RADIUS EXTensions (radext)
Internet-Draft
Expires: January 12, 2006

H. Tschofenig
Siemens
A. Mankin
Shinkuro, Inc
T. Tsenov
Siemens
A. Lior
Bridgewater Systems
July 11, 2005

RADIUS Quality of Service Support
draft-tschofenig-radext-qos-00.txt

Status of this Memo

Copyright Notice

Abstract

This document describes an extension to the RADIUS protocol that performs authentication, authorization, and accounting for Quality-of-Service reservations.

The described extensions allow network elements to authenticate the initiator of a reservation request (if desired), to ensure that the reservation is authorized, and to account for established QoS resources.

Flexibility is provided by offering support for different authorization models and by decoupling specific QoS attributes carried in the QoS signaling protocol from the AAA protocol. This document is the RADIUS complement to the DIAMETER QoS application.

Table of Contents

1. Introduction

To meet the quality-of-service needs of applications such as voice-over-IP, it will often be necessary to explicitly request resources from the network. This will allow the network to identify packets belonging to these application flows and ensure that bandwidth, delay, and error rate requirements are met.

This document is a complement to the ongoing work of the DIAMETER QoS application described in [12]. It describes RADIUS protocol extensions supporting AAA in an environment where better than best effort Quality of Service is desired. The suggested extensions to the RFC 2865 [1], RFC 2866 [2], RFC 2869 [3] and RFC 3576 [4] satisfy the requirements defined in [13].

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [5].

3. Goals

This document has a few ambitious goals, namely:

- Decouple the QoS signaling protocol (such as NSIS, RSVP or link layer QoS signaling protocols) from the AAA protocol. This goal is accomplished with the help of a generic QoS description, the QSPEC object.

- Support for different scenarios that demand authorization for QoS reservations. The impact is to provide flexibility with regard to the entities that trigger the QoS reservation, the QoS parameters that need to be provided to the RADIUS server for authorization, the granularity of the QoS reservation (e.g., for an individual application flow, for an aggregate).

4. QoS Authorization for a Session

A request from a Quality of Service enabled RADIUS clietn starts a RADIUS message exchange. The identity of the user, and depending on the scenario, the identity of the QoS authorizing application server and optional session identification information, are assembled into a RADIUS Access-Request message by the AAA client responsible for resource allocation and sent to a AAA server either co-located with an application server, to the local AAA server or to the RADIUS server in the user's home realm.

If the authentication procedure involves multiple Access-Requests (as in EAP), the RADIUS client MUST include the QoS-attributes in at least the last Access-Request of the authentication procedure.

The server processes the information and responds with a RADIUS Access-Accept message, which contains the QoS authorization result, accounting and bearer gating information. Also, the value of the Session-Timeout attribute is set to the duration of the session, the value of the "Termination-Action" attribute is set and the "State" attribute MUST be included as stated in [1].

If the authorization decision at the RADIUS server indiates that the request cannot be completed successfully then an Access-Reject message containing the Reply-Message attribute with the reason for rejection.

4.1 Session Establishment

When the QoS authorization exchange completes successfully, an RADIUS Accounting session SHOULD start for reporting accounting information and loss of bearer. Accounting information is reported as described in [2] and [3]. Loss of bearer information is reported using Access-Request message.

4.2 QoS Re-Authorization

4.2.1 Client-side initiated Re-Authorization

The "Authorize-ONLY" Access-Request MUST NOT include either User Password or a CHAP Password. In order to protect the RADIUS message, the RADIUS client MUST include the Message-Authenticator(80) attribute. The RADIUS client will compute the value for the Message-Authenticator based on [3].

The RADIUS server processes the information including the verification of the Message-Authenticator(80) as per [3] and responds with a RADIUS Access-Accept message which contains the "Service-Type"

(6) attribute with value "Authorize-ONLY", QoS authorization, accounting, bearer gating information, and the "State" attribute with new value or a Access-Reject message containing the Reply-Message attribute with the reason of rejection.

