document claims "T", and the evaluator agrees.

1.2.2 CHAP Support - CHAP support is widely deployed in RADIUS. The document claims [1] "T", and the evaluator concurs.

1.2.3 EAP Support - The document [1] indicates that EAP support in RADIUS is specified in [4]. The document claims [1] "T", and the evaluator concurs.

1.2.4 PAP/Clear-text Passwords - The document [1] indicates that RADIUS provides protection of clear-text passwords on a hop-by-hop basis. The protocol [2] indicates how additional data confidentiality may be obtained in section 4.3.2.2 of [2], using a CMS-data attribute, based in large part upon RFC 2630. The evaluator has not, at this time, investigated the applicability of RFC 2630 to the AAA work. The document claims [1] "F", but in light of the specifics of the protocol [2], the evaluator awards "P".

1.2.5 Reauthentication on demand - The document [1] indicates that RADIUS may accomplish re-authentication on demand by means of an Access-Challenge message sent from a server to a client. The evaluator disagrees that this is likely to work for a given session once an Access-Accept message has been received by the client. The document claims "T", and the evaluator awards "F".

1.2.6 Authorization w/o Authentication - This requirement, as applied to the protocol specification, mandates that non- necessary authentication credentials not be required in a request for authorization. The actual decision to provide authorization in the

absence of any authentication resides in the application (e.g. AAA server). RADIUS does require some form of credential in request messages. The document [1] claims "F", and the evaluator concurs.

1.3 Authorization Requirements

1.3.1 Static and Dynamic IP Addr Assignment - The document [1] indicates that RADIUS can assign IPv4 addresses, and can easily be extended to assign IPv6 addresses (see section 1.1.10). Of greater concern, however, is the issue of static vs. dynamic addresses. If dynamic address has the same meaning as it does for DHCP, then there are issues of resource management that RADIUS has traditionally not addressed. The document claims "P", and the evaluator concurs.

1.3.2 RADIUS Gateway Capability - The document [1] maintains that a RADIUS++ to RADIUS gateway is pretty much a tautology. The document claims "T", and the evaluator concurs.

1.3.3 Reject Capability - The document [1] maintains that RADIUS Proxy Servers, and potentially RADIUS++ Routing Brokers, have the ability to reject requests based on local policy. The document claims "T" and the evaluator concurs.

1.3.4 Preclude Layer 2 Tunneling - The document [1] indicates that [6] defines support for layer two tunneling in RADIUS. The document claims "T", and the evaluator concurs.

1.3.5 Reauth on Demand - The document [1] indicates that RADIUS provides this feature by means of the Session-Timeout and Termination- Action attributes. While this may, in fact, be sufficient to provide periodic re-authorization, it would not provide re- authorization on demand. The protocol [2] does not address this further. The document claims "P", and the evaluator awards "F".

1.3.6 Support for ACLs - The document [1] describes the attributes in RADIUS that are used to convey the access controls described in [3]. Certain of these (e.g. QoS) are not currently defined in RADIUS, but could easily be defined as new RADIUS attributes. The document claims "P", and the evaluator concurs.

1.3.7 State Reconciliation - The document [1] addresses each of the sub- items, as listed in the original AAA requirements document. In reviewing the document against the modified requirements of [3], there is still an issue with server-initiated state reconciliation messages. While the protocol [2] makes provision for such messages, as servers are allowed to initiate protocol dialogs, no detailed

message formats are provided. This is an area that has traditionally been a short coming of RADIUS. The document claims "P", and the evaluator awards "F".

1.3.8 Unsolicited Disconnect - Much of the discussion from the previous section applies to this section. The document [1] claims "F", and the evaluator concurs.

1.4 Accounting Requirements

1.4.1 Real Time Accounting - RADIUS Accounting is widely deployed and functions within the definition of real time contained in [3]. The document [1] claims "T", and the evaluator concurs.

1.4.2 Mandatory Compact Encoding - RADIUS Accounting contains TLVs for relevant accounting information, each of which is fairly compact. Note that the term "bloated" in [3] is somewhat subjective. The document [1] claims "T", and the evaluator concurs.

1.4.3 Accounting Record Extensibility - RADIUS Accounting may be extended by means of new attributes or by using the Vendor-Specific attribute. While it has been argued that the existing attribute number space is too small for the required expansion capabilities, the protocol [2] addresses this problem in section 3.0, and its subsections, of [2]. The document [1] claims "T", and the evaluator concurs.

1.4.4 Batch Accounting - RADIUS has no explicit provisions for batch accounting, nor does the protocol [2] address how this feature might be accomplished. The document [1] claims "F", and the evaluator concurs.

1.4.5 Guaranteed Delivery - RADIUS Accounting is widely deployed and provides guaranteed delivery within the context of the required application-level acknowledgment. The document [1] claims "T", and the evaluator concurs.

1.4.6 Accounting Timestamps - The document [1] indicates that this feature is specified in [4] as the Event-Timestamp attribute. The document claims [1] "T", and the evaluator concurs.

1.4.7 Dynamic Accounting - The document [1] indicates that this requirement is partially met using the accounting interim update message as specified in [4]. In addition, there was work in the RADIUS WG regarding session accounting extensions that has not been included in [4], i.e., some expired works in progress. The document claims [1] "P", and the evaluator concurs.

1.5 MOBILE IP Requirements

1.5.1 Encoding of MOBILE IP Registration Messages - The document [1] claims "F", and the evaluator concurs.

1.5.2 Firewall Friendly - The document [1] indicates that RADIUS deployment is know to have occurred in fire-walled environments. The document claims "T", and the evaluator concurs.

1.5.3 Allocation of Local Home Agent - The document [1] claims "F", and the evaluator concurs.

2. Summary Discussion

The document [1] and the protocol [2] suffer from having been written in a short time frame. While the protocol does provide specific guidance on certain issues, citing other relevant documents, it is not a polished protocol specification, with detailed packet format diagrams. There is a pool of prior work upon which the RADIUS++ protocol may draw, in that many of the concepts of Diameter were first postulated as works in progress within the RADIUS WG, in an attempt to "improve" the RADIUS protocol. All of these works in progress have long since expired, however.

3. General Requirements

RADIUS++ meets many of the requirements of an AAA protocol, as it is the current de facto and de jure standard for AAA. There are long-standing deficiencies in RADIUS, which have been well documented in the RADIUS and NASREQ WG proceedings. It is technically possible to revamp RADIUS to solve these problems. One question that will be asked, however, is: "What significant differences would there be between a finished RADIUS++ protocol and the Diameter protocol?".

4. Summary Recommendation

Recommended in part. What may possibly be learned from this submission is that it is feasible to have a more RADIUS-compliant RADIUS-compatibility mode in Diameter.

C.5 Diameter PRO Evaluation

Evaluation of Diameter against the AAA Requirements
PRO Evaluation
Evaluator - Basavaraj Patil

Ref [1] is "Diameter Framework Document".
Ref [2] is "Diameter NASREQ Extensions".
Ref [3] is the AAA evaluation criteria as modified by us.
Ref [4] is "Diameter Accounting Extensions".
Ref [5] is "Diameter Mobile IP Extensions".
Ref [6] is "Diameter Base Protocol".
Ref [7] is "Diameter Strong Security Extension".
Ref [8] is "Comparison of Diameter Against AAA Network Access Requirements".

The document uses T to indicate total compliance, P to indicate partial compliance and F to indicate no compliance.

Evaluator’s note : The Diameter compliance document [8] claims Total "T" compliance with all the requirements except : - 1.2.5 - 1.5.2

Section 1 - Per item discussion

1.1 General Requirements

1.1.1 Scalability

Diameter is an evolution of RADIUS and has taken into consideration all the lessons learned over many years that RADIUS has been in service. The use of SCTP as the transport protocol reduces the need for multiple proxy servers (Sec 3.1.1 Proxy Support of [1]) as well as removing the need for application level acks. The use and support of forwarding and redirect brokers enhances scalability. Evaluator concurs with the "T" compliance on this requirement.

