RADIUS EXTensions (radext)
Internet-Draft
Expires: April 25, 2006

H. Tschofenig
Siemens
A. Mankin
Shinkuro, Inc
T. Tsenov
Siemens
A. Lior
Bridgewater Systems
October 22, 2005

RADIUS Quality of Service Support
draft-tschofenig-radext-qos-02.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. RADIUS functional considerations

Being a value-added service, QoS provisioning SHOULD go along with explicit authorization, accounting and control over the QoS-featured user session. Specifically, the management of the authorized session with Session-Timeout(27) and Termination-Action(29) attributes raises a number of issues, identified in [14]. The solution presented in this document aims to allow explicit control by the RADIUS server (Authorizing entity) over the authorization session and its parameters. In addition, it aims to support flexible deployment scenarios of QoS authorization and parameter provisioning by Authorization entities, which know the user and its subscription profile (Home AAA server) or can provide authorization for a session requested by the user (Application server). QoS authorization and parameter provisioning MAY be incorporated into initial

authentication and authorization RADIUS exchange or MAY be triggered at a later moment by a reception of a QoS signalling message.

5. Authorization and QoS parameter provision

5.1. QoS enabled initial access authentication and authorization

QoS enabled RADIUS client (NAS) initiates the authentication and authorization process by sending a RADIUS Access-Request to the user's Home AAA server. In addition to authentication related attributes, it includes the QSPEC(TBD) attribute, which MAY specify

the QoS-Model [15] supported by the NAS and description of the currently available QoS resources or description of the QoS explicitly requested by the user. In the second case, additional session and flow identification information MIGHT be included together with the identity of the QoS authorizing application server.

If the authentication process involves multiple Access-Requests (as in EAP), the RADIUS client MUST include the QSPEC(TBD) attribute and any additional QoS-authorization related information in at least the last Access-Request of the authentication process.

The Home AAA server receives the Access-Request message and authenticates the user. Based on the user profile it determines the subscription QoS parameters and includes them into the QSPEC(TBD) attribute of the Access-Accept message.

In case that the QoS authorization MUST be done by an Application server, which identity is included into the Access-Request message, the Home server forwards the Access-Request to the Application server. The Access-Request will contain the QSPEC(TBD) attribute and session identification information. Upon successful authorization, the Application server generates an Access-Accept containing the QSPEC(TBD) attribute, flow identification information and optionally bearer gating information.

The QSPEC attribute returned to the client SHOULD contain the duration of the QoS enabled session.

If the authentication or authorization of the user is not successful, the Home AAA server or the application server sends back an Access-Reject message containing Reply-Message(18) attribute with the reason for rejection.

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

5.2. Mid-Session QoS authorization

5.2.1. Client-side initiated QoS authorization/re-authorization

Two types of QoS-related events MIGHT initiate Authorize-Only Access-Request messages - reception of a QoS signaling message or expiration of authorization lifetime of ongoing QoS-enabled session. In both cases, the RADIUS client sends an Access-Request with Service-Type(6) attribute set to a value of "Authorize-Only", QSPEC(TBD) attribute and session and flow identification information. The QSPEC(TBD) attribute includes description of new QoS parameters explicitly required by the user or the QoS parameters that SHOULD be re-authorized. Session and flow (only in the re-authorization case) identification information SHOULD be the same as those used during the initial Access-Request. For example, if the User-Name(1) attribute was used in the initial Access-Request it MUST be included, especially if the User-Name(1) attribute is used to route the Access-Request to the Home RADIUS server.

The "Authorize-ONLY" Access-Request MUST NOT include either User Password(2) or a CHAP Password(3). 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(80) based on [3].

The RADIUS server processes the information, including the verification of the Message-Authenticator(80) as per [3], and upon successful authorization it responds with a RADIUS Access-Accept message. It contains the Service-Type(6) attribute with value "Authorize-ONLY", the QSPEC(TBD) attribute, flow identification information and optionally bearer gating information. The QSPEC(TBD) attribute returned to the client SHOULD contain the new duration of the QoS enabled session. In case of unsuccessful authorization an Access-Reject message is sent, containing the Reply-Message(18) attribute with the reason of rejection.

In case that an Application server MUST be contacted for the QoS authorization, the Home server forwards the Access-Request to the indicated Application server, which processes the QoS authorization request.

