Submitted to AAA Working Group
INTERNET DRAFT

<draft-tjoens-aaa-radius-comp-00.txt>

Ronnie Ekstein
Yves T'Joens
Marc De Vries
Alcatel

May 2000
Expires November, 2000

# Comparison of RADIUS Against AAA Network Access Requirements

## Status of this memo



## Abstract

The AAA Working Group has completed a document that itemizes their requirements for Network Access Applications (NASREQ, Mobile IP, and ROAMOPS). This document compares the current RADIUS protocol to the Network Access AAA Evaluation Criteria, and illustrates where and how RADIUS can be improved to become unconditionally compliant to these requirements. This document is provided to the AAA Working Group as

an official submission for an AAA protocol.

## 1.0 Introduction

The AAA Working Group has completed a document that itemizes their requirements for Network Access Applications (NASREQ, Mobile IP, and ROAMOPS). This document compares the current RADIUS protocol to the Network Access AAA Evaluation Criteria, and illustrates where and how RADIUS can be improved to become unconditionally compliant to these requirements.

The main point the authors want to make is that the Network Access AAA requirements can be met by completing the definition of the RADIUS protocol, which ensures real backwards compatibility with a huge installed base (classic network access AAA services) without requiring each administrative domain to deploy RADIUS/non-RADIUS gateways, and without requiring the diverse platforms hosting AAA client or server applications to support an additional (even untried) transport layer protocol on top of IP.

## 1.1 Requirements language

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

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

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

## 2.0 Requirements Summary

This section contains the same four sections as found in the AAA Network Access requirements. Each section contains a new column,



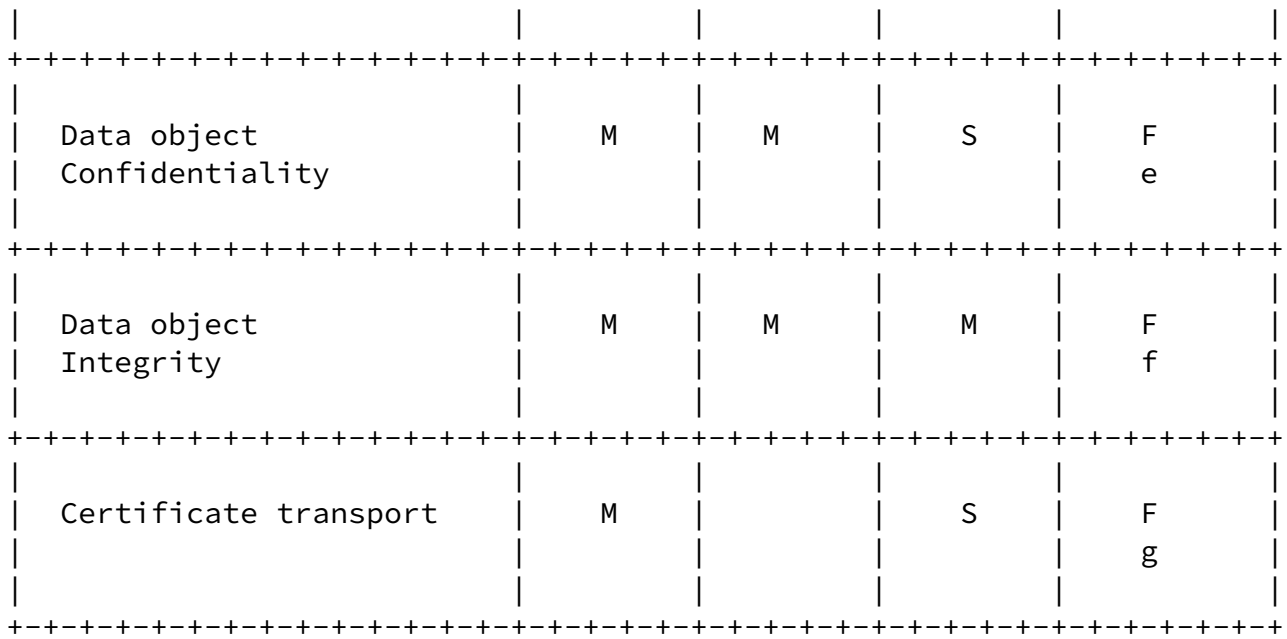


named RADIUS. For each requirement, it is noted whether the RADIUS protocol meets (T), Partially meets (P), or does not meet (F) the stated requirement. Furthermore, each requirement has a footnote, which contains additional justification.

## 2.1 General requirements

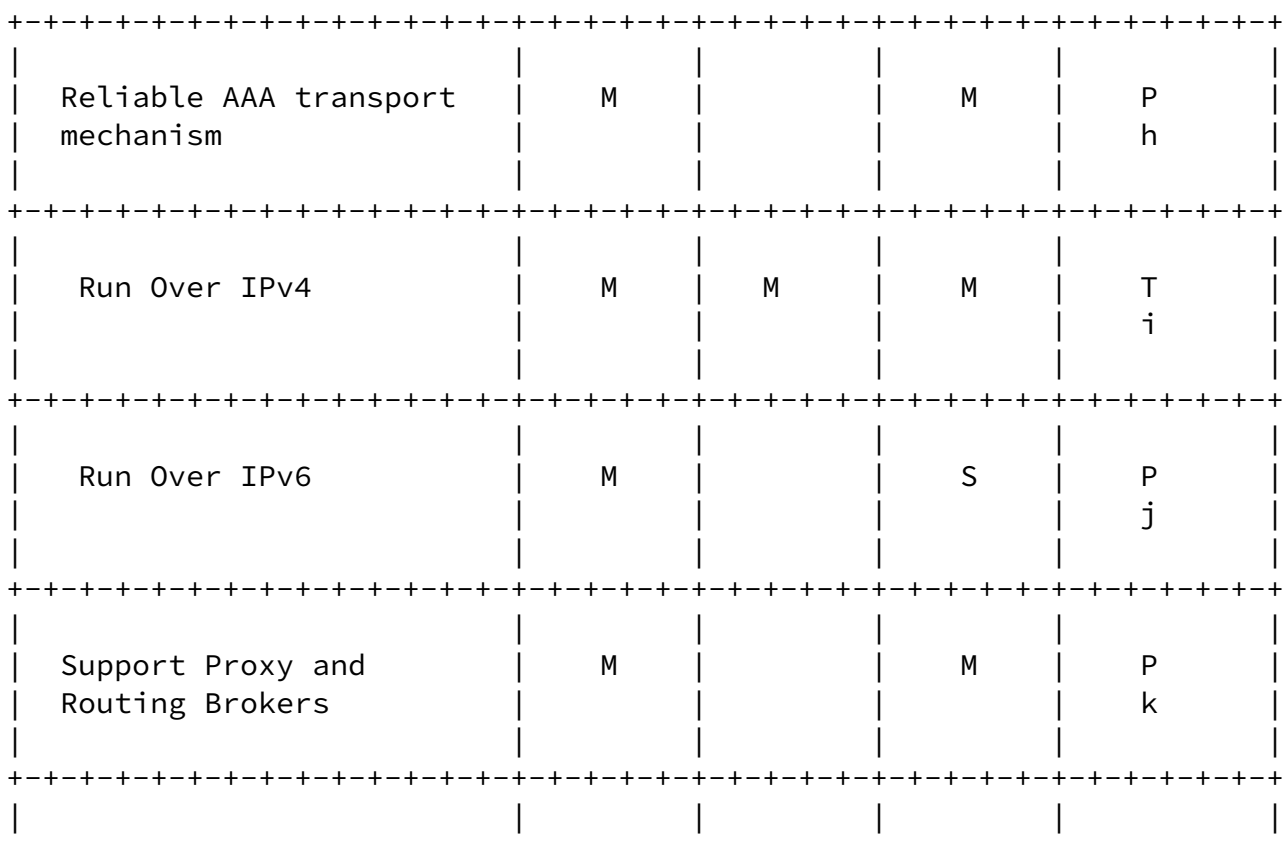
These requirements apply to all aspects of AAA and thus are considered general requirements.