1.1.2 Fail-over

Again with the use of SCTP, Diameter is able to detect disconnect indications upon which it switches to an alternate server (Sec 4.0 [6]). Also Requests and Responses do not have to follow the same path and this increases the reliability. Evaluator concurs with the "T" compliance on this requirement.

1.1.3 Mutual Authentication

The compliance document quotes the use of symmetric transforms for mutual authentication between the client and server (Sec 7.1 of [6]). The use of IPSec as an underlying security mechanism and thereby use the characteristics of IPSec itself to satisfy this requirement is also quoted. Evaluator concurs with the "T" compliance on this requirement.

1.1.4 Transmission Level Security

Although this requirement has been deprecated by the AAA evaluation team the document complies with it based on the definition (referring to hop-by-hop security). Section 7.1 of [6] provides the details of how this is accomplished in Diameter. Evaluator concurs with the "T" compliance on this requirement.

1.1.5 Data Object Confidentiality

This requirement seems to have come from Diameter. Ref [7] explains in detail the use of Cryptographic Message Syntax (CMS) to achieve data object confidentiality. A CMS-Data AVP is defined in [7]. Evaluator concurs with the "T" compliance on this requirement.

1.1.6 Data Object Integrity

Using the same argument as above and the hop-by-hop security feature in the protocol this requirement is completely met by Diameter. Evaluator concurs with the "T" compliance on this requirement.

1.1.7 Certificate Transport

Again with the use of the CMS-Data AVP, objects defined as these types of attributes allow the transport of certificates. Evaluator concurs with the "T" compliance on this requirement.

1.1.8 Reliable AAA Transport

Diameter recommends that the protocol be run over SCTP. SCTP provides the features described for a reliable AAA transport. Although the compliance is not a perfect fit for the definition of this tag item, it is close enough and the functionality achieved by using SCTP is the same. Evaluator concurs with the "T" compliance on this requirement.

1.1.9 Run over IPv4

Is an application layer protocol and does not depend on the underlying version of IP. Evaluator concurs with the "T" compliance on this requirement.

1.1.10 Run over IPv6

Is an application layer protocol and does not depend on the underlying version of IP. Evaluator concurs with the "T" compliance on this requirement.

1.1.11 Support Proxy and Routing Brokers

Section 3.1.1/2 of the framework document [1] provides an explanation of how Diameter supports proxy and routing brokers. In fact it almost appears as though the requirement for a routing broker came from Diameter. Evaluator concurs with the "T" compliance on this requirement.

1.1.12 Auditability

With the use of CMS-Data AVP [7] a trail is created when proxies are involved in the transaction. This trail can provide auditability. Evaluator concurs with the "T" compliance on this requirement.

1.1.13 Shared Secret Not Required

With the use of IPSec as the underlying security mechanism, Diameter does not require the use of shared secrets for message authentication. Evaluator concurs with the "T" compliance on this requirement.

1.1.14 Ability to Carry Service Specific Attributes

The base protocol [6] is defined by Diameter and any one else can define specific extensions on top of it. Other WGs in the IETF can design an extension on the base protocol with specific attributes and have them registered by IANA. Evaluator concurs with the "T" compliance on this requirement.

1.2 Authentication Requirements

1.2.1 NAI Support

The base protocol [6] defines an AVP that can be used to support NAIs. Diameter goes one step further by doing Message forwarding based on destination NAI AVPs. Evaluator concurs with the "T" compliance on this requirement.

1.2.2 CHAP Support

Reference [2] section 3.0 describes the support for CHAP. Evaluator concurs with the "T" compliance on this requirement.

1.2.3 EAP Support

Reference [2] section 4.0 describes the support for EAP. Evaluator concurs with the "T" compliance on this requirement.

1.2.4 PAP/Clear-text Passwords

Reference [2] section 3.1.1.1 describes the support for PAP. Evaluator concurs with the "T" compliance on this requirement.

1.2.5 Reauthentication on demand

The use of Session-Timeout AVP as the mechanism for reauthentication is claimed by the compliance document. However no direct references explaining this in the base protocol [6] document were found.

Evaluator deprecates the compliance on this to a "P"

Note: However this is a trivial issue.

1.2.6 Authorization w/o Authentication

Diameter allows requests to be sent without having any authentication information included. A Request-type AVP is defined in [2] and it can specify authorization only without containing any authentication. Evaluator concurs with the "T" compliance on this requirement.

1.3 Authorization Requirements

1.3.1 Static and Dynamic IP Addr Assignment

The base protocol includes an AVP for carrying the address. References [6.2.2 of 2] and [4.5 of 5] provide detailed explanations of how this can be done. Evaluator concurs with the "T" compliance on this requirement.

1.3.2 RADIUS Gateway Capability

One of the basic facets of Diameter is to support backward compatibility and act as a RADIUS gateway in certain environments. Evaluator concurs with the "T" compliance on this requirement.

1.3.3 Reject Capability

Based on the explanation provided in the compliance document for this requirement evaluator concurs with the "T" compliance on this requirement.

1.3.4 Preclude Layer 2 Tunneling

Ref [2] defines AVPs supporting L2 tunnels Evaluator concurs with the "T" compliance on this requirement.

1.3.5 Reauth on Demand

A session timer defined in [6] is used for reauthorization. However Diameter allows reauthorization at any time. Since this is a peer-to-peer type of protocol any entity can initiate a reauthorization request. Evaluator concurs with the "T" compliance on this requirement.

1.3.6 Support for ACLs

Diameter defines two methods. One that supports backward compatibility for RADIUS and another one with the use of a standard AVP with the filters encoded in it. Evaluator concurs with the "T" compliance on this requirement.

1.3.7 State Reconciliation

A long explanation on each of the points defined for this tag item in the requirements document. Evaluator concurs with the "T" compliance for this requirement.

1.3.8 Unsolicited Disconnect

The base protocol [6] defines a set of session termination messages which can be used for unsolicited disconnects. Evaluator concurs with the "T" compliance on this requirement.

1.4 Accounting Requirements

1.4.1 Real Time Accounting

Evaluator concurs with the "T" compliance based on explanations in [4].

1.4.2 Mandatory Compact Encoding

Use of Accounting Data Interchange Format (ADIF)-Record-AVP for compact encoding of accounting data. Evaluator concurs with the "T" compliance.

1.4.3 Accounting Record Extensibility

ADIF can be extended. Evaluator concurs with the "T" compliance.

1.4.4 Batch Accounting

Sec 1.2 of [4] provides support for batch accounting.

1.4.5 Guaranteed Delivery

Sections 2.1/2 of [4] describe messages that are used to guarantee delivery of accounting records. Evaluator concurs with the "T" compliance.

1.4.6 Accounting Timestamps

Timestamp AVP [6] is present in all accounting messages. Evaluator concurs with the "T" compliance.

1.4.7 Dynamic Accounting

Interim accounting records equivalent to a call-in-progress can be sent periodically. Evaluator concurs with the "T" compliance.

1.5 MOBILE IP Requirements

1.5.1 Encoding of MOBILE IP Registration Messages

Ref [5] provides details of how Diameter can encode MIP messages. Evaluator concurs with the "T" compliance.

1.5.2 Firewall Friendly

Some handwaving here and a possible way of solving the firewall problem with a Diameter proxy server. Document claims "T", evaluator deprecates it to a "P"

1.5.3 Allocation of Local Home Agent

Diameter can assign a local home agent in a visited network in conjunction with the FA in that network. Evaluator concurs with the "T"

Summary Recommendation

Diameter is strongly recommended as the AAA protocol. The experience gained from RADIUS deployments has been put to good use in the design of this protocol. It has also been designed with extensibility in mind thereby allowing different WGs to develop their own specific extension to satisfy their requirements. With the use of SCTP as the transport protocol, reliability is built in. Security has been addressed in the design of the protocol and issues that were discovered in RADIUS have been fixed. Diameter also is a session based protocol which makes it more scalable. The support for forwarding and redirect brokers is well defined and this greatly improves the scalability aspect of the protocol.