5.2.2. Server-side initiated Re-Authorization

In order to take advantage of the dynamic authorization capabilities of RADIUS as defined in [4], the Authorization entity (Home or Application server) MUST be sure that the RADIUS client supports them too. An advertising approach proposed in [14] MIGHT be used.(TBD)

At any time during the QoS session the RADIUS server MAY send a Change-of-Authorization (CoA) message with Service-Type(6) attribute set to value "Authorize-ONLY" and session and flow identification information. The RADIUS client MUST respond with a Change-of-Authorization NACK message with Service-Type(6) attribute with value "Authorize-ONLY" and Error-Cause(101) attribute set to value "Request-Initiated". The RADIUS client MUST then send an Access-Request containing Service-Type(6) attribute with value "Authorize-ONLY", QSPEC(TBD) attribute, session and flow identification 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].

5.3. Session Termination

5.3.1. Client-side initiated session termination

Service session MAY be related to a particular authorized QoS-provisioned data flow. In this case, session termination MAY be caused by a QoS signaling tear down message or loss of bearer report. In another scenario the service session is a QoS enabled access session, which can handle authorization of several QoS-provisioned user's data flows. In this case session termination MAY be caused by user log-off.

A RADIUS client indicates session termination by sending an Accounting-Request message with Acc-Status-Type(40) attribute set to "Stop" value and final QoS related accounting records(TBD).

5.3.2. Server-side initiated session termination

At anytime during a session the Authorizing Server may send a Disconnect message to terminate the session. This capability is described in detail in RFC 3576 [4]. The RADIUS server sends a Disconnect message that MUST contain identifiers that uniquely determine the subscriber's session and the RADIUS client serving that session and 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(101) attribute with 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(24) attribute SHOULD be used as specified in RFC 3576

[4].

6. Accounting

Application of the RADIUS protocol for QoS authorization presented in this document use RADIUS Accounting as defined in the RFC2865 [1], RFC2866 [2] and RFC2869 [3]. The attributes containing a QoS description and flow identification (see Section 7) are used in the accounting session for reporting the status and parameters of the provided QoS. The definition of new accounting attributes may be necessary. This aspect is 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(25) and Acc-Session-ID(44) attributes SHOULD be used according to [1] and [2]. The RADIUS server responds with an Accounting-Response message after successfully processing the Accounting-Request message. The Accounting-Response message MAY contain instructions for managing the accounting session, such as the Acct-Interim-Interval(85) attribute.

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

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

7. Attributes

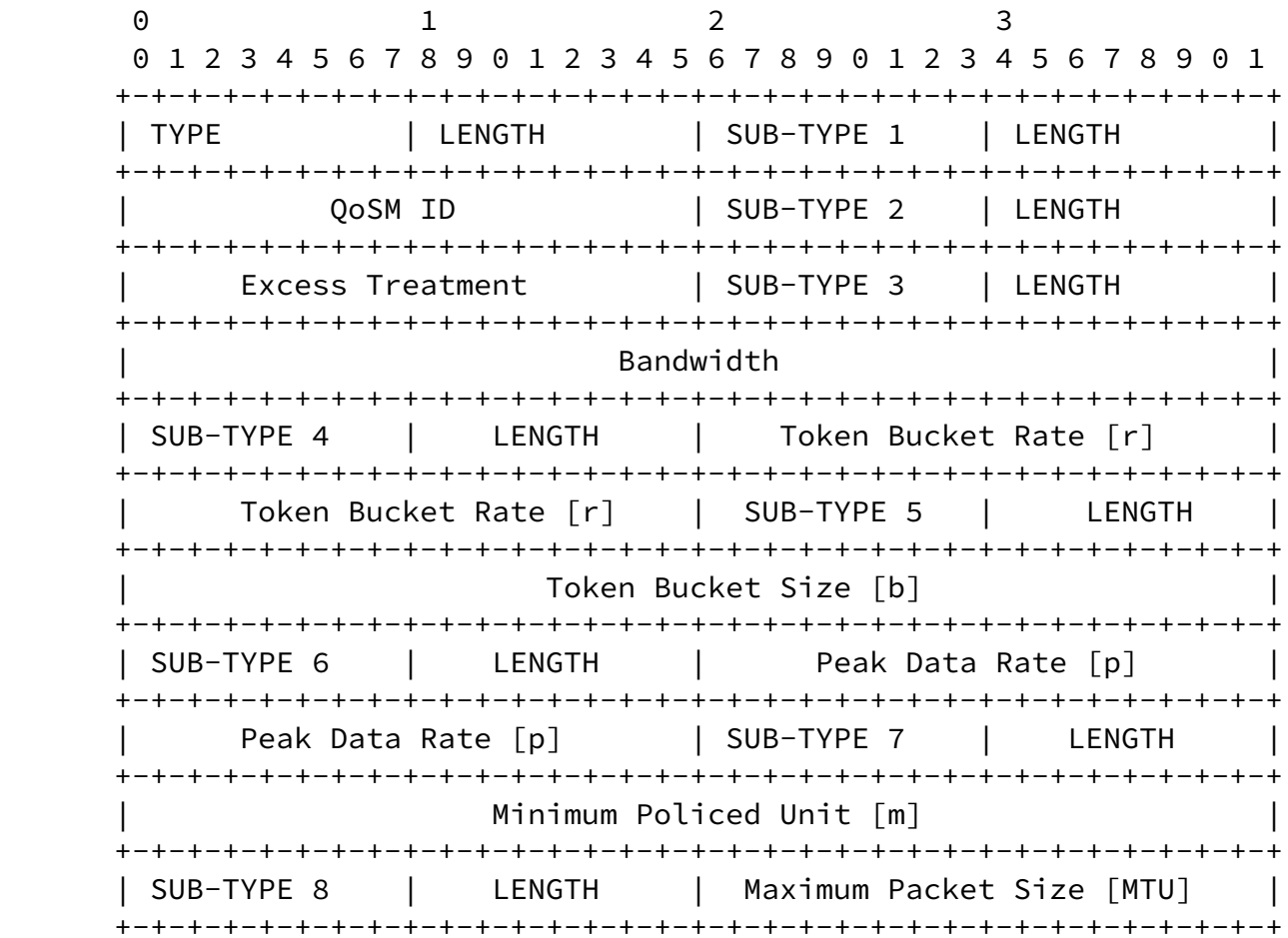
This section defines three categories of attributes:

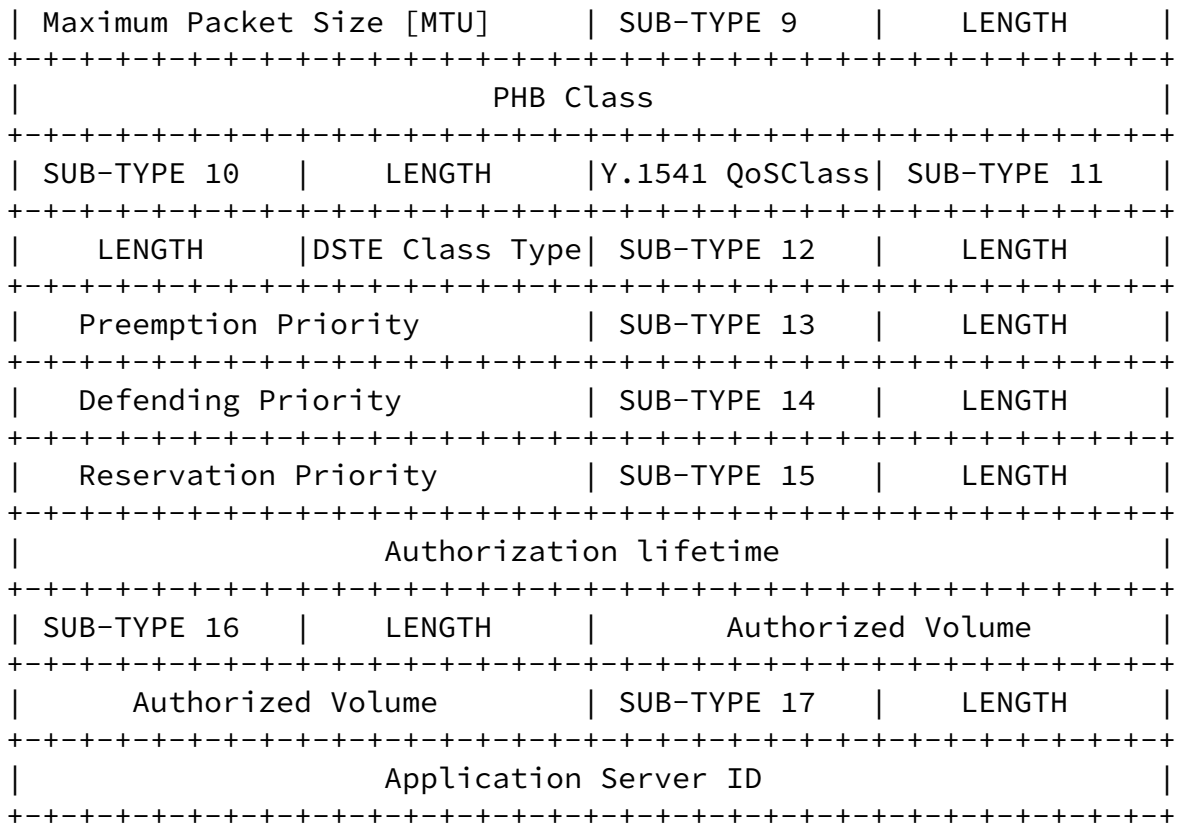
- QSPEC parameters describing requested/authorized QoS
- Identification of the flow that should receive QoS described in QSPEC
- Attributes required to carry authorization information (e.g., authorization tokens as specified in [6])

7.1. QSPEC Attribute

The generic QoS description is taken from QoS-NSLP QSpec Template [15] 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 Minimum 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]



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.[15]

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 [7].

