Authentication, Authorization and
Accounting
Internet-Draft
Expires: January 10, 2005

F. Alfano
P. McCann
Lucent Technologies
H. Tschofenig
Siemens
July 12, 2004

Diameter Quality of Service Application
draft-alfano-aaa-qosprot-00.txt

Status of this Memo

Copyright Notice

Abstract

This document describes a Diameter Application that performs Authentication, Authorization, and Accounting for Quality-of-Service reservations. This protocol is used by elements along the path of a given application flow to authenticate a reservation request, ensure that the reservation is authorized, and to account for resources used during the life of the application flow. This QoS AAA protocol may be used between any bearer-level network element that lies on the

path of an application flow and an application server that lies anywhere in the network, allowing for a wide variety of flexible service deployment models.

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. By performing admission control on individual flows, the network can avoid congestion and the resulting high packet drop rates.

When bandwidth is expensive and must be carefully managed, such as in wide-area cellular networks, and/or when applications and transport protocols lack the capability or cannot be trusted to perform congestion control, explicit reservation techniques are required. A variety of protocols could be used to make a reservation request, such as:

- RSVP
- NSIS
- Link-specific means
- SIP/SDP

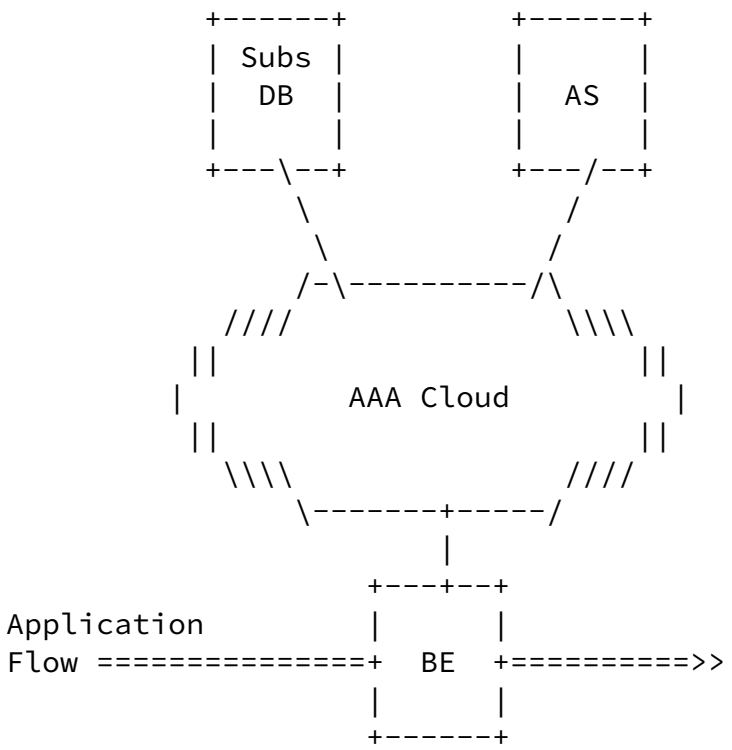


Figure 1: An architecture supporting QoS-AAA

Figure 1 depicts a bearer element through which application flows need to pass, a cloud of AAA servers, a database containing subscriber records, and an application server. Here the term "AAA Cloud" is used to refer to the network of AAA proxy/broker arrangements that may be in place. Also, note that there may be more

than one bearer element that needs to interact with the AAA cloud along the path of a given application flow, although the figure only depicts one for clarity. Similarly, a given user may have subscriber records stored in more than one place and might make use of multiple application servers. In the simplest case, bearer elements will request authentication and authorization for QoS from the AAA cloud, which will route the request to the home network and consult a static subscriber record of the endpoint making the request and return a grant/deny decision. In more complex deployment models, the authorization will be based on dynamic application state, so the request must be authenticated and authorized based on information from one or more application servers. If defined properly, the interface between the bearer element and AAA cloud would be identical in both cases. Bearer elements are therefore insulated from the details of particular applications and need not know that application servers are involved at all. Also, the AAA cloud would naturally encompass business relationships such as those between network operators and third-party application providers, enabling flexible intra- or inter-domain authorization, accounting, and settlement.