Lastly the protocol has been implemented by at least a few people and interop testing done. This in itself is a significant step and a positive point for Diameter to be the AAA protocol.

C.6 Diameter CON Evaluation

Evaluation of Diameter against the AAA Requirements
CON Brief
Evaluator: Barney Wolff

Section 1 - Per item discussion

1.1 General Requirements

1.1.1 Scalability - P (was T) The evaluator is concerned with scalability to the small, not to the large. Diameter/SCTP may prove difficult to retrofit to existing NAS equipment.

1.1.2 Fail-over - P (was T) SCTP gives an indication of peer failure, but nothing in any Diameter or SCTP document the evaluator was able to find even mentions how or when to switch back to a primary server to which communication was lost. After a failure, the state machines end in a CLOSED state and nothing seems to trigger exit from that state. It was not clear whether a server, on rebooting, would initiate an SCTP connection to all its configured clients. If not, and in any case when the communication failure was in the network rather than in the server, the client must itself, after some interval, attempt to re-establish communication. But no such guidance is given.

Of course, the requirement itself fails to mention the notion of returning to a recovered primary. That is a defect in the requirement. The evaluator has had unfortunate experience with a vendor's RADIUS implementation that had exactly the defect that it often failed to notice recovery of the primary.

1.1.3 Mutual Authentication - T

1.1.4 Transmission Level Security - T

1.1.5 Data Object Confidentiality - P (was T). Yes, the CMS data type is supported. But the work in progress, "Diameter Strong Security Extension", says:

> 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. 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.

Given all the fuss that has been made about "end-to-end" confidentiality (which really means "NAS-to-home_server"), the evaluator finds it absurd that the proposed solution is acknowledged to be unsuited to the NAS.

1.1.6 Data Object Integrity - P (was T). See above.

1.1.7 Certificate Transport - T

1.1.8 Reliable AAA Transport - T

1.1.9 Run over IPv4 - T

1.1.10 Run over IPv6 - T

1.1.11 Support Proxy and Routing Brokers - T

1.1.12 Auditability - T (based on our interpretation as non-repudiation, rather than the definition given in reqts)

1.1.13 Shared Secret Not Required - T

1.1.14 Ability to Carry Service Specific Attributes - T

1.2 Authentication Requirements

1.2.1 NAI Support - T

1.2.2 CHAP Support - T

1.2.3 EAP Support - T

1.2.4 PAP/Clear-text Passwords - T

1.2.5 Reauthentication on demand - P (was T). No mechanism was evident for the server to demand a reauthentication, based for example on detection of suspicious behavior by the user. Session-timeout is not sufficient, as it must be specified at the start.

1.2.6 Authorization w/o Authentication - T

1.3 Authorization Requirements

1.3.1 Static and Dynamic IP Addr Assignment - T

1.3.2 RADIUS Gateway Capability - P (was T). RADIUS has evolved from the version on which Diameter was based. EAP is a notable case where the convention that the Diameter attribute number duplicates the RADIUS one is violated. No protocol, not even RADIUS++, can claim a T on this.

1.3.3 Reject Capability - T (The evaluator fails to understand how any AAA protocol could rate anything other than T on this.)

1.3.4 Preclude Layer 2 Tunneling - T

1.3.5 Reauth on Demand - P (was T). As with reauthentication, there is no evident mechanism for the server to initiate this based on conditions subsequent to the start of the session.

1.3.6 Support for ACLs - P (was T). The evaluator finds the Filter-Rule AVP laughably inadequate to describe filters. For example, how would it deal with restricting SMTP to a given server, unless all IP options are forbidden so the IP header length is known? No real NAS could have such an impoverished filter capability, or it would not survive as a product.

1.3.7 State Reconciliation - P (was T). It is difficult for the evaluator to understand how this is to work in a multi-administration situation, or indeed in any proxy situation. Furthermore, SRQ with no session-id is defined to ask for info on all sessions, not just those "owned" by the requester.

1.3.8 Unsolicited Disconnect - T

1.4 Accounting Requirements

1.4.1 Real Time Accounting - T

1.4.2 Mandatory Compact Encoding - T

1.4.3 Accounting Record Extensibility - T

1.4.4 Batch Accounting - P (was T). The evaluator suspects that simply sending multiple accounting records in a single request is not how batch accounting should or will be done.

1.4.5 Guaranteed Delivery - T

1.4.6 Accounting Timestamps - T (The evaluator notes with amusement that NTP time cycles in 2036, not 2038 as claimed in the Diameter drafts. It’s Unix time that will set the sign bit in 2038.)

1.4.7 Dynamic Accounting - T

1.5 MOBILE IP Requirements

1.5.1 Encoding of MOBILE IP Registration Messages - T

1.5.2 Firewall Friendly - F (was T). Until such time as firewalls are extended to know about or proxy SCTP, it is very unlikely that SCTP will be passed. Even then, the convenient feature of being able

to send a request from any port, and get the reply back to that port, means that a simple port filter will not be sufficient, and statefulness will be required. Real friendship would require that both source and dest ports be 1812.

1.5.3 Allocation of Local Home Agent - T

2. Summary Discussion

In some areas, Diameter is not completely thought through. In general, real effort has gone into satisfying a stupendous range of requirements.

3. General Requirements

Diameter certainly fails the KISS test. With SCTP, the drafts add up to 382 pages - well over double the size of RADIUS even with extensions. The evaluator sympathizes with the political instinct when faced with a new requirement no matter how bizarre, to say "we can do that" and add another piece of filigree. But the major places where Diameter claims advantage over RADIUS, namely "end-to-end" confidentiality and resource management, are just the places where some hard work remains, if the problems are not indeed intractable.

More specifically, the evaluator sees no indication that specifying the separate transport protocol provided any advantage to defray the large increase in complexity. Application acks are still required, and no benefit from the transport acks was evident to the evaluator. Nor was there any obvious discussion of why "sequenced in-order" delivery is required, when AAA requests are typically independent. SCTP offers out-of-order delivery, but Diameter seems to have chosen not to use that feature.

Whether TLV encoding or ASN.1/BER is superior is a religious question, but Diameter manages to require both, if the "strong" extension is implemented. The evaluator has a pet peeve with length fields that include the header, making small length values invalid, but that is a minor point.

Finally, interoperability would be greatly aided by defining a standard "dictionary" format by which an implementation could adopt wholesale a set of attributes, perhaps from another vendor, and at least know how to display them. That is one of the advantages of MIBs.

4. Summary Recommendation

Diameter is clearly close enough to meeting the myriad requirements that it is an acceptable candidate, though needing some polishing. Whether the vast increase in complexity is worth the increase in functionality over RADIUS is debatable.

C.7 COPS PRO Evaluation

Evaluation of COPS AAA Requirements
PRO Evaluation
Evaluator - David Nelson

Ref [1] is "Comparison of COPS Against the AAA NA Requirements", work in progress, a.k.a. 'the document'
Ref [2] is RFC 2748 a.k.a. 'the protocol'
Ref [3] is the AAA evaluation criteria as modified by us.
Ref [4] is "AAA Protocols: Comparison between RADIUS, Diameter, and COPS" work in progress.
Ref [5] is "COPS Usage for AAA", work in progress.

This document uses T to indicate total compliance, P to indicate partial compliance and F to indicate no compliance.

Section 1 - Per item discussion

1.1 General Requirements

1.1.1 Scalability - The document [1] claims "T", and the evaluator concurs.

1.1.2 Fail-over - The document [1] claims "T", and the evaluator concurs.

1.1.3 Mutual Authentication - The document claims "T", and the evaluator concurs.

1.1.4 Transmission Level Security - The document [1] indicates that transmission layer security, as defined in [3], is provided in the protocol, using the mechanisms described in [2]. It should be noted that this requirement is now a SHOULD in [3]. The document claims "T", and the evaluator concurs.