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 [7].

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 [7].

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 [7].

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 [7].

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 [8].

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 [16].

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.[9].

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. [Editor's Note: Reference to be included here.]

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)

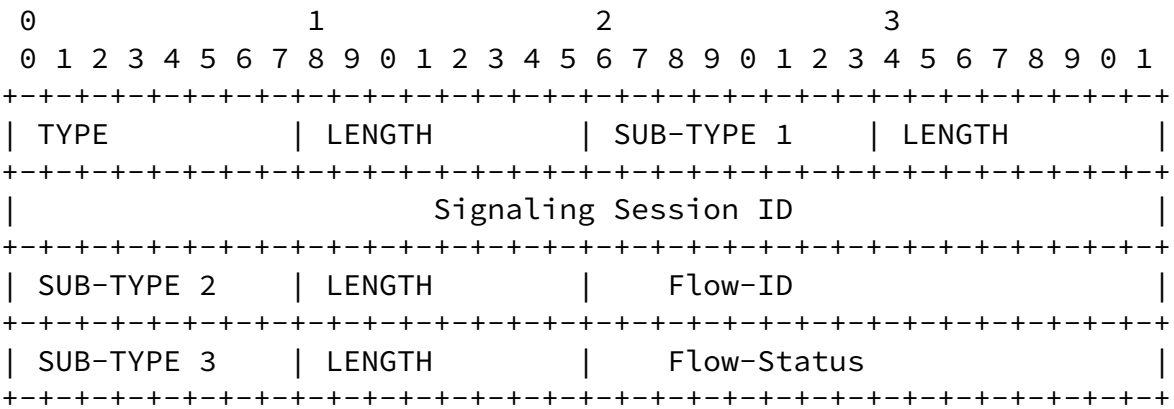
Application server ID:

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

Provided QSPEC parameters list is not exhaustive and SHOULD be updated according to [15].

7.2. Flow Identification

Depending on the deployment and used QoS signaling protocol, identification of the flow that SHOULD receive 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:

With the NSIS framework [10], a signaling session ID is a unique identifier of the signaling session that remains unchanged for the entire lifetime of the session. It is locally mapped to the specific flow identifiers.

Sub-Type (=2): Flow-ID

Length : Length of Flow-ID attribute

Flow-ID:

The Flow-ID attribute is an application assigned identifier for an IP flow that identifies the IP flow in an application layer session (e.g., SIP/SDP). It might be used in conjunction with a QoS-Filter-Rule [17] attribute for provision of flow description and identification. Note that more than one Flow-ID sub-attributes MAY be present in the QoS-Flow-Id attribute.

Sub-Type (=3): Flow-State

Length : Length of Flow-State attribute

Flow-State:

The Flow-State attribute indicates the action that MUST be performed on the flow(s) to which QoS authorization message exchange applies as identified by the QoS-Flow-Id. The flow could

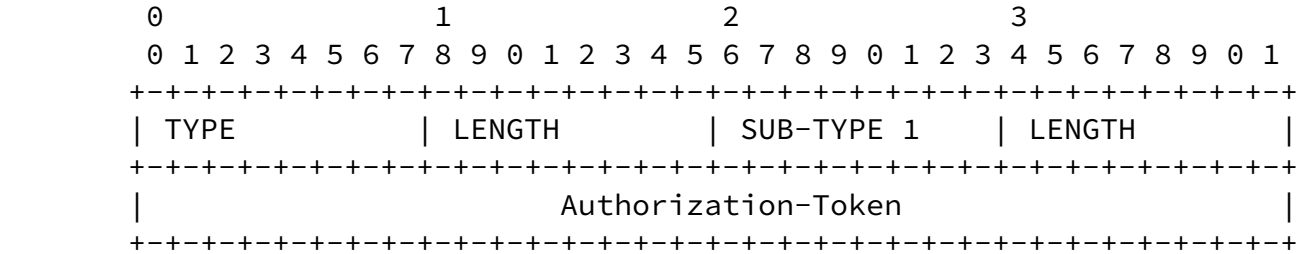
be enabled (i.e., it is allowed to trespass the QoS element) and it is treated according to the QoS described in the QSPEC attribute. The flow could be disabled, i.e., the QoS described in the QSPEC could be reserved but additional authorization approval by the Authorizing entity is required in order for the flow to receive this QoS treatment and to trespass the QoS element.