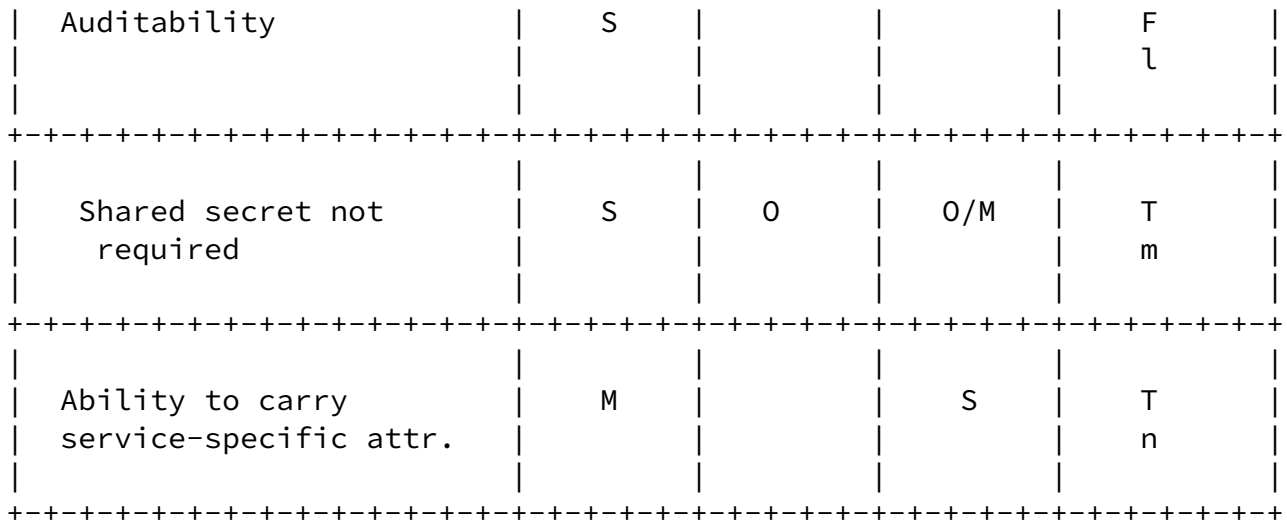
| General Reqts. | NASREQ | ROAMOPS | MOBILE IP | RADIUS |
|---|---|---|---|---|
| Scalability | M | M | M | P a |
| Failover | M | | M | T b |
| Mutual auth AAA client/server | M | | M | T c |
| Transmission level security | | M | S | P d |











| | | | | |
|---|---|---|---|---|
| Auditability | S | | | F<br>l |
| Shared secret not required | S | O | O/M | T<br>m |
| Ability to carry service-specific attr. | M | | S | T<br>n |

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

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





Clarifications

[a] The RADIUS protocol supports the scalability requirements, with the exception of tens of thousands of simultaneous requests between two communicating devices, as only up to 256 requests can be outstanding at any given time. This restriction can be worked around, for example, by increasing the number of transport addresses (IP address + UDP port) on either of the communicating devices. There are existing implementations using this technique. Other implementations have extended the request-to-reply mapping using a RADIUS attribute that MUST be returned unmodified by the server to the client, thereby extending the possible outstanding requests to 256 x 2^32 if both client and server support this extention.

[b] RADIUS allows for failover, failback and retransmission to be implemented on clients, by providing a means for clients to detect non-acknowledgement of requests and by providing a means for servers to detect retransmission. Additionally, the RADIUS message set could easily be extended to include alive checks, failover notification or server controlled failover and failback if required. Note that implementations exist that allow for RADIUS servers to send requests to RADIUS clients on a well-known UDP port of the client.

[c] RADIUS supports authentication of server to client during authentication (using a request and response authenticator with shared secret), and supports mutual client-server authentication during accounting (again using authenticators with shared secret). Stronger mutual authentication between client and server can be accomplished for example by an underlying security service (like IPSec) or by support of the Message Authenticator as defined in [7].

[d] RADIUS supports hop-by-hop authentication and integrity for authentication responses and accounting requests and responses. Hop-by-hop confidentiality is currently provided for password attributes in authentication requests and responses. The hop-by-hop integrity of authentication requests can be provided by including an integrity check vector attribute. Stronger security can be accomplished by an underlying security service like IPSec.

[e] RADIUS does not yet support end-to-end confidentiality at the attribute level. It is however possible to extend the RADIUS protocol to allow data objects (attribute groups) to be encapsulated and encrypted for this purpose.





[f] RADIUS does not yet support end-to-end authentication and integrity at the attribute level. It is however possible to extend the RADIUS protocol to allow data objects (attribute groups) to be encapsulated and marked with an end-to-end authenticated integrity check vector.

[g] RADIUS does not yet support certificate transport. This can however be provided by defining new messages and/or attributes

for out-of-band and/or in-band certificate exchange.

[h] The RADIUS protocol uses UDP/IP for transport of messages.