1.1.5 Data Object Confidentiality - The document [1] indicates that end-to-end confidentiality is provided using a CMS-data attribute, based in large part upon RFC 2630. The evaluator has not, at this time, investigated the applicability of RFC 2630 to the AAA work. The document claims "T", and the evaluator concurs.

1.1.6 Data Object Integrity - The document [1] indicates that data object integrity is provided using a CMS-data attribute, based in large part upon RFC 2630. The evaluator has not, at this time, investigated the applicability of RFC 2630 to the AAA work. The document claims "T", and the evaluator concurs.

1.1.7 Certificate Transport - The document [1] indicates that certificate transport is provided using a CMS-data attribute, based in large part upon RFC 2630 and RFC 1510. The evaluator has not, at this time, investigated the applicability of RFC 2630 to the AAA work. The document claims "T", and the evaluator concurs.

1.1.8 Reliable AAA Transport - The document [1] indicates that COPS uses TCP, which certainly meets the requirements for a reliable transport. The document claims "T", and the evaluator concurs.

1.1.9 Run over IPv4 - The document [1] claims "T", and the evaluator concurs.

1.1.10 Run over IPv6 - The document [1] claims "T", and the evaluator concurs.

1.1.11 Support Proxy and Routing Brokers - Reasonable detail of proxy operations is provided in [5]. The document [1] claims "T", and the evaluator concurs.

1.1.12 Auditability - The document [1] alludes to a History PIB that would enable auditing without explaining how it would work. The AAA Extension [5] does not provide additional insight. The document claims "T", and the evaluator awards "P".

1.1.13 Shared Secret Not Required - The document [1] claims "T" and the evaluator concurs.

1.1.14 Ability to Carry Service Specific Attributes - The document [1] claims "T", and the evaluator concurs.

1.2 Authentication Requirements

1.2.1 NAI Support - The document [1] indicates that NAI is to be supported in the Information Model, but notes that for cases where certificates are in use, the more restrictive syntax of RFC 2459 applies. The document claims "T", and the evaluator awards "P".

1.2.2 CHAP Support - The document [1] claims "T", and the evaluator concurs.

1.2.3 EAP Support - The document [1] claims "T", and the evaluator concurs.

1.2.4 PAP/Clear-text Passwords - The document [1] indicates compliance, presumably using a CMS-data attribute, based in large part upon RFC 2630. The evaluator has not, at this time, investigated the applicability of RFC 2630 to the AAA work. The document claims "T", and the evaluator concurs.

1.2.5 Reauthentication on demand - The document [1] claims "T", and the evaluator concurs.

1.2.6 Authorization w/o Authentication - This requirement, as applied to the protocol specification, mandates that non- necessary authentication credentials not be required in a request for authorization. The actual decision to provide authorization in the absence of any authentication resides in the application (e.g. AAA server). The document [1] claims "T", and the evaluator concurs.

1.3 Authorization Requirements

1.3.1 Static and Dynamic IP Addr Assignment - The document [1] claims "T", and the evaluator concurs.

1.3.2 RADIUS Gateway Capability - The document [1] claims "T", and in the absence of any detailed discussion of how this is accomplished, in either [1] or [5], the evaluator awards "P".

1.3.3 Reject Capability - The document claims [1] "T" and the evaluator concurs.

1.3.4 Preclude Layer 2 Tunneling - The document [1] claims "T", and in the absence of any detailed discussion of how this is accomplished, in either [1] or [5], the evaluator awards "P".

1.3.5 Reauth on Demand - The document [1] claims "T", and the evaluator concurs.

1.3.6 Support for ACLs - The document [1] "T", and the evaluator concurs.

1.3.7 State Reconciliation - The document [1] "T", and the evaluator concurs.

1.3.8 Unsolicited Disconnect - The document [1] claims "T", and the evaluator concurs.

1.4 Accounting Requirements

1.4.1 Real Time Accounting - The document [1] claims "T", and the evaluator concurs.

1.4.2 Mandatory Compact Encoding - Note that the term "bloated" in [3] is somewhat subjective. The document [1] claims "T", and the evaluator concurs.

1.4.3 Accounting Record Extensibility - The document [1] claims "T", and the evaluator concurs.

1.4.4 Batch Accounting - The protocol [2] [5] does not address how in detail this feature might be accomplished. The document [1] claims "T", and the awards "P".

1.4.5 Guaranteed Delivery - Guaranteed delivery is provided by TCP. The document [1] claims "T", and the evaluator concurs.

1.4.6 Accounting Timestamps - The document [1] claims "T", and the evaluator concurs.

1.4.7 Dynamic Accounting - The document [1] claims "T", and the evaluator concurs.

1.5 MOBILE IP Requirements

1.5.1 Encoding of MOBILE IP Registration Messages - The document [1] claims "T", and the evaluator concurs.

1.5.2 Firewall Friendly - The document [1] claims "T", and the evaluator concurs.

1.5.3 Allocation of Local Home Agent - The document [1] claims "T", and the evaluator concurs.

2. Summary Discussion

It may appear, upon initial inspection, that the evaluator has not lent a critical eye to the compliance assertions of the document [1]. First, this memo is a "PRO" brief, and as such reasonable benefit of doubt is to be given in favor of the protocol submission. Second, there is a fundamental conceptual issue at play. The COPS-PR model provides a sufficient set of basic operations and commands, a stateful model, the ability for either "peer" to initiate certain kinds of requests, as well as an extensible command set, to be able to support a wide variety of network and resource management protocols. The details of protocol specific messages is left to

Policy Information Base (PIB) data objects. Since no AAA PIB has been written, the evacuator can only (optimistically) assess the inherent capabilities of the base protocol to accomplish the intended requirements of [3], given a reasonable set of assumptions about what an AAA PIB might look like.

In some sense, this akin to asserting that a given algorithm can be correctly implemented in a specific programming language, without actually providing the code.

The PIB model used by COPS is a powerful and flexible model. The protocol document [5] spends a considerable amount of time enumerating and describing the benefits of this data model, and explaining its roots in Object Oriented (OO) design methodology. Analogies are made to class inheritance and class containment, among others. It’s always hard to say bad things about OO.

3. General Requirements

COPS-AAA would appear to meet (totally or partially) all of the requirements of [3], at least as can be determined without the benefit of an AAA PIB.

4. Summary Recommendation

Recommended with reservation. Before final acceptance of COPS-AAA, someone is going to have to write the AAA PIB and evaluate its details.

C.8 COPS CON Evaluation

Evaluation of COPS against the AAA Requirements
CON Evaluation
Evaluator - David Mitton

The Primary document discussed here is [COPSComp] and the arguments therein based on the proposal [COPSAAA].

[COPSComp] "Comparison of COPS Against the AAA NA Requirements", Work in Progress.
[COPSAAA] "COPS Usage for AAA", Work in Progress.
[EksteinProtoComp] "AAA Protocols: Comparison between RADIUS, Diameter, and COPS", Work in Progress.

References: (in order of relevancy)

[COPSBase] Durham, D., Boyle, J., Cohen, R., Herzog, S., Rajan, R. and A. Sastry, "The Common Open Policy Service Protocol", RFC 2748, January 2000.

[COPSFwork] Yavatkar, R., Pendarakis, D. and R. Guerin, "A Framework for Policy-based Admission Control", RFC 2753, January 2000.

[COPSPR] "COPS Usage for Policy Provisioning", Work in Progress.

[COPSSPPI] "Structure of Policy Provisioning Information (SPPI)", Work in Progress.

[COPSCMS] "COPS Over CMS", Work in Progress.

[COPSTLS] "COPS Over TLS", Work in Progress.

[COPSGSS] "COPS Extension for GSS-API based Authentication Support", Work in Progress.