In the current approach, there is a one to one binding between a

QSPEC and a QoS-Flow-Id attribute in a RADIUS message. It is for further study whether different QoS authorization information (i.e., multiple QSPEC attributes) for different groups of flows (i.e., multiple QoS-Flow-Id attributes) might need to be carried in a single RADIUS message.

7.3. Authorization Objects

Depending on the deployment, different attributes MAY be used as an input for computing the QoS authorization decision by the Authorizing entity. In addition to the credentials of the end host, requesting QoS reservation (e.g., User-Name(1) attribute), an authorization token MAY be used. This occurs in a deployment scenario, where the QoS parameters are negotiated as part of an application layer signaling exchange and where the authorization decision at this application layer exchange needs to be associated with the authorization of the QoS reservation of the QoS signaling exchange. The QoS-Authorization-Data attribute is designated to encapsulate such information.



Type : Value of QoS-Authorization-Data

Length: variable, greater than 8

String: The String value MUST be encoded as follows:

Sub-Type (=1): Authorization-Token

Length : Length of Authorization-Token attribute

Authorization-Token:

The Authorization-Token sub-attribute is a container that encapsulates an authorization token received via the QoS signaling message typically sent by the end host. The token is generated by the Authorizing entity during the application layer signaling exchange and identifies the application service session, for which the QoS reservation request applies. A possible structure for the

authorization token is proposed in context of RSVP [6], with the Open Settlement Protocol (OSP) [18] or using SAML as outlined in [19] and [20]. The structure of the token is considered to be out of the scope for this document.