1. Hop-by-hop retransmission and failover is supported, under control of the application (e.g. requires stateful proxies and tuned retransmission timers).

2. The retransmission mechanism is entirely controlled by the application, not the underlying transport.

3. For authentication requests, receipt is not acknowledged until the response is available. For authentication and accounting responses, receipt is not acknowledged (although some implementations use an Accounting-Request/Start message as acknowledgement for Access-Accept). Accounting-Request messages are explicitly acknowledged. Message independent acknowledgement can be provided in RADIUS by introducing an explicit acknowledge message.

4. (item not listed in Evaluation Requirements)

5. Piggy-backing of acknowledgments can be provided in the explicit acknowledge message to be defined. Piggy-backing on actual AAA messages would require windowing support which is difficult to introduce in RADIUS.

6. Timely delivery of responses is controlled by the application.

[i] RADIUS messages can be transported over IPv4. The RADIUS protocol depends on the underlying IP version since certain attributes can have an 'address' data type which is defined as an IPv4 address. IPv4 is supported.

[j] RADIUS messages can be transported over IPv6. The RADIUS protocol depends on the underlying IP version since certain attributes can have an 'address' data type which is defined as an IPv4 address. An IPv6 address data type can be defined to support IPv6 address values.





[k] RADIUS supports proxy and transparent brokers, as explicitly

clarified in [5]. The RADIUS protocol does not by itself support a means for routing brokers to provide the client with a new server address. This can be accomplished by extending the RADIUS message set with routing messages or redirection attributes within the existing message set.

[l] RADIUS does not yet support tracing of the end-to-end message path nor the changes made to attributes along that path. This information may be logged for off-line auditing purposes at each hop.

[m] The RADIUS protocol currently requires shared secrets between communicating devices to match. In case an underlying security service (e.g. IPSec) is used, it is possible to configure the communicating devices with empty shared secret values.

[n] The RADIUS protocol currently defines attributes and messages for AAA services, out of a message and attribute number space of size 255 each. Within the common attribute number space, a single attribute type is used to encapsulate Vendor-Specific attributes. The same mechanism can be used to encapsulate standard attributes defined as extensions for other services.

## 2.2 Authentication Requirements

| Authentication Reqts. | NASREQ | ROAMOPS | MOBILE IP | RADIUS |
|---|---|---|---|---|
| NAI Support | M | M | S | T a |
| CHAP Support | M | M | O | T b |
| EAP Support | M | S | O | T c |
| PAP/Clear-Text Support | M | B | O | P d |
| Re-authentication on demand | M | | S | T e |
| Authorization Only without Authentication | M | | O | F f |

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

T = Meets Requirement
P = Partly Meets Requirement





F = Does Not Meet Requirement

Clarifications

[a] The RADIUS protocol defines a User-Name attribute for authentication and accounting, supporting the NAI format [5][13] and allowing for message forwarding based on e.g. realm identification prefixes or suffixes.

[b] The RADIUS protocol supports authentication of a PPP user using the CHAP authentication mechanism by passing the CHAP challenge and challenge response in attributes to the home AAA server for verification.

[c] The RADIUS protocol has been extended in [7] to support PPP users using the EAP authentication mechanism, supporting attributes to carry EAP messages.

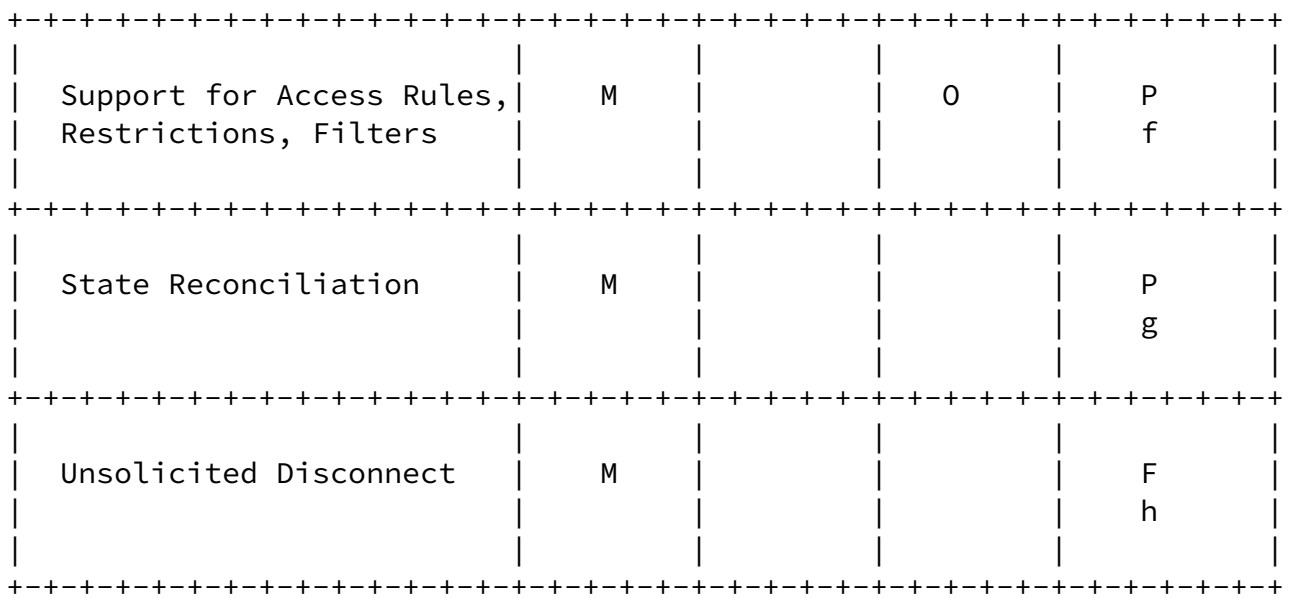
[d] The RADIUS protocol supports authentication of a PPP user using the PAP authentication mechanism as well as terminal access users using clear-text passwords. The passwords are transmitted in a confidential manner for hop-by-hop communication. End-to-end confidentiality of password attributes is not yet supported. It is, however, possible to extend the RADIUS protocol to allow data objects (attribute groups) to be encapsulated and encrypted for this purpose.

[e] 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.

[f] The RADIUS protocol does not yet explicitly support non-authenticated authorisation. This can easily be supported by defining a new request message type or a new end-to-end secured attribute.