Other COPS & RSVP RFCs & drafts not listed as not directly relevant.

Compliance: T==Total, P==Partial, F=Failed

Section 1 - Per item discussion

Initial Note: [COPSComp] claims "unconditional compliance" with all requirements.

1.1 General Requirements

1.1.1 Scalability - P (was T) The evaluator is concerned with scalability of many always-on TCP connections to a server supporting a lot of clients, particularly with the heartbeat messages. The claim that the request handle is "unbounded" sounds fishy.

1.1.2 Fail-over - P (was T) COPS gives an indication of peer failure, and has mechanisms to restart state, but there seems to be a bias toward a single state server. COPS has decided that synchronizing state between multiple hot servers is out of scope.

Because COPS uses TCP, it is at the mercy of the TCP timers of the implementation which can be significant. Connection timeout reporting to the application may be delayed beyond the client authentication timeouts. Tuning the Keep-Alive message to a tighter period will increase the session and system overhead.

1.1.3 Mutual Authentication - P (was T) The explanation is sort of for message object integrity. It does not describe authentication techniques. The evaluator assumes that COPS peers would authenticate each other at Client-Open time. But cannot understand how this would work if proxies are involved.

1.1.4 Transmission Level Security - T

1.1.5 Data Object Confidentiality - T Seems almost a carbon copy of the Diameter capabilities. This evaluator echoes the high overhead concerns of the Diameter evaluator for the CMS capability. TLS is not mentioned here, but is piled on later.

1.1.6 Data Object Integrity - T See above.

1.1.7 Certificate Transport - T

1.1.8 Reliable AAA Transport - T (maybe P) COPS meets this requirement as well as any other protocol we've evaluated. That is it does have one application level ACK. Statements such as "TCP provides guaranteed delivery" are incorrect. COPS does attempt to identify outages by using a keep-alive message between TCP peers.

1.1.9 Run over IPv4 - T

1.1.10 Run over IPv6 - T

1.1.11 Support Proxy and Routing Brokers - P (was T) How client types are supported forward is not well understood by this evaluator. Does each client type require the Broker to make a different client Open request to it's upstream servers? What about routing brokers?

1.1.12 Auditability - P (was T) (based on our interpretation as non-repudiation, rather than the definition given in reqts) The explanation of a History PIB is incomplete and therefore inconclusive.

1.1.13 Shared Secret Not Required - T Except this clause in [COPSAAA] 6.2 page 14 "COPS MUST be capable of supporting TLS"

1.1.14 Ability to Carry Service Specific Attributes - P (was T)

a) COPS only allows a small number of unique objects to be added. 256 Object "classes" or types, with 256 subtypes or versions. Client types are 16 bits long, where the high bit indicates "enterprise" specific values. But pertain to a COPS peer-

connection session. The client type seems to just identify the information model for the message. eg. it will be fixed to one value for AAA.

b) Service specific objects are not the same as Vendor Specific Objects. They pertain to objects within a client type.

c) The PIB model leads to a different model interoperability. Because most vendor product differ in some way, each PIB will be different, and sharing common provisioning profiles will be a rather difficult mapping problem on the server.

d) It's not clear the different client types can be mixed or that other objects definitions can be used from other defined client types. It's really unclear how the client type of a connection propagates in a proxy situation.

1.2 Authentication Requirements

1.2.1 NAI Support - T The requirement that RFC 2459 (X.509 profiles) be met presumes that Auth servers would not have a mapping or local transformation.

1.2.2 CHAP Support - T An Information Model is being invoked, which I don't see really fleshed out anywhere. [COPSAAA] does a bit of handwaving and definitions but doesn't deliver much meat. Nonetheless, this could be handled ala RADIUS.

1.2.3 EAP Support - P (was T) Again with the non-existent Information Model. To do EAP, this evaluator thinks another Request or Decision type is needed here to indicate to proxies that an extended message exchange is in progress.

1.2.4 PAP/Clear-text Passwords - T

1.2.5 Reauthentication on demand - T

1.2.6 Authorization w/o Authentication - T

The comment "Please note: with existing algorithms, any authorization scheme not based on prior authentication is meaningless" is meaningless out of application context.

1.3 Authorization Requirements

1.3.1 Static and Dynamic IP Addr Assignment - T

1.3.2 RADIUS Gateway Capability - P (was T). It would be interesting to see RADIUS attributes wrapped in some COPS "Information Model".

1.3.3 Reject Capability - T

1.3.4 Preclude Layer 2 Tunneling - T

More work for the "Information Model" author!

1.3.5 Reauthorization on Demand - T

1.3.6 Support for Access Rules & Filters - P (was T) Yet more work for the "Information Model" author, including some design issues which alluded the RADIUS and Diameter designers. At least an attempt was made in Diameter. There is nothing here.

1.3.7 State Reconciliation - P (was T). It is difficult for the evaluator to understand how well the COPS mechanisms work in a multi-administration situation, or in any proxy situation. Multi-server coordination, if allowed, seems to be lacking a description.

1.3.8 Unsolicited Disconnect - T

1.4 Accounting Requirements

1.4.1 Real Time Accounting - T

1.4.2 Mandatory Compact Encoding - T This evaluator does not believe that ADIF is a compact format. But does believe that the Information Model author can design a PIB with accounting statistics that will satisfy this requirement.

1.4.3 Accounting Record Extensibility - P (was T) By defining a vendor/device specific PIB for additional elements.

1.4.4 Batch Accounting - P (was T) Offered description does not seem to match the requirement.

1.4.5 Guaranteed Delivery - P (was T) TCP does NOT "guarantee delivery", only application Acks can do that. If these acks can be generated similar to the description here, then this requirement is met.

1.4.6 Accounting Timestamps - T Another item for the "Information Model" author.

1.4.7 Dynamic Accounting - T Event and interim accounting can be supported.

1.5 MOBILE IP Requirements

1.5.1 Encoding of MOBILE IP Registration Messages - P (was T) Yet more work for the "Information Model" author. Hope he can handle it.

1.5.2 Firewall Friendly - P (was T) I guess. Because it uses TCP and can be identified by known connection port. But there is an issue with respect to the impact level of mixed COPS traffic coming through a common firewall port.

1.5.3 Allocation of Local Home Agent - P (was T) Just add another element to that "Information Model" definition.

2. Summary Discussion

COPS was designed to do some things similar to what we want and be somewhat flexible, but with a totally different set of assumptions on how many clients and requests would be funneled through the infrastructure and the acceptable overhead. This evaluator is not sure that it scales well to the fast evolving access market where every product doesn’t implement a small set of common features, but a large set of overlapping ones.

3. General Requirements

COPS started out with small and easily met set of design goals for RSVP and DiffServe, and is evolving as a new hammer to hit other nails [COPSPR]. As COPS implementors get more operational experience, it is interesting to see more reliability fixes/features quickly get patched in.

Understanding COPS requires that you read a number RFCs and drafts which do not readily integrate well together. Each application of COPS has spawned a number of drafts. It’s not clear if one wants to or can implement a single COPS server that can service AAA and other application clients.

The COPS authors seem to overly believe in the goodness of TCP, and rely on it to solve all their transport problems, with concessions to application keep-alive messages to probe the connection status and sequence numbers to prevent replay attacks. This evaluator believes this type of approach may work for many networks but really doesn’t

scale well in larger configurations. End-to-end application acks are the only guaranteed delivery solution, particularly where distributed state is involved.

COPS falls into an in between place on encoding. It has small number of simple data object blobs which are concatenated ala RADIUS/Diameter TLVs to form a flexible message layout. However, they attempt to limit the number of objects by making them arbitrarily complex ala SNMP MIBs, and defining yet another data structuring language for these PIBs. There is a lot of computer science style grandstanding in [COPSAAA] Section 1.2, but no translation into how a set of data objects can be used to meet these wonderful features in operation. (or even if we needed them) This will be the crux of the interoperability issue. RADIUS implementations interoperate because they at least, understand a common set of functional attributes from the RFCs. And vendor extent ions can be simply customized in as needed via dictionaries. If PIB definitions are needed for every piece and version of access equipment, before you can use it, then the bar for ease of configuration and use has been raised quite high.