4.2.2 Server-side initiated Re-Authorization

At any time during the QoS session the RAIDUS server MAY send a

Change-of-Authorization (CoA) message with the "Service-Type" (6) attribute with the value "Authorize-ONLY". The RADIUS client MUST respond with a Change-of-Authorization NACK message with the "Service-Type" (6) attribute with the value "Authorize-ONLY" and the Error-Cause attribute with value "Request-Initiated". The RADIUS client MUST then send an Access-Request containing "Service-Type" (6) attribute with value "Authorize-ONLY" and re-authorization information. This approach is compatible with the DIAMETER re-authorization procedure and is defined in RFC 3576 [4]. Furthermore, the "State" attribute SHOULD be used as specified in RFC 3576 [4].

4.3 Session Termination

4.3.1 Client-side initiated session termination

A QoS session may be terminated from the client side by sending a Access-Request message with unchanged "State" attribute received from the RADIUS server. This action is defined in [6].

4.3.2 Server-side initiated session termination

At anytime during a session the Authorizing Server may send a Disconnect message to terminate a session. This capability is described in detail in RFC 3576 [4]. The RADIUS server sends a Disconnect message that MUST contain identifiers that uniquely identify the subscribers data session and the RADIUS client serving that session and the "Service-Type" (6) attribute with value "Authorize-ONLY".

If the RADIUS client receives a Disconnect message, it MUST respond with the Disconnect-NACK message with "Service-Type" (6) attribute with value "Authorize-ONLY" and Error-Cause attribute with the value "Request-Initiated". If it is able to terminate the session it will send Access-Request message with "Service-Type" (6) attribute with value "Authorize-ONLY" and attributes for session termination. This message flow is required for compatibility with DIAMETER protocol. Also the "State" attribute SHOULD be used as specified in RFC 3576 [4].

5. Accounting

Application of the RADIUS protocol for QoS Authorization presented in this document use RADIUS Accounting as defined in the RFC2865, RFC2866 and RFC2869. The definition of new accounting attributes may be necessary but left for further study.

After a successful QoS authorization the RADIUS client starts the corresponding accounting session by sending the Accounting-Request message. This message SHOULD contain necessary attributes to bind the current accounting session to the reported QoS session. "Class" and "Acc-Session-ID" attributes SHOULD be used according to [1] and [2].The RADIUS server responds with a Accounting-Accept message after successfully processing the Accounting-Request message. The Accounting-Accept message MAY contain instructions for managing the accounting session, such as the Accounting-Interim-Interval AVP.

After every successful re-authorization procedure the RADIUS client SHOULD re-initiate accounting message exchange.

After successful session termination the RADIUS client SHOULD initiate a final exchange of accounting messages with the RADIUS server.