## 2.3 Authorization Requirements

| Authorization Reqts. | NASREQ | ROAMOPS | MOBILE IP | RADIUS |
|---|---|---|---|---|
| Static and Dynamic IPv4/6 Address Assign. | M | M | M | Pa |
| RADIUS gateway capability | M | M | O | Tb |
| Reject capability | M | M | M | Tc |
| Precludes layer 2 tunneling | N | N | | Td |
| Re-Authorization on demand | M | | S | Pe |



| | | | | |
|---|---|---|---|---|
| Support for Access Rules, Restrictions, Filters | M | | O | P f |
| State Reconciliation | M | | | P g |
| Unsolicited Disconnect | M | | | F h |





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

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

Clarifications

[a] RADIUS allows for both static and dynamic address assignement. Currently only an IPv4 address data type is defined. An IPv6 address data type can be defined to support IPv6 address values. The Address field of the transported Framed-IP-Address or NAS-IP-Address attributes can be extended to 16 octets [5].

[b] This is always true when RADIUS is used as base protocol. Moreover, by completing RADIUS within the new scope of the AAA Working Group, not only can backwards compatibility with user profile databases be guaranteed, it can also guarantee protocol and application level compatibility for the installed base RADIUS/AAA applications. Therefore this approach does not even

require a gateway application.

[c] RADIUS supports proxy and transparent brokers [5]. RADIUS allows brokers to reject authentication requests before or after contacting the home AAA server. This behaviour is entirely under control of the application (e.g based on the requested Service-Type, or based on the authorisation attributes included in the response).

[d] [10] defines a set of RADIUS attributes designed to support the provision of compulsory tunneling in dial-up networks. [11] defines the necessary new RADIUS accounting Attributes and new values for the existing Acct-Status-Type Attribute.

[e] The RADIUS protocol has defined the Session-Timeout attribute [5] to set the maximum number of seconds of service to be provided to the user before termination of the session or prompt. In order to renew a session, a re-authorization MUST be submitted. Re-authorization without re-authentication is not currently supported in RADIUS, but can be provided by defining a new message type or attribute. Active termination of a session from a RADIUS server or broker is not currently supported, but existing implementations have proven that RADIUS can be extended





to support this as a Disconnect-Request from server to client [9].

[f]

[1][2][3]Time/day,port location and dialed/dialling number restrictions are typically applied at the AAA home or broker servers.

[4] Concurrent login restriction is supported (per AAA client) by the Port-Limit attribute. Global concurrent login restriction can be implemented by stateful brokers and home AAA servers.

[5] RADIUS provides for a Session-Timeout attribute to aid enforcement of the time/day restriction and session duration restriction on the AAA client. RADIUS also defines an Idle-Timeout attribute to force termination of idle sessions on the AAA client.

[6] RADIUS specifies the Filter-Id attribute [5], which indicates the name of the filter list for this user. Zero or more Filter-Id attributes MAY be sent in an Access-Accept packet. Identifying a filter list by name allows the filter to be used on different NASes without regard to filter-list implementation details. Existing implementations are known to use the Vendor-Specific attribute defined in RADIUS to implement an attribute that contains the filter rule in a vendor-specifc format.

[7] Static routes can be enforced via zero or more occurences of the RADIUS attribute Framed-Route. Existing implementations are known to support new attributes to enforce other types of forced access paths (e.g. fixed uplink PVC, bypassing the AAA client's routing function).

[8] QOS parameters are not currently defined in RADIUS, but can easily be provided by defining the corresponding attributes. Existing implementations are known to use Vendor-Specific attributes to provide QoS (e.g. TOS bit masks, VPN IDs) parameters to the AAA client.

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

[1] Re-authorization capabilities - The RADIUS protocol provides the Session-Timeout attribute [5], which indicates the number of seconds of service to be provided to the user before termination of the session or prompt. The AAA client





may re-authorise in order to retrieve this value if lost on the client. However RADIUS currently forces re-authorisation to include re-authentication as well.

[2] Session disconnect message - RADIUS does not yet support a session disconnect message. This can, however, be provided by defining a Disconnect-Request message and by requiring the Acct-Session-Id attribute to be included in all session-related messages. Examples of existing RADIUS implementations using this technique are provided in [9].

[3] Transport and application-layer reliability - RADIUS relies on UDP for the delivery/transport of information between client and server, the protocol handles the loss of request by implementing a time-out and retransmission strategy. However, the protocol specification failed to define a standard retransmission and timeout scheme. It is in fact the application layer that takes care of retransmission, fail-over and timely delivery of responses. RADIUS does not take care of acknowledgements and windowing. RADIUS can, however, be extended to optimise delivery reliability as described under the General Requirements section above.

[4] An interim message - RADIUS allows to include in the Accounting Request the "Interim-Update" value in a Acct-Status-Type attribute [6]. RADIUS provides the possibility for a server that wishes to receive interim accounting messages for the given user to include the Acct-Interim-Interval RADIUS attribute in the authentication response message, which indicates the interval in seconds between interim messages [7].

[5] A mechanism for the AAA server to retrieve state information from the NAS. This mechanism will provide timely information although a complete state dump may not be immediately available. - RADIUS as originally defined did not require AAA servers to keep state. The documents [5] and [6] include clarifications on using RADIUS with stateful brokers or proxy servers. Existing implementations of RADIUS brokers/proxies are capable of providing resource management (concurrent session limitation, port wholesale, centralised IP pools, ...). Although RADIUS allows for stateful implementations, it does not yet support state retrieval between AAA client and AAA server. Existing implemenations are known to support this today using extentions to RADIUS (new messages and attributes).





[6] A NAS reboot message - RADIUS supports the Accounting On/Off messages which may imply an AAA client reboot (before and after). An extra attribute can be defined to explicitly state the reason for the Accounting On/Off mes-

sages.

[7] Accounting On/Off messages - The RADIUS protocol has defined the Accounting-Status-Type attribute to indicate whether an Accounting-Request marks the beginning of the user service (Start) or the end (Stop). [7] has defined additional values to support the Accounting On/Off messages.

[h] Session disconnect message - RADIUS does not yet support a session disconnect message. This can, however, be provided by defining a new Disconnect-Request message, a correspondant disconnect reason value in the Acct-Terminate-Cause attribute [6], and the requirement to include the Acct-Session-Id attribute in all session-related messages.