Support for PIB definition and vendor extensions will be on the same order as MIB integration in SNMP management products and put the supposed complexity of Diameter to shame.

4. Summary Recommendation

COPS has a structure that could be made to serve as a AAA protocol, perhaps by just copying the features of RADIUS and Diameter into it. The author of [COPSAAA] and [COPSComp] has not done the whole job yet and some of the missing pieces are vexing even for those already in the field.

While some of the synergy with other COPS services is attractive, this evaluator is concerned about the liabilities of combining AAA services with the new emerging COPS applications in a single server entity will introduce more complexity than needed and opportunities to have progress pulled into other rat-holes. (eg. Policy Frameworks)

Appendix D - Meeting Notes

The minutes of the team meetings as recorded by various members.

D.1 Minutes of 22-Jun-2000 Teleconference

Recorded by: Mark Stevens

Arguments for and against SNMP as an AAA protocol were given. Stuart Barkley gave a summary of the pro argument. Mike St. Johns gave a summary of the con argument. Dave Nelson asked for "instructions to the jury" in an effort to determine what evidence could and could not be used in making decisions.

The AAA evaluation criteria is weak in some areas and in others it appears to be written with what might be interpreted as undue influence from the NASREQ working group.

Mike St. Johns offered that we must restrict ourselves to considering only the evidence provided in the compliance documents and any supporting documents to which they may refer.

In summary: AAA evaluation criteria document, AAA evaluation criteria source documents, protocol response documents and reference documents.

The question as to what the group should do with malformed requirements came up. The consensus seemed to be that we would use the requirements as adjusted in our last meeting where the requirements made no sense.

The floor was then given to Stuart Barkley for the pro SNMP argument.

Highlights:

* In most areas the requirements are met by SNMP.
* Confidentiality and Certificate transport mechanisms may be weak, but workable.
* With regard to Authentication, every technique can be supported although support for PAP or cleartext passwords is weak.
* With regard to Authorization, there is nothing in the requirements that cannot be supported.
* Accounting everything supported, although there is no specific consideration for compact encoding. SNMP not as bloated as ASCII or XML based encoding schemes. Requirement for compact encoding weakly indicated in requirements anyway. Server-specific attributes needed, but compact encoding preclude w/o tradeoffs.

* With regard to mobile IP requirement, everything works well, although firewall friendliness is a judgment call.
* Proxy mechanisms of SNMPv3 mitigates problems w/ firewalls.
* Scalability is ok.
* Overall, meets most requirements and shortfalls are minor.
* In some cases requirements seemed to expressed in a manner that "stacks" the odds against SNMP.
* SNMP is deployed everywhere already.

* The protocol has a well-understood behavior despite the tedium of MIB definition, so it has the advantage of not requiring the creation of a new infrastructure.
* AAA response document is silent on architecture and MIB definition, but there is too much work to do at this stage of evaluation. Not having done the MIB definitions and architecture is not a limitation of the protocol.
* SNMP is a good candidate.

Mike St. Johns took the floor to give a summary of the con argument.

* Neither the requirements, core documents nor response document specify the mechanism of operation.
* Liberties were taken in the assertion that the server to server interaction requirements were met.
* The scaling arguments are weak.
* Fail-over arguments are weak.
* Security aspects work well with the manager/server paradigm, but not well in bidirectional interactions among peers.
* The authentication requirements not understood by authors of the response document. * SNMP is just data moving protocol.
* Message formats not specified.
* What is the method for supporting authentication? Storing the information is handled, but what do the nodes do with it?

* The protocol certainly shined in the area of meeting accounting requirements.
* Although SNMP could certainly play a role in the accounting space, it is unusable in the areas of Authorization and Authentication.
* The response document does not address how the problem will be solved.
* It does not address the scalability issues that may arise in the transition from a manager-agent mode of operation to a client-server model.

The group then examined each requirement against SNMP in a line-by-line exercise.

D.2 Minutes of 27-Jun-2000 Teleconference

Attendees - All (Mike St. John, Dave Mitton, Dave Nelson, Mark Stevens, Barney Wolff, Stuart Barkley, Steven Crain, Basavaraj Patil)

Minutes recorded by : Basavaraj Patil

Evaluation of RADIUS++ AAA Requirements

Pro : Mark Stevens
Con : Dave Nelson

- Question raised on if all meetings held so far have been recorded. Last week's meeting was recorded by Mark. Previous meetings have been recorded by Mike. All of these minutes should be available in the archive.

- Dave Nelson mentioned that Pat Calhoun has responded on the AAA WG mailing list to the changes made to the requirements document by the evaluation team. Pat's response includes arguments for inclusion of some of the requirements that were deleted by the eval team.

- Mike concluded that we can reinstate these requirements after reviewing Pat's comments in detail and the RFCs referenced. The intent is to take Pat's comments/document and review it between now and next Thursday (July 6th) and integrate the comments based on the findings at that time.

Voting Procedure for evaluation : No voting during the discussion. All votes MUST be submitted to Mike by COB, June 28th, 00.

- Dave Nelson's summary of the Con statement for RADIUS++.
  Overview of the points on which the evaluator disagrees with the compliance statement.

  Conclusion from Dave : Not recommended (Details in the con statement).

  Q: Is it possible to use it for accounting?
  A: Authentication and Authorization could be separated, but Accounting is the weak link in this protocol and hence is not suitable.

- Mark Steven's summary of the Pro statement
  Agreed with most of the observations made by Dave Nelson. The biggest thing going for it is that it has been running in this environment for a while and it does meet most of the requirements

in the document. Transition will be easy and backwards compatibility is a key plus point.

Point-by-point Discussion:

General (1.1):

1.1.1 Scalability

BW - There is no actual limit on the number of outstanding requests. The protocol itself does not limit the number.

DN -Simultaneous requests is not the same as outstanding requests.

Discussion of workarounds that have been implemented to overcome this problem.

1.1.2 Fail-over

DN - This is an application layer protocol and uses application level time-outs to provide fail-over solutions. Analogy and discussion on the use of round-trip-timer in TCP.

Example of how robust a network can be based on a machine at MIT that was decommissioned and a new one with the same name installed in the network.

Discussion of environments where proxies for primary, secondary and tertiaries exist and the possible effect of flooding messages in the event of a fail-over detection.

1.1.3 Mutual Authentication

No Discussion. Accepted as stated.

1.1.4 Transmission level security

This requirement was deleted from the list by the evaluation team. It was deleted because it is an overgeneralization of Roam Ops.

DN - There is a concern regarding what this really means. Referred to what Pat is saying about this on the list and the need for it to be reinstated.

Suggestion to change the tag in the requirements document to hop-by-hop security.

Does the Roamops group use transmission level security to imply hop-by-hop security?

1.1.5 Data Object Confidentiality

Mike explained the concept of Cryptographic Message Syntax (CMS - RFC2630). There are some issues regarding the use of CMS at an end point. Symmetric or Asymmetric keys can be used.

There does not seem to be a problem with the suggested usage of CMS in RADIUS++.

1.1.6/7 Data Object Integrity/Certificate Transport

No discussion. (I guess everyone concurs with the statement in the compliance document and the reviewers comments).

1.1.8 Reliable AAA Transport

BW - Radius provides reliability at the application layer by doing retransmissions. So why is there a need for a reliable AAA transport protocol?

- Is it packet loss that the protocol needs to be concerned about?

DN - This requirement is tied to the failover issue. Explanation of the negative impact of retransmissions in a network, especially in the case of a web of proxies.

Conclusion is that this requirement deals with packet loss.

1.1.9/10 Run over IPv4/6

Running over IPv6 should be a trivial issue.