6. Attributes

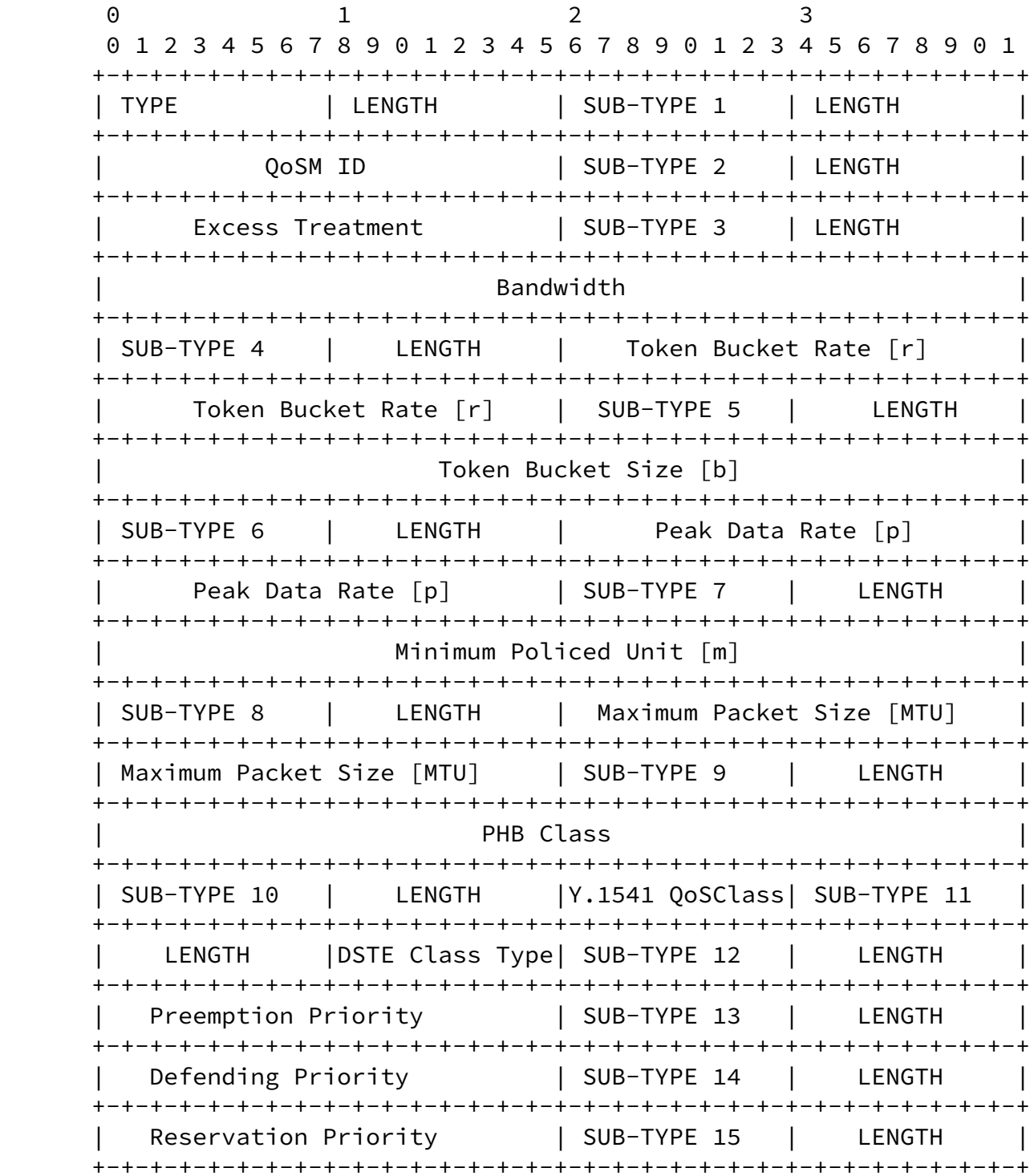
This section defines three categories of attributes:

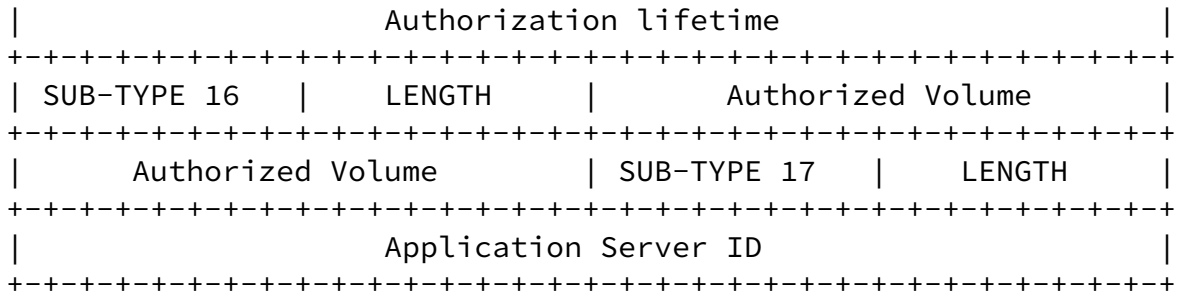
- QSPEC parameters describing requested/authorized QoS
- Identification of the flow that should receive QoS described in QSPEC
- AVPs required to carry authorization information (e.g., authorization tokens as specified in [7])

6.1 QSPEC Attribute

The generic QoS description is taken from QoS-NSLP QSpec Template [14] which aims to support QoS parameters for all QoS reservations and is independent of a specific QoS model (QOSM). The QSPEC template format is organized into QoS Control information, Requested, Reserved, Available and Minimun objects. Each of the objects contains a number of QSPEC parameters. For QoS authorization purposes only part of the parameters SHOULD be used, e.g., mainly those included into the QoS Desired and some of those included into QoS Control information objects. In addition information for duration of the authorized QoS SHOULD be provided.