## 2.4 Accounting Requirements

| Accounting Reqts. | NASREQ | ROAMOPS | MOBILE IP | RADIUS |
|---|---|---|---|---|
| Real-time accounting | M | M | M | Ta |
| Mandatory Compact Encoding | | M | M | Tb |
| Accounting Record Extensibility | M | M | M | Tc |
| Batch Accounting | S | | | Fd |
| Guaranteed Delivery | M | | M | Te |
| Accounting Time Stamps | M | | S | Tf |
| Dynamic Accounting | M | | S | Pg |

Key
M = MUST
S = SHOULD

O = MAY





N = MUST NOT
B = SHOULD NOT

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

Clarifications

[a] The RADIUS implementation, based on the extensions as defined in [7] allows for indicating an accounting interval time at which cumulative accounting information should be sent to the Accounting Server.

[b] The present set of attributes defined in [6] and [7] represents a compact representation of accounting data. If it would be required to transport entire accounting records, RADIUS could be extended with an attribute along the ADIF definition [14].

[c] By definition of new attributes for accounting data, the accounting information transported can be easily extended. If it would be required to transport entire accounting records, RADIUS could be extended with an attribute along the ADIF definition, which allows for easy extension.

[d] RADIUS does not yet support batch accounting. It is, however, possible to extend the attribute space of RADIUS with an accounting batch attribute.

[e] RADIUS prescribes every Accounting-Request message to be acknowledged by an Accounting-Response message indicating successfull delivery. A retransmission scheme allows for repeated attempts for delivery.

[f] The RADIUS extensions specification [7] defines the Event-Timestamp Attribute as an extension to the Accounting-Request message.

[g] RADIUS does not yet support dynamic authorization. It is, however, possible to extend the message set of RADIUS (or semantic

interpretation of the existing message set) to include dynamic (re-)authorization. RADIUS allows for interim updates of accounting information, as defined in [7].





## 2.5 Unique Mobile IP requirements

In addition Mobile IP also has the following requirements:

| Unique Mobile IP requirements | NASREQ | ROAMOPS | MOBILE IP | RADIUS |
|---|---|---|---|---|
| Encoding of Mobile IP registration messages | | | M | Fa |
| Firewall friendly | | | M | Tb |
| Allocation of local Home agent | | | S/M | Fc |

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

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

Clarifications

[a] RADIUS does not yet support Mobile IP registration messages. It is, however, possible to extend the attribute space of RADIUS to include the registration information.

[b] RADIUS is known to be operational in environments where firewalls acting as a proxy are active.

[c] RADIUS does not yet support allocation of local Home agents. It is, however, possible to extend the attribute space of RADIUS to





allocate the local home agent.

## 3.0 Conclusion

The RADIUS protocol, and its associated extensions [7], is presently not fully compliant with the AAA Network Access requirements [2]. However, as is indicated at the relevant places in this document it is possible with a small effort to extend present procedures to meet the requirements as listed in [2], while maintaining a high level of interoperability with the wide deployment and installed base of RADIUS clients and servers.

## 4.0 References

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

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

[3] Rigney, C., Rubens, A., Simpson, W., Willens, S., "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, April 1997

[4] Rigney, C., "RADIUS Accounting", RFC 2139, April 1997

[5] Rigney, C., Rubens, A., Simpson, W., Willens, S., "Remote Authentication Dial In User Service (RADIUS)", Internet-Draft, draft-ietf-radius-radius-v2-06.txt, February 2000.

[6] Rigney, C., "RADIUS Accounting", draft-ietf-radius-accounting-v2-05.txt, February 2000.

[7] Rigney C., Willats W., Calhoun P., "RADIUS Extensions", draft-ietf-radius-ext-07.txt, Internet Draft, February 2000.

[8] B. Aboba, G. Zorn, "Criteria for Evaluating Roaming Protocols", RFC 2477 (Informational), January 1998

[9] Mitton, D.,"Network Access Servers Requirements: Extended RADIUS Practices", draft-ietf-nasreq-ext-radiuspract-03.txt, Internet Draft, May 2000.

[10] Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M. and I. Goyret, "RADIUS Attributes for Tunnel Protocol Support", draft-ietf-radius-tunnel-auth-09.txt, Internet Draft (work in progress), August 1999 (Expired)





[11] Zorn, G., Mitton, D., "RADIUS Accounting Modifications for Tunnel Protocol Support", draft-ietf-radius-tunnel-acct-05.txt, Internet Draft (work in progress), October 1999 (Expired)

[12] B. Aboba, G. Zorn, "Implementation of L2TP Compulsory Tunneling via RADIUS", draft-ietf-radius-tunnel-imp-05.txt, Internet Draft (work in progress), 20 August 1999, (Expired)

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

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

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

## 5.0 Security Considerations

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

## 6.0 IANA Considerations

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

## 7.0 Acknowledgements

## 8.0 Authors Addresses

Ronnie Ekstein
Alcatel Network Strategy Group
Francis Wellesplein 1, 2018 Antwerp, Belgium
Phone : +32 3 241 5958
E-mail : ronnie.ekstein@alcatel.be





Yves T'Joens
Alcatel Network Strategy Group
Francis Wellesplein 1, 2018 Antwerp, Belgium
Phone : +32 3 240 7890
E-mail : yves.tjoens@alcatel.be

Marc De Vries
Alcatel Carrier Internetworking Division
De Villermontstraat 38, 2550 Kontich, Belgium
E-mail : marc.de_vries@alcatel.be

## 9.0 Full Copyright Statement





---

Submitted to AAA Working Group
INTERNET DRAFT

<draft-tjoens-aaa-radius-comp-00.txt>

Ronnie Ekstein
Yves T'Joens
Marc De Vries
Alcatel

May 2000
Expires November, 2000

Comparison of RADIUS Against AAA Network Access Requirements

## Status of this memo



## Abstract

The AAA Working Group has completed a document that itemizes their requirements for Network Access Applications (NASREQ, Mobile IP, and ROAMOPS). This document compares the current RADIUS protocol to the Network Access AAA Evaluation Criteria, and illustrates where and how RADIUS can be improved to become unconditionally compliant to these requirements. This document is provided to the AAA Working Group as





an official submission for an AAA protocol.

## 1.0 Introduction

The AAA Working Group has completed a document that itemizes their requirements for Network Access Applications (NASREQ, Mobile IP, and ROAMOPS). This document compares the current RADIUS protocol to the Network Access AAA Evaluation Criteria, and illustrates where and how RADIUS can be improved to become unconditionally compliant to these requirements.

The main point the authors want to make is that the Network Access AAA requirements can be met by completing the definition of the RADIUS protocol, which ensures real backwards compatibility with a huge installed base (classic network access AAA services) without requiring each administrative domain to deploy RADIUS/non-RADIUS gateways, and without requiring the diverse platforms hosting AAA client or server applications to support an additional (even untried) transport layer protocol on top of IP.