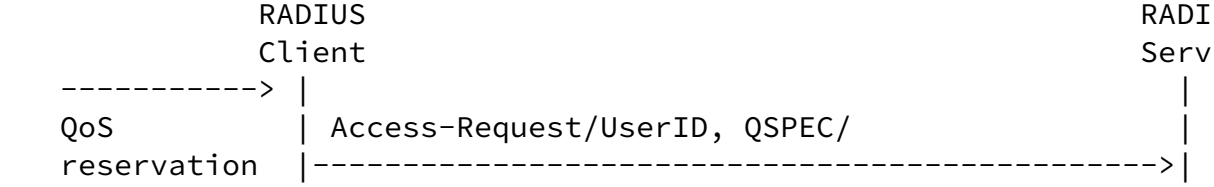
8. Diameter RADIUS Interoperability

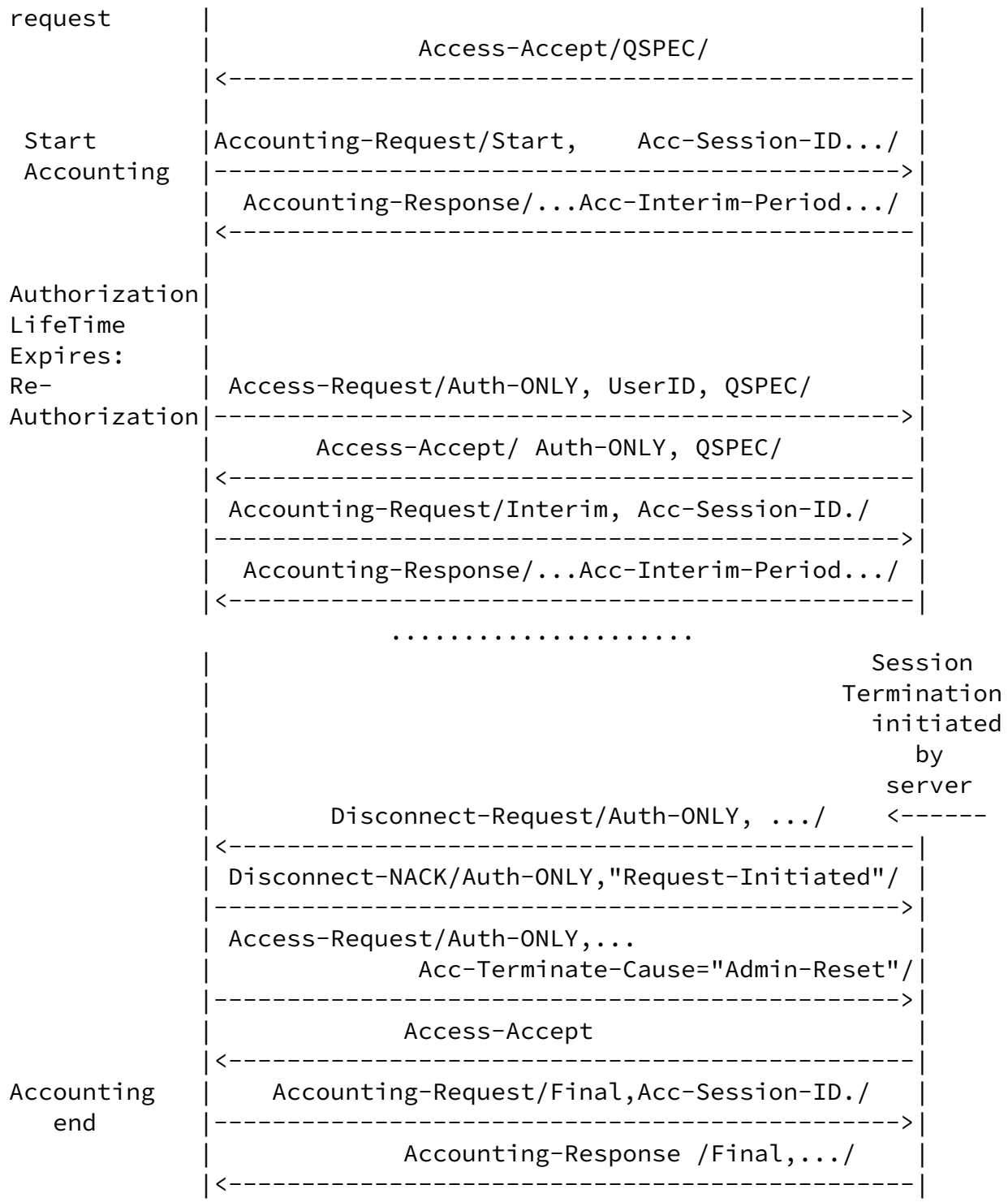
In deployments where RADIUS clients communicate with DIAMETER servers or DIAMETER clients communicate with RADIUS servers then a translation agent will be deployed and operate. The DIAMETER-QoS specification [12] provides a natural candidate for mapping the RADIUS QoS related AVPs to DIAMETER AVPs and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

9. Examples

The following diagrams show RADIUS protocol interactions for different scenarios and deployment architectures.

9.1. RADIUS authorization of a QoS signaling reservation request


RADIUS
Client
RADIUS
Server
QoS
reservation
Access-Request/UserID, QSPEC/



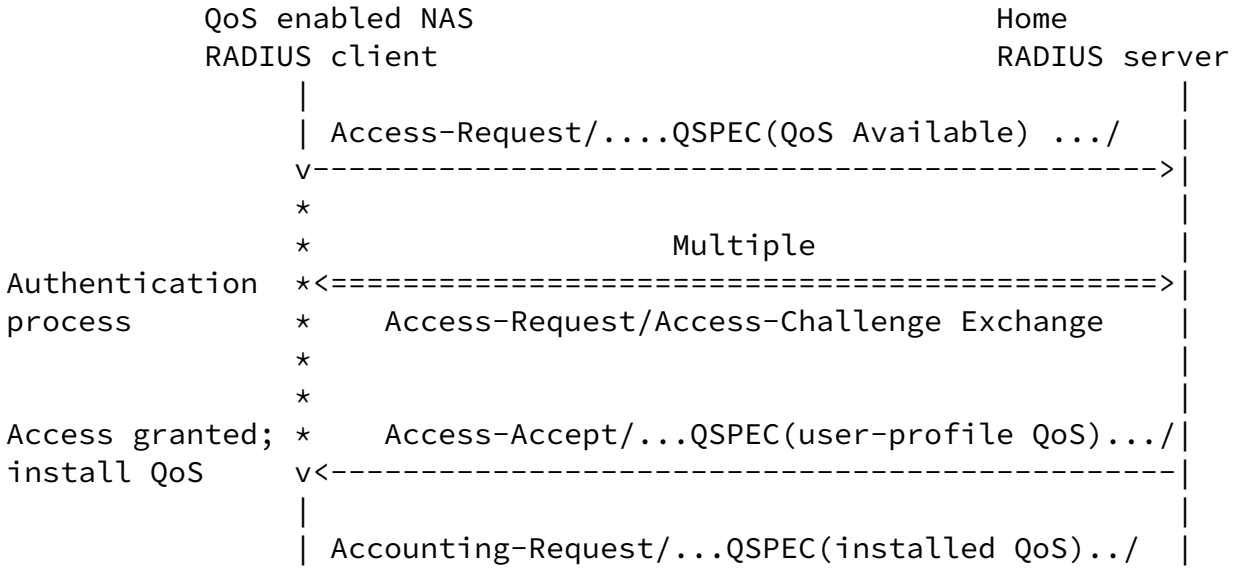
This example shows the protocol exchange between the RADIUS client and the RADIUS server. An incoming QoS reservation request received at the QoS policy aware node (i.e., RADIUS client) invokes the