QSPEC parameters and QoS authorization session management parameters are included as subtypes into the QSPEC attribute. Subtypes not used are omitted in the message.


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
TYPE
LENGTH
SUB-TYPE 1
LENGTH
QoSM ID
SUB-TYPE 2
LENGTH
Excess Treatment
SUB-TYPE 3
LENGTH
Bandwidth
SUB-TYPE 4
LENGTH
Token Bucket Rate [r]
Token Bucket Rate [r]
SUB-TYPE 5
LENGTH
Token Bucket Size [b]
SUB-TYPE 6
LENGTH
Peak Data Rate [p]
Peak Data Rate [p]
SUB-TYPE 7
LENGTH
Minimum Policed Unit [m]
SUB-TYPE 8
LENGTH
Maximum Packet Size [MTU]
Maximum Packet Size [MTU]
SUB-TYPE 9
LENGTH
PHB Class
SUB-TYPE 10
LENGTH
Y.1541 QoSClass
SUB-TYPE 11
LENGTH
DSTE Class Type
SUB-TYPE 12
LENGTH
Preemption Priority
SUB-TYPE 13
LENGTH
Defending Priority
SUB-TYPE 14
LENGTH
Reservation Priority
SUB-TYPE 15
LENGTH



Type: Value of QSPEC

Length: variable, greater than 8

String: The String value MUST be encoded as follows:

Sub-Type (=1): Sub-Type for QoS-Model ID attribute

Length : Length of QoS-Model ID attribute (= 6 octets)

QoS-Model ID (QoSM ID):

Identifier of the used QoS signaling model.[14]

Sub-Type (=2): Sub-Type for Excess Treatment attribute

Length : Length of Excess Treatment attribute (= 3 octets)

Excess Treatment:

Description of how the excess traffic to be processed (out-of-profile traffic). Excess traffic MAY be dropped, shaped and/or remarked.

Sub-Type (=3): Sub-Type for Bandwidth attribute

Length : Length of Bandwidth attribute (= 6 octets)

Bandwidth:

Link bandwidth needed by a flow.

Sub-Type (=4): Sub-Type for Token Bucket Rate attribute

Length : Length of Token Bucket Rate attribute (= 6 octets)

Token Bucket Rate:

Rate is a Token Bucket parameter as specified in [8].

Sub-Type (=5): Sub-Type for Token Bucket Size attribute

Length : Length of Token Bucket Size attribute (= 6 octets)

Token Bucket Size:

Size is a Token Bucket parameter as specified in [8].

Sub-Type (=6): Sub-Type for Peak Data Rate attribute

Length : Length of Peak Data Rate attribute (= 6 octets)

Token Bucket Size:

Peak Data Rate is a Token Bucket parameter as specified in [8].

Sub-Type (=7): Sub-Type for Minimum Policed Unit attribute

Length : Length of Minimum Policed Unit attribute (= 6 octets)

Minimum Policed Unit:

Minimum Policed Unit is a Token Bucket parameter as specified in [8].

Sub-Type (=8): Sub-Type for Maximum Packet Size [MTU] attribute

Length : Length of Maximum Packet Size [MTU] attribute (= 6 octets)

Maximum Packet Size [MTU]:

Maximum Packet Size [MTU] is a Token Bucket parameter as specified in [8].

Sub-Type (=9): Sub-Type for PHB class attribute

Length : Length of PHB class attribute (= 6 octets)

PHB class:

Indicates the QoS class used in DiffServ per-hop behavior QoS signaling [9].

Sub-Type (=10): Sub-Type for Y.1541 QoS class attribute

Length : Length of Y.1541 QoS class attribute (= 3 octets)

Y.1541 QoS class:

Indicates the Y.1541 QoS Class [15].