## 1.1 Requirements language

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

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

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

## 2.0 Requirements Summary

This section contains the same four sections as found in the AAA Network Access requirements. Each section contains a new column,

named RADIUS. For each requirement, it is noted whether the RADIUS protocol meets (T), Partially meets (P), or does not meet (F) the stated requirement. Furthermore, each requirement has a footnote, which contains additional justification.

## 2.1 General requirements

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

| General Reqts. | NASREQ | ROAMOPS | MOBILE IP | RADIUS |
|---|---|---|---|---|
| Scalability | M | M | M | P a |
| Failover | M | | M | T b |
| Mutual auth AAA client/server | M | | M | T c |
| Transmission level security | | M | S | P d |
| Data object Confidentiality | M | M | S | F e |
| Data object Integrity | M | M | M | F f |

| | | | | |
|---|---|---|---|---|
| Certificate transport | M | | S | F g |





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

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

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

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





Clarifications

[a] The RADIUS protocol supports the scalability requirements, with the exception of tens of thousands of simultaneous requests between two communicating devices, as only up to 256 requests can be outstanding at any given time. This restriction can be worked around, for example, by increasing the number of transport addresses (IP address + UDP port) on either of the communicating devices. There are existing implementations using this technique. Other implementations have extended the request-to-reply mapping using a RADIUS attribute that MUST be returned unmodified by the server to the client, thereby extending the possible outstanding requests to 256 x 2^32 if both client and server support this extention.

[b] RADIUS allows for failover, failback and retransmission to be implemented on clients, by providing a means for clients to detect non-acknowledgement of requests and by providing a means for servers to detect retransmission. Additionally, the RADIUS message set could easily be extended to include alive checks, failover notification or server controlled failover and failback if required. Note that implementations exist that allow for RADIUS servers to send requests to RADIUS clients on a well-known UDP port of the client.

[c] RADIUS supports authentication of server to client during authentication (using a request and response authenticator with shared secret), and supports mutual client-server authentication during accounting (again using authenticators with shared secret). Stronger mutual authentication between client and server can be accomplished for example by an underlying security service (like IPSec) or by support of the Message Authenticator as defined in [7].

[d] RADIUS supports hop-by-hop authentication and integrity for authentication responses and accounting requests and responses. Hop-by-hop confidentiality is currently provided for password attributes in authentication requests and responses. The hop-by-hop integrity of authentication requests can be provided by including an integrity check vector attribute. Stronger security can be accomplished by an underlying security service like IPSec.

[e] RADIUS does not yet support end-to-end confidentiality at the attribute level. It is however possible to extend the RADIUS protocol to allow data objects (attribute groups) to be encapsulated and encrypted for this purpose.





[f] RADIUS does not yet support end-to-end authentication and integrity at the attribute level. It is however possible to extend the RADIUS protocol to allow data objects (attribute groups) to be encapsulated and marked with an end-to-end authenticated integrity check vector.

[g] RADIUS does not yet support certificate transport. This can however be provided by defining new messages and/or attributes for out-of-band and/or in-band certificate exchange.

[h] The RADIUS protocol uses UDP/IP for transport of messages.

1. Hop-by-hop retransmission and failover is supported, under control of the application (e.g. requires stateful proxies and tuned retransmission timers).

2. The retransmission mechanism is entirely controlled by the application, not the underlying transport.

3. For authentication requests, receipt is not acknowledged until the response is available. For authentication and accounting responses, receipt is not acknowledged (although some implementations use an Accounting-Request/Start message as acknowledgement for Access-Accept). Accounting-Request messages are explicitly acknowledged. Message independent acknowledgement can be provided in RADIUS by introducing an explicit acknowledge message.

4. (item not listed in Evaluation Requirements)

5. Piggy-backing of acknowledgments can be provided in the explicit acknowledge message to be defined. Piggy-backing on actual AAA messages would require windowing support which is difficult to introduce in RADIUS.

6. Timely delivery of responses is controlled by the application.

[i] RADIUS messages can be transported over IPv4. The RADIUS protocol depends on the underlying IP version since certain attributes can have an 'address' data type which is defined as an IPv4 address. IPv4 is supported.

[j] RADIUS messages can be transported over IPv6. The RADIUS protocol depends on the underlying IP version since certain attributes can have an 'address' data type which is defined as an IPv4 address. An IPv6 address data type can be defined to support IPv6 address values.





[k] RADIUS supports proxy and transparent brokers, as explicitly clarified in [5]. The RADIUS protocol does not by itself support a means for routing brokers to provide the client with a new server address. This can be accomplished by extending the RADIUS message set with routing messages or redirection attributes within the existing message set.

[l] RADIUS does not yet support tracing of the end-to-end message path nor the changes made to attributes along that path. This information may be logged for off-line auditing purposes at each hop.

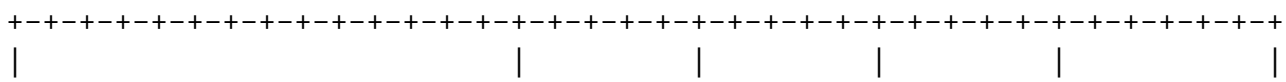
[m] The RADIUS protocol currently requires shared secrets between communicating devices to match. In case an underlying security service (e.g. IPSec) is used, it is possible to configure the communicating devices with empty shared secret values.

[n] The RADIUS protocol currently defines attributes and messages for AAA services, out of a message and attribute number space of size 255 each. Within the common attribute number space, a single attribute type is used to encapsulate Vendor-Specific attributes. The same mechanism can be used to encapsulate standard attributes defined as extensions for other services.





## 2.2 Authentication Requirements



| Authentication Reqts. | NASREQ | ROAMOPS | MOBILE IP | RADIUS |
|---|---|---|---|---|
| NAI Support | M | M | S | T a |
| CHAP Support | M | M | O | T b |
| EAP Support | M | S | O | T c |
| PAP/Clear-Text Support | M | B | O | P d |
| Re-authentication on demand | M | | S | T e |
| Authorization Only without Authentication | M | | O | F f |

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

T = Meets Requirement
P = Partly Meets Requirement

F = Does Not Meet Requirement

Clarifications

[a] The RADIUS protocol defines a User-Name attribute for authentication and accounting, supporting the NAI format [5][13] and allowing for message forwarding based on e.g. realm identification prefixes or suffixes.

[b] The RADIUS protocol supports authentication of a PPP user using the CHAP authentication mechanism by passing the CHAP challenge and challenge response in attributes to the home AAA server for verification.