This document describes a Diameter Application protocol that is used for AAA in an environment where user applications request better than best effort Quality of Service. This Diameter QoS application protocol when combined with [RFC3588], satisfies the QoS related requirements defined in [I-D.alfano-aaa-qosreq].

This document first describes the operation of a Diameter QoS application. Then it defines the Diameter message Command-Codes. The following sections enumerate the AVPs used in these messages.

Diameter nodes conforming to this specification MAY advertise support by including the value of TBD in the Auth-Application-Id or the Acct-Application-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands [RFC3588].

The value of TBD (TBD) MUST be used as the Application-Id in all QAR and QAA commands. The value of TBD (TBD) MUST be used as the Application-Id in all ACR/ACA commands, because this application defines new, mandatory AVPs for accounting. The value of zero (0) SHOULD be used as the Application-Id in all STR/STA, ASR/ASA, and RAR/RAA commands, because these are defined in the Diameter base

protocol and no additional mandatory AVPs for those commands are defined in this document.

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 [RFC2119].

Furthermore, we use terminology defined in [RFC3588].

3. QoS Authorization for a Session

The request for a quality of service enabled bearer starts a Diameter QoS message exchange. The identity of the user, message authentication information, and depending on the scenario, the identity of the QoS authorizing application server and session identification information, are assembled into a Diameter QoS

Authorization Request (QAR) message by the bearer control element(s) responsible for resource allocation and sent either to the identified application server, or to a supporting diameter server in the user's home realm.

The server processes the information and responds with a Diameter QoS Answer message (QAA) which contains QoS authorization, accounting, and bearer gating information, or a failure code(Result-Code AVP).

3.1 Session Establishment

When the QoS authorization exchange completes successfully, the QoS Diameter application SHOULD start a session context for reporting accounting information and loss of bearer. Accounting information is reported as described in [RFC3588] and as extended in this Diameter application. Loss of bearer information is reported using Diameter QoS defined command codes (QAR) and AVPs.

3.2 QoS Re-Authorization

It is for further study whether a re-authorization capability is required. Thereby an application server can specify a period of time for which an application is authorized to use QoS resources.

3.3 Session Termination

A Diameter QoS Session is terminated when the authorizing entity sends an Abort Session Request [RFC3588] to the bearer control element, either in response to a loss of bearer report, or session termination at the application layer.

4. Diameter QoS Messages

This section defines new Diameter message Command-Code [RFC3588] values that MUST be supported by all Diameter implementations that conform to this specification. The Command Codes are:

Command-Name	Abbrev.	Code	Reference
QoS-Request	QAR	XXX	Y.1
QoS-Answer	QAA	XXX	Y.2

4.1 QoS-Request (QAR) Command

The QoS-Request message (QAR), indicated by the Command-Code field set to XXX and 'R' bit set in the Command Flags field, is used by bearer control elements to request quality of service related resource authorization for a given user and application flow.

The message MUST carry authenticating information to validate that the QAR-Request is coming from a valid bearer element. The Request SHOULD carry enough information to identify the user. If the QoS-Request is intended for a specific application server, the Request MUST include session identification AVPs.

Message Format

```
<QoS-Request> ::= < Diameter Header: XXX, REQ, PXY >
                        < Session-Id >
                        { Auth- Application-Id }
                        { Origin-Host }
                        { Origin-Realm }
                        { Destination-Host }
                        { Destination Realm }
                        { Auth-Request-Type }
                        [ QoS-Account-Corr-Id ]
                        [ User-Name ]
                        [ State ]
                    *   [ AVP ]
```

4.2 QoS-Answer (QAA) Command

The QoS-Answer message (QAA), indicated by the Command-Code field set to XXX and 'R' bit cleared in the Command Flags field, is sent in response to the QoS-Request message. If the QoS-Request message is processed successfully, the response will include the AVPs to allow

authorization of the QoS resources as well as accounting and bearer gating information.

```
<QoS-Answer>        ::= < Diameter Header: XXX, PXY >
                        < Session-Id >
                        { Auth-Application-Id }
                        { Result-Code }
                        { Origin-Host }
                        { Origin-Realm }
                        [ QoS-Auth-Resources ]
                        [ QoS-Flow-State ]
                    *   [ AVP ]
```

5. Diameter QoS AVPs

Each of the AVPs identified in the QoS-Request and QoS-Answer command codes and the assignment of their value(s) is given in this section.