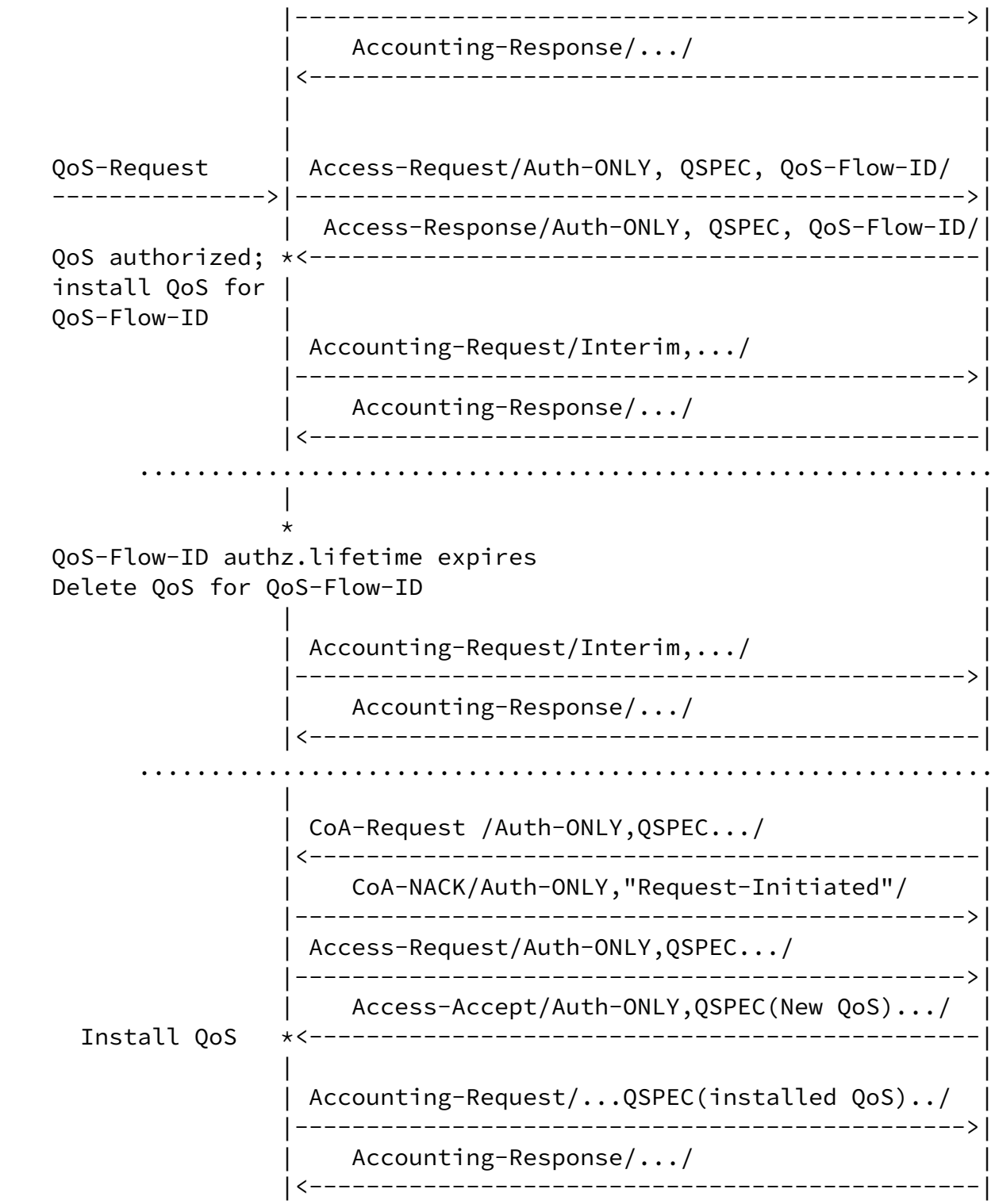
transmission of a Access-Request message (AR) to the RADIUS server. This message contains the requested QoS resources in a QSPEC attribute along with user identification and authentication information. After the request is successfully authenticated and authorized, the RADIUS server replies with a Access-Accept message (AA), which grants a reservation for a certain amount of resources (as included in the QSPEC attribute). After the successful exchange of the AR/AA messages, the RADIUS client starts an accounting session by sending an Accounting-Request message. The server replies with an Accounting-Response message that MAY include instructions for further handling of the accounting session, such as the Acc-Interim-Period attribute.