[c] The RADIUS protocol has been extended in [7] to support PPP users using the EAP authentication mechanism, supporting attributes to carry EAP messages.

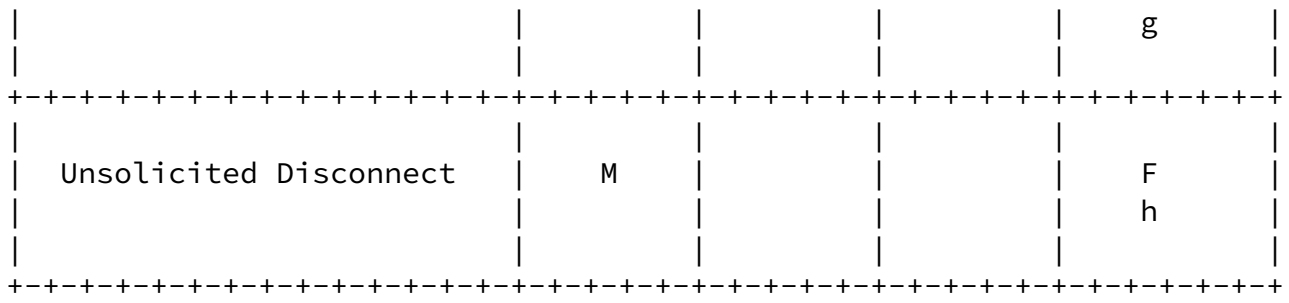
[d] The RADIUS protocol supports authentication of a PPP user using the PAP authentication mechanism as well as terminal access users using clear-text passwords. The passwords are transmitted in a confidential manner for hop-by-hop communication. End-to-end confidentiality of password attributes is not yet supported. It is, however, possible to extend the RADIUS protocol to allow data objects (attribute groups) to be encapsulated and encrypted for this purpose.

[e] 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.

[f] The RADIUS protocol does not yet explicitly support non-authenticated authorisation. This can easily be supported by defining a new request message type or a new end-to-end secured attribute.

## 2.3 Authorization Requirements

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



| | | | | |
|---|---|---|---|---|
| | | | | g |
| Unsolicited Disconnect | M | | | F<br>h |





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

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

Clarifications

[a] RADIUS allows for both static and dynamic address assignement. Currently only an IPv4 address data type is defined. An IPv6 address data type can be defined to support IPv6 address values. The Address field of the transported Framed-IP-Address or NAS-IP-Address attributes can be extended to 16 octets [5].

[b] This is always true when RADIUS is used as base protocol. Moreover, by completing RADIUS within the new scope of the AAA Working Group, not only can backwards compatibility with user profile databases be guaranteed, it can also guarantee protocol and application level compatibility for the installed base RADIUS/AAA applications. Therefore this approach does not even require a gateway application.

[c] RADIUS supports proxy and transparent brokers [5]. RADIUS allows brokers to reject authentication requests before or after contacting the home AAA server. This behaviour is entirely under control of the application (e.g based on the requested Service-Type, or based on the authorisation attributes included in the response).

[d] [10] defines a set of RADIUS attributes designed to support the provision of compulsory tunneling in dial-up networks. [11] defines the necessary new RADIUS accounting Attributes and new values for the existing Acct-Status-Type Attribute.

[e] The RADIUS protocol has defined the Session-Timeout attribute [5] to set the maximum number of seconds of service to be provided to the user before termination of the session or prompt. In order to renew a session, a re-authorization MUST be submitted. Re-authorization without re-authentication is not currently supported in RADIUS, but can be provided by defining a new message type or attribute. Active termination of a session from a RADIUS server or broker is not currently supported, but existing implementations have proven that RADIUS can be extended





to support this as a Disconnect-Request from server to client [9].

[f]

[1][2][3]Time/day,port location and dialed/dialling number restrictions are typically applied at the AAA home or broker servers.

[4] Concurrent login restriction is supported (per AAA client) by the Port-Limit attribute. Global concurrent login restriction can be implemented by stateful brokers and home AAA servers.

[5] RADIUS provides for a Session-Timeout attribute to aid enforcement of the time/day restriction and session duration restriction on the AAA client. RADIUS also defines an Idle-Timeout attribute to force termination of idle sessions on the AAA client.

[6] RADIUS specifies the Filter-Id attribute [5], which indicates the name of the filter list for this user. Zero or more Filter-Id attributes MAY be sent in an Access-Accept packet. Identifying a filter list by name allows the filter to be used on different NASes without regard to filter-list implementation details. Existing implementations are known to use the Vendor-Specific attribute defined in RADIUS to

implement an attribute that contains the filter rule in a vendor-specifc format.

[7] Static routes can be enforced via zero or more occurences of the RADIUS attribute Framed-Route. Existing implementations are known to support new attributes to enforce other types of forced access paths (e.g. fixed uplink PVC, bypassing the AAA client's routing function).

[8] QOS parameters are not currently defined in RADIUS, but can easily be provided by defining the corresponding attributes. Existing implementations are known to use Vendor-Specific attributes to provide QoS (e.g. TOS bit masks, VPN IDs) parameters to the AAA client.

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

[1] Re-authorization capabilities - The RADIUS protocol provides the Session-Timeout attribute [5], which indicates the number of seconds of service to be provided to the user before termination of the session or prompt. The AAA client





may re-authorise in order to retrieve this value if lost on the client. However RADIUS currently forces re-authorisation to include re-authentication as well.

[2] Session disconnect message - RADIUS does not yet support a session disconnect message. This can, however, be provided by defining a Disconnect-Request message and by requiring the Acct-Session-Id attribute to be included in all session-related messages. Examples of existing RADIUS implementations using this technique are provided in [9].

[3] Transport and application-layer reliability - RADIUS relies on UDP for the delivery/transport of information between client and server, the protocol handles the loss of request by implementing a time-out and retransmission strategy. However, the protocol specification failed to define a standard retransmission and timeout scheme. It is in fact the application layer that takes care of retransmission, fail-over and timely delivery of

responses. RADIUS does not take care of acknowledgements and windowing. RADIUS can, however, be extended to optimise delivery reliability as described under the General Requirements section above.

[4] An interim message - RADIUS allows to include in the Accounting Request the "Interim-Update" value in a Acct-Status-Type attribute [6]. RADIUS provides the possibility for a server that wishes to receive interim accounting messages for the given user to include the Acct-Interim-Interval RADIUS attribute in the authentication response message, which indicates the interval in seconds between interim messages [7].