Sub-Type (=11): Sub-Type for DSTE class attribute

Length : Length of DSTE class attribute (= 3 octets)

DSTE Class:

Indicates the QoS class used in DiffServ-enabled MPLS traffic engineering.[10].

Sub-Type (=12): Sub-Type for Preemption Priority attribute

Length : Length of Preemption Priority attribute (= 4 octets)

Preemption Priority:

Parameter used in the process of differentiation of flows. Indicates the priority of the new flow compared with the defending priority of previously admitted flows.

Sub-Type (=13): Sub-Type for Defending Priority attribute

Length : Length of Defending Priority attribute (= 4 octets)

Defending Priority:

Parameter used in the process of differentiation of flows. It is compared with the preemption priority of new flows.

Sub-Type (=14): Sub-Type for Reservation Priority attribute

Length : Length of Reservation Priority attribute (= 4 octets)

Reservation Priority:

Parameter used in the process of differentiation of flows for emergency services, ETS, E911, etc., and assigning them a higher admission priority.

Sub-Type (=15): Sub-Type for Authorization lifetime attribute

Length : Length of Authorization lifetime attribute (= 6 octets)

Authorization lifetime:

The parameter indicates the duration of the authorized QoS provisioning.

Sub-Type (=16): Sub-Type for Authorized volume attribute

Length : Length of Authorized volume attribute (= 6 octets)

Authorized volume:

The parameter indicates the data volume that should receive the authorized QoS.

Sub-Type (=17): Sub-Type for Application server ID attribute

Length : Length of Authorized volume attribute (IPv4 = 6 octets, IPv6= 18 octets)

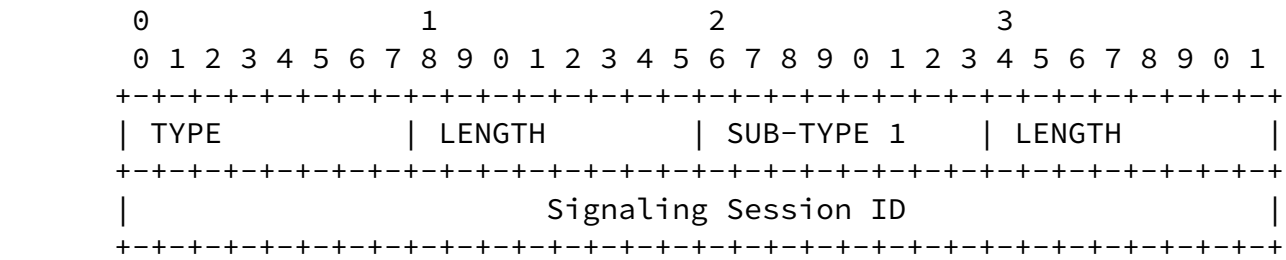
Application server ID:

Application server ID indicates the address of the authorizing Application Server.

Provided QSPEC parameters list is not exhaustive and SHOULD be updated according to [14].

6.2 Flow Identification

Depending on the deployment and used QoS signaling protocol, identification of the flow that SHOULD received authorized QoS takes a different format. Signaling session Identifier (NSIS) or flow identifier and explicit filter specifications are used. The Attribute QoS-Flow-ID is designated to encapsulate such information.



Type : Value of QoS-Flow-ID

Length: variable, greater than 8

String: The String value MUST be encoded as follows:

Sub-Type (=1): Signaling Session ID

Length : Length of Signaling Session ID attribute (= 6 octets)

Signaling Session ID:

In NSIS framework [11], Signaling session ID is an unique identifier of the signaling session that remains unchanged for the duration of the session. It is locally mapped to the specific flow identifiers.