1.1.11 Support Proxy and Routing Brokers

- Discussion on what this requirement means and analogy to DNS servers in a network.

- RADIUS can be extended to support this requirement and from the compliance document this does not appear to be fully cooked yet.

1.1.12 Auditability

No Discussion

1.1.13 Shared Secret Not Required

This seems to be a trivial issue to be addressed in RADIUS++.

1.1.14 Ability to carry Service Specific Attributes

No Discussion

Authentication Requirements:

1.2.1 NAI Support

Trivial - Total compliance.

1.2.2 CHAP Support

Comment : RADIUS support of CHAP could be better and the response needs to be encrypted.

1.2.3/4 EAP/PAP

No Discussion

1.2.5 Reauthentication on Demand

DN - Document claims that the server can reauthenticate by issuing an Access-challenge. There is a change to the state machine and the suggested solution is too simplistic. Also backwards compatibility would be an issue.

1.2.6 Authorization w/o Authentication

DN - This is trivial to fix, but this is not mentioned in the compliance document.

Authorization Requirements:

1.3.1 Static and Dynamic IP Addr assignment

- RADIUS does not rise to the demands of being a resource manager
- RADIUS assigns an address and it stays assigned for the session. There is no concept of leasing.

1.3.2 RADIUS Gateway Capability

This is a requirement written that is not applicable to RADIUS itself.

1.3.3/4/5/6/7/8

Call dropped. Somebody else needs to fill in here. (Mike ????)

Accounting Requirements:

1.4.1 Real time accounting

No dissent. No discussion

1.4.2 Mandatory compact encoding

Comment made regarding ASN.1 and XML in this context

1.4.3 Accounting Record Extensibility

No discussion

1.4.4 Batch Accounting

No specific wording in the document to show how this can be done. Basically it is real time accounting without the real time constraint.

It may be a trivial issue.

1.4.5/6 Guaranteed Delivery/Accounting Timestamps

No Discussion

1.4.7 Dynamic Accounting

There is ongoing discussion in the AAA WG on this requirement. The RADIUS WG is also discussing this (comment). The idea here is to be able to send the equivalent of a phonecall in progress type of messages.

Mobile IP Requirements:

1.5.1 Encoding of Mobile IP Reg. Messages

May be trivial. Discussion on what this requirement really is. Is it just the ability to carry the reg. message as payload? Does the AAA protocol have to delve into the reg. message and behave differently.

1.5.2 Firewall Friendly

No Discussion

1.5.3 Allocation of Local Home Agents

This concept needs to be clarified as the author writing the compliance statement did not understand it either.

If you notice anything that I recorded here as something misinterpreted, please feel free to make corrections.

D.3 Minutes of 29-Jun-2000 Teleconference

Attendees: Mike St. John, Dave Mitton, Dave Nelson, Barney Wolff, Stuart Barkley, Steven Crain, Basavaraj Patil.
Missing: Mark Stevens.

Minutes recorded by: Stuart Barkley

Evaluation of Diameter AAA Requirements

Advocates:

Pro: Basavaraj Patil
Con: Barney Wolff

Summary discussion:

PRO summary (Basavaraj Patil):

session based
lightweight base + extensions
has implementation experience
based upon radius
fixes specific problems with radius,
interoperates with radius
looks like requirements are written for diameter

CON summary (Barney Wolff):

meets most needs, designed with requirements in mind

issues: scalability in small devices (strong crypto specifically)

failover (need guidance on failover recovery procedures)

Data object confidentiality has been expressed as very important, diameter glosses over it referring to rfc2630, cost to run on NAS device

ACL: filter style syntax seems inadequate

state reconciliation: difficult over global multiple administrative domains

batch accounting: implementation doesn't meet intended need

firewall friendly: until firewalls support SCTP will be failure

summary very close

concerns:

size and complexity needs almost all extensions to actually support needs separation of SCTP and data (as per IESG suggestion?) application vs transport acks

Point-by-point Discussion:

General (1.1):

1.1.1 Scalability

Handles large number of requests

SCTP reduces proxy needs (how? what is justification for this statement?)

Scalability in large

1.1.2 Fail-over

Recovery from SCTP failure needs discussion (Note to DM: Include in final document considerations)

1.1.3 Mutual Authentication

No Discussion

1.1.4 Transmission level security

No Discussion

1.1.5/6 Data Object Confidentiality/Data Object Integrity

Crypto in NAS
NAS needs knowledge of when to use crypto
One Time Passwords

1.1.7 Certificate Transport

No Discussion

1.1.8 Reliable AAA Transport

No Discussion

1.1.9/10 Run over IPv4/6

No Discussion

1.1.11 Support Proxy and Routing Brokers

No Discussion

1.1.12 Auditability

No Discussion

1.1.13 Shared Secret Not Required

No Discussion

1.1.14 Ability to carry Service Specific Attributes

No Discussion

Authentication Requirements:

1.2.1 NAI Support

No Discussion

1.2.2 CHAP Support

No Discussion

1.2.3/4 EAP/PAP

No Discussion

1.2.5 Reauthentication on Demand

No Discussion

1.2.6 Authorization w/o Authentication

No Discussion

Authorization Requirements:

1.3.1 Static and Dynamic IP Addr assignment

No Discussion

1.3.2 RADIUS Gateway Capability

Protocol requirement or implementation/application requirement?
Which RADIUS versions are to be supported? Which subset?

1.3.3 Reject Capability

No Discussion

1.3.4 Preclude L2TP

No Discussion

1.3.5 Reauthorize on demand

Raj to look at this again

1.3.6 Support for ACLs

Standardizes syntax not semantics.
Standardizes semantics in NASREQ extension, but is very weak

1.3.7 State reconciliation

Appears to be weak in that server must "query the world" to restore its state
Just in time reconciliation
Simultaneous usage limitations
More discussion needed

1.3.8 Unsolicited disconnect

No Discussion

Accounting Requirements:

1.4.1 Real time accounting

No Discussion

1.4.2 Mandatory compact encoding

Is ADIF compact?
Is ADIF UTF-8 compatible?

1.4.3 Accounting Record Extensibility

No Discussion

1.4.4 Batch Accounting

Diameter okay for small batches. Specification doesn't seem suitable for large batch transfers (100,000+ records)

1.4.5 Guaranteed Delivery

No Discussion

1.4.6 Accounting Timestamps

No Discussion

1.4.7 Dynamic Accounting

No Discussion

Mobile IP Requirements:

1.5.1 Encoding of Mobile IP Reg. Messages

Taken of faith

1.5.2 Firewall Friendly

Issues with SCTP being supported initially through firewalls

1.5.3 Allocation of Local Home Agents

Still lack of understanding of the AAA protocol requirements here (versus just being a roaming attribute)

Overall summary:

Diameter seems to meet most requirements and is a likely candidate to support AAA requirements.

Other matters:

Votes on Diameter should be in by Sunday evening. Same format as before. Mike will tally up as both majority and average votes.

Should different requirements have different weight?

Possibility of SNMP reconsideration as per ADs? To close off our task in timeframe allocated, should not reopen submissions or discussions. Could cause to drag on for long time causing us to miss our July 15 date.

Possibility of needing a few extra days to finish report due to editing and review needs of the group. Mike to ask ADs to consider slight time extension possibility.

"No discussion" means that the topic was mentioned but there we no objections/issues raised on that requirement being met.

These are based upon my notes. Please send any corrections to the list.

D.4 Minutes of 06-Jul-2000 Teleconference

Minutes of AAA-Team Telecon 7/6/00
By: Barney Wolff

Pro review of COPS - Dave Nelson

Likes the object model.
No apparent showstoppers.
Will resend review with typos corrected.

Con review of COPS - Dave Mitton

Architecture is mostly there.
Strong dependency on info model, sceptical of object model.
Problem with info model in multi-vendor, multi-administration environment.
How does server speak to multiple client flavors?
Will resend review with typos corrected.