[5] A mechanism for the AAA server to retrieve state information from the NAS. This mechanism will provide timely information although a complete state dump may not be immediately available. - RADIUS as originally defined did not require AAA servers to keep state. The documents [5] and [6] include clarifications on using RADIUS with stateful brokers or proxy servers. Existing implementations of RADIUS brokers/proxies are capable of providing resource management (concurrent session limitation, port wholesale, centralised IP pools, ...). Although RADIUS allows for stateful implementations, it does not yet support state retrieval between AAA client and AAA server. Existing implemenations are known to support this today using extentions to RADIUS (new messages and attributes).





[6] A NAS reboot message - RADIUS supports the Accounting On/Off messages which may imply an AAA client reboot (before and after). An extra attribute can be defined to explicitly state the reason for the Accounting On/Off messages.

[7] Accounting On/Off messages - The RADIUS protocol has defined the Accounting-Status-Type attribute to indicate whether an Accounting-Request marks the beginning of the user service (Start) or the end (Stop). [7] has defined additional values to support the Accounting On/Off messages.

[h] Session disconnect message - RADIUS does not yet support a session disconnect message. This can, however, be provided by defining a new Disconnect-Request message, a correspondant disconnect reason value in the Acct-Terminate-Cause attribute [6], and the requirement to include the Acct-Session-Id attribute in all session-related messages.





## 2.4 Accounting Requirements

| Accounting | NASREQ | ROAMOPS | MOBILE | RADIUS |
|---|---|---|---|---|

| Reqts. | | | IP | |
|---|---|---|---|---|
| Real-time accounting | M | M | M | T a |
| Mandatory Compact Encoding | | M | M | T b |
| Accounting Record Extensibility | M | M | M | T c |
| Batch Accounting | S | | | F d |
| Guaranteed Delivery | M | | M | T e |
| Accounting Time Stamps | M | | S | T f |
| Dynamic Accounting | M | | S | P g |

Key
M = MUST
S = SHOULD
O = MAY

N = MUST NOT
B = SHOULD NOT

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

Clarifications

[a] The RADIUS implementation, based on the extensions as defined in [7] allows for indicating an accounting interval time at which cumulative accounting information should be sent to the Accounting Server.

[b] The present set of attributes defined in [6] and [7] represents a compact representation of accounting data. If it would be required to transport entire accounting records, RADIUS could be extended with an attribute along the ADIF definition [14].

[c] By definition of new attributes for accounting data, the accounting information transported can be easily extended. If it would be required to transport entire accounting records, RADIUS could be extended with an attribute along the ADIF definition, which allows for easy extension.

[d] RADIUS does not yet support batch accounting. It is, however, possible to extend the attribute space of RADIUS with an accounting batch attribute.

[e] RADIUS prescribes every Accounting-Request message to be acknowledged by an Accounting-Response message indicating successfull delivery. A retransmission scheme allows for repeated attempts for delivery.

[f] The RADIUS extensions specification [7] defines the Event-Timestamp Attribute as an extension to the Accounting-Request message.

[g] RADIUS does not yet support dynamic authorization. It is, however, possible to extend the message set of RADIUS (or semantic interpretation of the existing message set) to include dynamic (re-)authorization. RADIUS allows for interim updates of accounting information, as defined in [7].

## 2.5 Unique Mobile IP requirements

In addition Mobile IP also has the following requirements:

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

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

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

Clarifications

[a] RADIUS does not yet support Mobile IP registration messages. It is, however, possible to extend the attribute space of RADIUS to include the registration information.

[b] RADIUS is known to be operational in environments where firewalls acting as a proxy are active.

[c] RADIUS does not yet support allocation of local Home agents. It is, however, possible to extend the attribute space of RADIUS to





allocate the local home agent.

## 3.0 Conclusion

The RADIUS protocol, and its associated extensions [7], is presently not fully compliant with the AAA Network Access requirements [2]. However, as is indicated at the relevant places in this document it is possible with a small effort to extend present procedures to meet the requirements as listed in [2], while maintaining a high level of interoperability with the wide deployment and installed base of RADIUS clients and servers.

## 4.0 References

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

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

[3] Rigney, C., Rubens, A., Simpson, W., Willens, S., "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, April 1997

[4] Rigney, C., "RADIUS Accounting", RFC 2139, April 1997

[5] Rigney, C., Rubens, A., Simpson, W., Willens, S., "Remote Authentication Dial In User Service (RADIUS)", Internet-Draft, draft-ietf-radius-radius-v2-06.txt, February 2000.

[6] Rigney, C., "RADIUS Accounting", draft-ietf-radius-accounting-v2-05.txt, February 2000.

[7] Rigney C., Willats W., Calhoun P., "RADIUS Extensions", draft-

ietf-radius-ext-07.txt, Internet Draft, February 2000.

[8] B. Aboba, G. Zorn, "Criteria for Evaluating Roaming Protocols", RFC 2477 (Informational), January 1998

[9] Mitton, D.,"Network Access Servers Requirements: Extended RADIUS Practices", draft-ietf-nasreq-ext-radiuspract-03.txt, Internet Draft, May 2000.

[10] Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M. and I. Goyret, "RADIUS Attributes for Tunnel Protocol Support", draft-ietf-radius-tunnel-auth-09.txt, Internet Draft (work in progress), August 1999 (Expired)





[11] Zorn, G., Mitton, D., "RADIUS Accounting Modifications for Tunnel Protocol Support", draft-ietf-radius-tunnel-acct-05.txt, Internet Draft (work in progress), October 1999 (Expired)

[12] B. Aboba, G. Zorn, "Implementation of L2TP Compulsory Tunneling via RADIUS", draft-ietf-radius-tunnel-imp-05.txt, Internet Draft (work in progress), 20 August 1999, (Expired)

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

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

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

## 5.0 Security Considerations

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

## 6.0 IANA Considerations

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

## 7.0 Acknowledgements

## 8.0 Authors Addresses

Ronnie Ekstein
Alcatel Network Strategy Group
Francis Wellesplein 1, 2018 Antwerp, Belgium
Phone : +32 3 241 5958
E-mail : ronnie.ekstein@alcatel.be





Yves T'Joens
Alcatel Network Strategy Group
Francis Wellesplein 1, 2018 Antwerp, Belgium
Phone : +32 3 240 7890
E-mail : yves.tjoens@alcatel.be

Marc De Vries
Alcatel Carrier Internetworking Division
De Villermontstraat 38, 2550 Kontich, Belgium
E-mail : marc.de_vries@alcatel.be

## 9.0 Full Copyright Statement