Additional Sub-Type attributes SHOULD be added, which combined with filter specifications (such as QoS-Filter-Rule [16]) provide flow identification. [TBD]

6.3 Authorization Objects

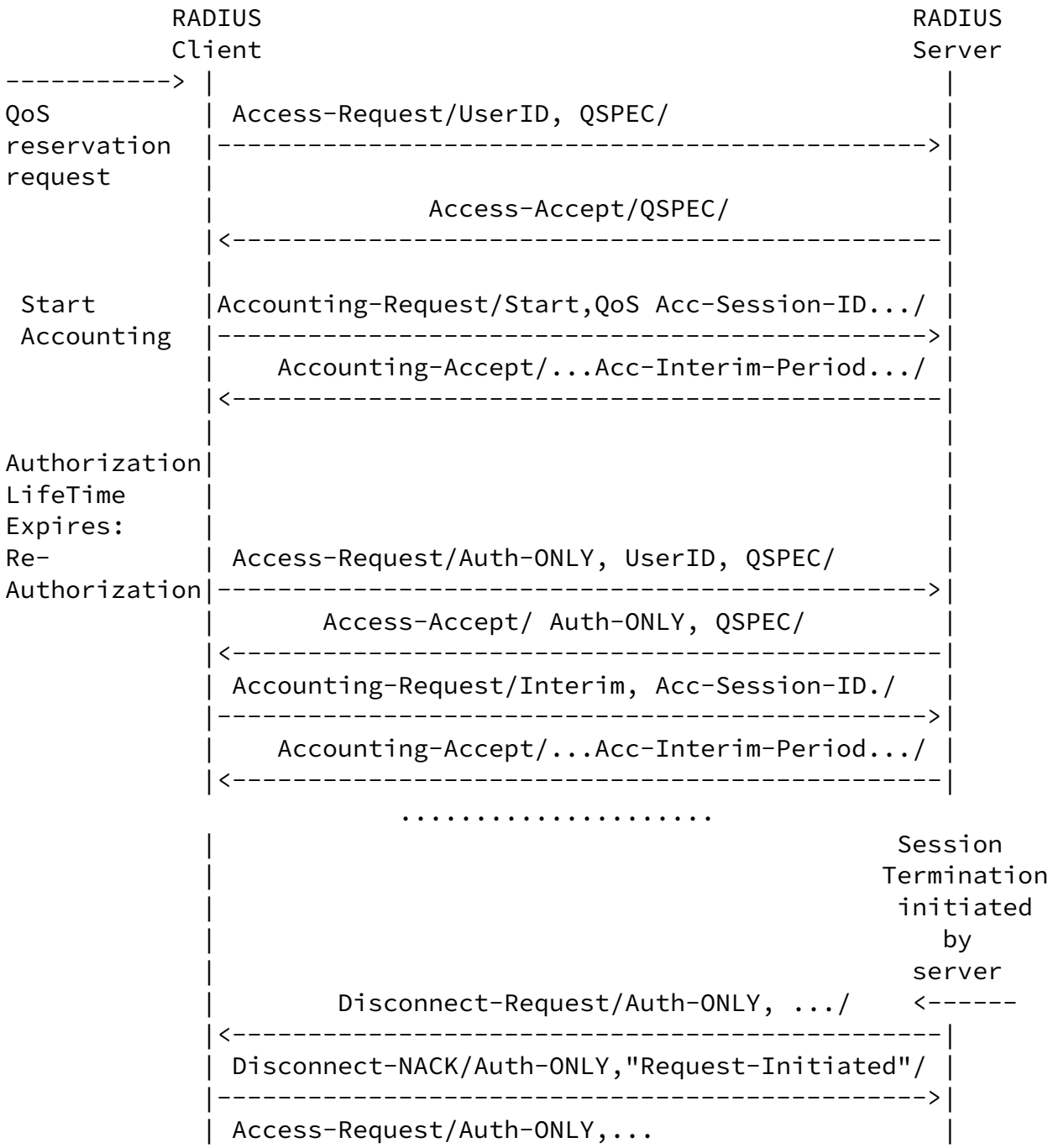
TBD:

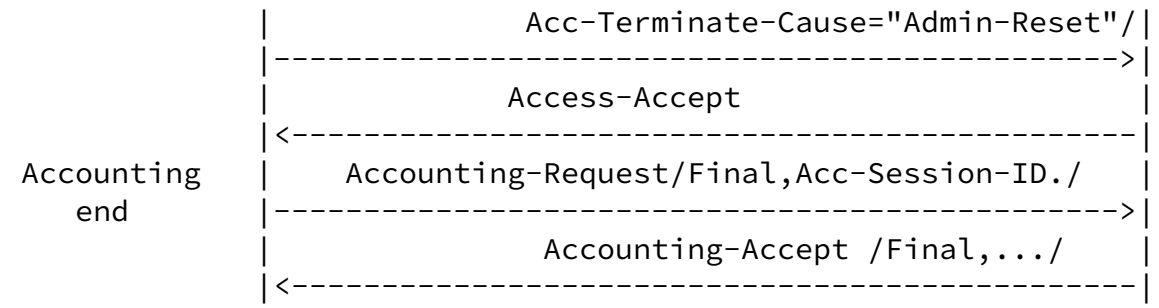
7. Diameter RADIUS Interoperability

In deployments where RADIUS clients communicate with DIAMETER servers or DIAMETER clients communicate with RADIUS servers then a translation agent will be deployed and operate. The DIAMETER-QoS specification [12] provides a natural candidate for mapping the RADIUS QoS related AVPs to DIAMETER AVPs and messages.

8. Examples

TBD: Description of the example goes in here.





9. Security Considerations

For this extension to RADIUS protocol the security considerations defined in RFC2865 [1], RFC2866 [2], RFC2869 [3] and RFC3576 [4] are applicable. Furthermore, the security of the QoS signaling protocol and the QoS authorization framework must be considered in the evaluation of the security properties.

[Editor's Note: A more detailed treatment will be provided in a future document version.]

10. Acknowledgments

We would like to thank Pete McCann and Franck Alfano for their work on the DIAMETER QoS application.

11. References

11.1 Normative References

[1] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

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

[3] Rigney, C., Willats, W., and P. Calhoun, "RADIUS Extensions", RFC 2869, June 2000.

[4] Chiba, M., Dommety, G., Eklund, M., Mitton, D., and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 3576, July 2003.

[5] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", March 1997.

[6] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[7] Hamer, L-N., Gage, B., Kosinski, B., and H. Shieh, "Session Authorization Policy Element", RFC 3520, April 2003.

[8] Shenker, S. and J. Wroclawski, "General Characterization Parameters for Integrated Service Network Elements", RFC 2215, September 1997.

[9] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, December 1998.

[10] Le Faucheur, F. and W. Lai, "Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering", RFC 3564, July 2003.

[11] Hancock, R., Karagiannis, G., Loughney, J., and S. Van den Bosch, "Next Steps in Signaling (NSIS): Framework", RFC 4080, June 2005.

11.2 Informative References

[12] Alfano, F., "Diameter Quality of Service Application", draft-alfano-aaa-qosprot-02 (work in progress), February 2005.

[13] Alfano, F., "Requirements for a QoS AAA Protocol",

draft-alfano-aaa-qosreq-01 (work in progress), October 2003.

[14] Ash, J., "QoS-NSLP QSPEC Template", draft-ietf-nsis-qspec-04 (work in progress), May 2005.

[15] Ash, J., "Y.1541-QOSM -- Y.1541 QoS Model for Networks Using Y.1541 QoS Classes", draft-ash-nsis-y1541-qosm-00 (work in progress), May 2005.

[16] Congdon, P., "RADIUS Extensions for IEEE 802", draft-congdon-radext-ieee802-03 (work in progress), February 2005.

Authors' Addresses

Hannes Tschofenig
Siemens
Otto-Hahn-Ring 6
Munich, Bavaria 81739
Germany

Email: Hannes.Tschofenig@siemens.com
URI: http://www.tschofenig.com

Allison Mankin
Shinkuro, Inc
1025 Vermont Avenue
Washington, DC 20005
US

Phone: +1 301-728-7199 (mobile)
Email: mankin@psg.com

Tseno Tsenov
Siemens
Otto-Hahn-Ring 6
Munich, Bayern 81739
Germany

Email: tseno.tsenov@mytum.de

Avi Lior
Bridgewater Systems Corporation
303 Terry Fox Drive
Ottawa, Ontario K2K 3J1
Canada

Phone: +1 613-591-6655
Email: avi@bridgewatersystems.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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