The client-side re-authorization caused by expiration of the authorization lifetime initiates an Authorize-ONLY Access-Request / Access-Accept message exchange. After a successful re-authorization an Accounting-Request message SHOULD be sent to indicate the new authorization parameters. The server replies with an Accounting-Response message.

In this example, the RADIUS server initiates a session termination. It therefore sends a Disconnect-Request message. The client responds with a Disconnect-NACK message and sends an AR message indicating the termination cause. The server replies to the AR message with an AA message. After receiving the AA message sent by the server, the client sends remaining accounting information with the Accounting-Request message. The server replies with the Accounting-Response message.

9.2. RADIUS authentication, authorization and management of a QoS-enabled access session





This example shows the interaction between a QoS enabled NAS and a

Home AAA server. This example aims to show a QoS-enabled access session. The NAS performs authorization of the QoS-provisioned flows as part of the user's access session.

The NAS performs initial authentication and authorization of the end user for an access session. This process MAY take several Access-

Request / Access-Challenge message exchanges. By including the QSPEC attribute, the RADIUS server provides a description of the QoS parameters of the user access session. The NAS allocates certain QoS resources according to the QoS parameters provided by the RADIUS server and currently available QoS resources. The NAS initiates an accounting session by sending the Accounting-Request message in which it reports the actually allocated QoS resources for the access session. The server replies with an Accounting-Response message that MAY include instructions for further handling of the accounting session, such as the Acc-Interim-Period attribute.

Later, when the NAS intercepts a QoS signaling message sent from the end host an Authorize-ONLY Access-Request message is triggered and sent to the RADIUS server. It includes the description of the requested QoS resources in the QSPEC attribute. Optionally, an identifier of the flow that should receive the requested QoS treatment is included into the Access-Request message. The RADIUS server (in the user's home domain) validates the QoS request and replies with Authorize-ONLY Access-Accept message. The message includes a QSPEC attribute with description of the authorized QoS parameters and the duration of authorization. An identifier of the flow that should receive the requested QoS is also provided. The RADIUS client will install a QoS reservation based on the provided QoS parameters for that flow and sends an Accounting-Request message reporting the new QoS session. The server replies with an Accounting-Response message.

In this example, the authorization lifetime of the QoS-provisioned flow expires. The NAS releases the reserved QoS resources allocated for the flow when the authorization has expired. In addition, the NAS sends an Accounting-Request message to the RADIUS server, indicating the stop of QoS provisioning for the flow.

If the Home AAA server decides to change QoS parameters for the user's access session it sends an Authorize-ONLY Change-of-

Authorization-Request message to the RADIUS client, identifying the affected access session. The NAS replies with a CoA-NACK message indicating that an Access-Request has to be generated. The Authorize-ONLY Access-Request message contains the QSPEC attribute with the QoS resources currently available at the NAS. The RADIUS server replies with the Authorize-ONLY Access-Accept message with a QSPEC attribute containing the new QoS parameters that should be provided to the user's session. The NAS allocates certain QoS resources according to the QoS parameters provided by the RADIUS server and the currently available QoS resources. It sends an Accounting-Request message in which it reports the actual allocated QoS resources for the access session. The server replies with an Accounting-Response message.

10. 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.]

11. Acknowledgments

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

12. References

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

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

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

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

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

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

12.2. Informative References

[12] Alfano, F., "Diameter Quality of Service Application", draft-alfano-aaa-qosprot-04 (work in progress), September 2005.

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

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

[14] Lior, A., "PrePaid Extensions to Remote Authentication Dial-In User Service (RADIUS)", draft-lior-radius-prepaid-extensions-08 (work in progress), July 2005.

[15] Ash, J., "QoS-NSLP QSPEC Template", draft-ietf-nsis-qspec-06

(work in progress), October 2005.

[16] 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.

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

[18] European Telecommunications Standards Institute, "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Open Settlement Protocol (OSP) for Inter-domain pricing, authorization, and usage exchange", TS 101 321.

[19] Peterson, J., "Trait-based Authorization Requirements for the Session Initiation Protocol (SIP)", draft-ietf-sipping-trait-authz-01 (work in progress), February 2005.

[20] Tschofenig, H., "Using SAML for SIP", draft-tschofenig-sip-saml-04 (work in progress), July 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.