Comment by Mike StJ "replace SNMP with COPS" - :) I think.

Per-Item discussion

1.1.1 Scalability - concern re always-on TCP. Direction to DM - add general issue of number of connections.

1.1.2 Failover - No hot backup, but true of all protocols. (ie, no explicit mention of server-server protocol that might keep a backup server in sync so it could take over instantly.)

1.1.3 Mutual Authentication - perhaps relies on TLS. Draft does not otherwise support this.

1.1.8 Reliable AAA Transport - TCP + appl heartbeat.

1.1.11 Proxy & Routing Brokers - client-type interaction with proxy is questionable. (In later discussion, it appears client-type is a field in the request, and perhaps all AAA is one type, so may not be an issue.)

1.1.13 Shared secret not req'd - runs over TLS, no multiple levels of security.

1.2.1 NAI Support - some uncertainty on the impact of RFC 2459 (X.509 profiles) on this - may restrict NAI in some way?

1.2.3 EAP Support - multi-pass handshake needs work.

1.2.6 Authorization without Authentication - Mike comments the requirement is broken. BW comment (post-meeting) - the requirement appears intended specifically to chastise RADIUS for requiring User-Name and some sort of password in an Access-Request, even if it's sent pre-connect, on receipt of DNIS, for example. Sure it's silly, but does it really matter whether an attribute is absent or filled with "NONE"? This was just nasty sniping at RADIUS on somebody's part, imho.

1.3.2 RADIUS Gateway - skepticism was expressed.

1.3.4 Preclude L2 Tunnels - too much handwaving.

1.3.6 Access Rules - lots of work needed.

1.3.7 State Reconciliation - multi-server coordination is an issue.

1.4.4 Batch Accounting - for small batches, perhaps.

1.4.5 Guaranteed Delivery - application acks are an area of mystery.

1.5.2 Firewall-Friendly - COPS like any Swiss-Army-Knife protocol (SNMP) requires the firewall to look inside the packets, because passing AAA may be allowed but not other protocol uses. So it would be a big help, for both COPS and SNMP, to define a different port for its AAA application.

D.5 Minutes of 11-Jul-2000 Teleconference

Present: Mike, Bernard, Paul, Bert, Raj, Dave N., Dave M., Barney, Stuart, Mark
Recorded By: Dave Nelson

Mike St. Johns set the ground rules.

An item by item review of the summary results was held.

1.1.1 Question as to why SNMP and RADIUS++ are "P"? There are issues regarding scaling of retries in a web of proxies (multi-layer proxy; primary, secondary tertiary servers at each level).

1.1.2 No protocol did very well. Similar issues as above, e.g. web of proxies. Recovery of state from a previously failed primary server?

1.1.3 Question as to how serious is the need for this requirement? May be some legitimate requirements from Mobile IP. Is this requirement an AAA-level issue?

1.1.4 Called hop-by-hop or transmission level?

1.1.5 Most protocols evaluated used CMS to meet this requirement. Question as to applicability of CMS for NASes and other edge devices? There is a requirement for object by object confidentiality. consider three-party scenarios.

1.1.6 Question as to why SNMP did not rate the same as for item 1.1.5? The evaluation is based on what was contained in the submission documents, rather than capabilities of the protocol itself. Too much hand waving.

1.1.7 No comments.

1.1.8 Question as to meaning of "reliable"? Discussion of transport protocols was deferred to later in the meeting.

1.1.9 No comments.

1.1.10 SNMP received "P" because of hand waving in the submission documents.

1.1.11 SNMP received "F" because this section of the submission document indicated "t.b.d.". Diameter was the only protocol submission to completely address this item.

1.1.12 We treated this requirement as "non-repudiation". There is a concern that digital signatures are computationally expensive and are not globally available. COPS has more work to do on this item.

1.1.13 Question that "no shared secrets" should be interpreted to mean that an alternative key management mechanism is available? We treated this as meaning that application-layer security could be turned off in deference to transport layer security. There had been discussion of the use of IKE in the AAA protocol.

1.1.14 No comments.

1.2.1 No comments.

1.2.2 No comments.

1.2.3 No comments.

1.2.4 Is there a need for a clear-text "password" for service such as OTP, SecurID, et. al.? It was noted that all plain passwords are exposed in clear-text at the NAS or other edge device, which is no more inherently trustworthy than any AAA server or proxy.

1.2.5 We distinguished event-driven reauthentication from timer-driven (or lifetime-driven). How is this requirement to be met in a proxy environment?

1.2.6 We asserted that this requirement is an oxymoron.

1.3.1 We had difficulty in determining what "static" meant, and from which reference point it was measured.

1.3.2 We agreed that NAIs could be handled, possibly with some restrictions.

1.3.3 No comment.

1.3.4 The SNMP submission documents contained significant hand waving.

1.3.5 Similar comments as to item 1.2.5. The question was raised as to how the server knows when to send this request?

1.3.6 We found that the notation in Diameter was weak, and of a least common denominator nature. In general, there was concern about achieving interoperability when the syntax was standardized but the

semantics were not. This area needs further work.

1.3.7 Question as to how this requirement is achieved via proxies?

1.4.1 No comment.

1.4.2 No comment.

1.4.3 No comment.

1.4.4 There was significant skepticism regarding batch accounting as part of the AAA protocol. How large are the "batches"? Should this requirement be met using FTP or something similar?

1.4.5 No comment.

1.4.6 No comment.

1.4.7 No comment.

1.5.1 No comment.

1.5.2 There was some discussion of what constitutes firewall friendly. It was suggested that the firewall didn't want to look into packets much past the application protocol address (e.g. UDP or TCP port number). Protocols such as SNMP and COPS that have usage other than AAA are at a disadvantage, since the firewall must look deep into the application PDU to determine the intended purpose of the packet. Diameter suffers from reliance of SCTP, which is not widely deployed or widely recognized by firewalls. Should firewalls

also be AAA proxy engines? Has this issue anything to do with interoperability with NAT?

1.5.3 We had some confusion as to what the requirement actually was. Raj seemed to be able to explain it, but the rest of us had to take it on faith.

A poll was taken on overall acceptability and effort for each of the protocols submitted, for requirements conformance.

Each member indicated their evaluation in the form of (Acceptable, Not-Acceptable) with qualifiers for (Accounting, or effort to change) This information will be summarized in the final report.

A general wrap-up discussion was held.

It was considered important that as much of the thought processes and rationales be placed in the final report as is feasible. Mike St. John will work with Dave Mitton on the ID. We really need to meet the IETF July 14 submission deadline, even if we have to issue an update on the AAA WG mailing list. All agreed that the process went fairly well. In future evaluations of this nature, it would be well for the evaluators to follow the requirements documents closely, for the submitters to create accurate and complete conformance documents, and to allow a "re-spin" cycle to correct errors and omissions in the requirements documents and conformance documents.

A discussion of the transport protocol was held.

The issue with transport is congestion control. There has been a problem with streams-oriented applications over TCP. The IESG is increasingly sensitive to this issue in new protocols. It was noted that AAA was a transaction-oriented application. Other request-response applications, such as DNS, seem to scale welt to Internet-scale using simple application-level retries and UDP transport. TCP has problems with head-of-line blocking, especially when multiple sessions are using a single TCP connection. AAA typically will send 3 or 4 iterations and then indicate a failure to the upper layers. It won’t continue retransmissions in the face of congestion, like TCP. It was noted that bulk data transfer may not best be implemented in the AAA protocol. Concern was voiced that SCTP is not a widely implemented protocol. AAA will implement congestion control by limiting the number of outstanding requests. Some RADIUS implementations send lots of traffic when they encounter misconfigured shared secrets, but this is likely caused by a lack of proper error recovery. Diameter, as currently drafted, relies on SCTP. Can AAA run over UDP? The IESG didn’t say "no"; their issue is addressing congestion control.

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.