5.1 Diameter Base Protocol AVPs

The AVPs in this section are defined in the Base Protocol, and are included here for reference. For more information, see [RFC3588].

Session-Id AVP

The Diameter QoS Application client MUST create a unique value for the Session-Id. This value serves the purpose of uniquely identifier a particular session.

Auth-Application-Id

The Auth-Application-Id is assigned by IANA to Diameter Applications. The value of the Auth-Application-Id for the Diameter QoS Application is XXX.

Result-Code AVP

The Result-Code AVP indicates if a particular request was completed successfully.

Origin-Host

The Origin-Host AVP identifies the endpoint that originated the Diameter message.

Origin-Realm

The Origin-Realm AVP contains the Realm of the originator of the Diameter message.

5.2 Credit Control

The AVPs in this section are defined as part of the Diameter draft [I-D.ietf-aaa-diameter-cc].

Accounting-Correlation-Id

The Accounting-Correlation-Id AVP (AVP Code TBD) is of type OctetString and contains information to correlate accounting data generated produced by different components of the service, e.g.

transport and application level. In the Diameter QoS Application, this AVP is assigned a value by the Diameter QoS client and sent to the server in a QAR message.

5.3 Authentication/Authorization

Authentication and authorization is important for the Diameter QoS application. Therefore, a number of AVPs of related Diameter applications can be used, such as [I-D.ietf-aaa-eap], [I-D.ietf-aaa-diameter-sip-app] and [I-D.ietf-aaa-diameter-nasreq]

The details of the required attributes for authentication and authorization is for further study.

5.4 Accounting

Applications implementing this specification use Diameter Accounting as defined in the draft [I-D.ietf-aaa-diameter-cc]. The Diameter QoS Application uses a Credit Control Application AVP in its QAR message to specify an Accounting-Correlation ID.

5.5 Diameter QoS Application Defined AVPs

This section defines the Quality of Service AVPs that are specific to the Diameter QoS Application that MAY be included in the Diameter QoS Application messages. The following table describes the Diameter AVPs in the QoS Application, their AVP code values, types, possible flag values, and whether the AVP MAY be encrypted.

				AVP Flag rules				
Attribute Name	AVP Code	Section Defined	Data Type	MUST	MAY	SHLD NOT	MUST NOT	Encr
QoS-Auth-Resources	XXX	4.3	Grouped					
QoS-Filter-Rule	XXX	4.3	IPfltrRul					
QoS-Flow-State	XXX	4.3	Enumerated					
QoS-SDP	XXX	4.3	OctetString					
QoS-RSVP	XXX	4.3	OctetString					
QoS-NSIS	XXX	4.3	OctetString					

QoS-Auth-Resources

The QoS-Auth-Resources AVP (AVP Code N) is of type Grouped. Each individual AVP in the grouped QoS-Auth-Resources describes the value of a resource that has been authorized by an application server for a particular user (described by the User-Name AVP) and session (described by the Session-Id AVP). The QoS-Auth-Resources AVP is Optional, however one of QoS-Auth-Resources, or QoS-Flow-State is mandatory in a QAA message. The QoS-Auth-Resources also defines the mandatory fields for a Users Subscription QoS Profile. These AVPs correspond to the QoS Parameters of the Application and may not be the same as the QoS parameters requested of the bearer. If this is the case, some translation from the application level parameters to the bearer level parameters may be required.

```
QoS-Auth-Resources ::=  *  [ QoS-Filter-Rule ]
                       0*1 < QoS-SDP >
                       0*1 < QoS-RSVP >
                       0*1 < QoS-NSIS >
```

The AVPs that are part of QoS-Auth-resource AVP are:

QoS-Filter-Rule:

The QoS-Filter-Rule AVP is of type IPFilterRule, and provides filter rules for the packet flow of the user. One or more such AVPs MAY be present in a QAA response.

QoS-SDP:

The QoS-SDP AVP is of type OctetString. It contains the SDP data from the application layer session negotiation. The format of the data is as specified in [RFC2327].

QoS-RSVP:

The QoS-RSVP AVP is of type OctetString. It contains the information carried in the FLOWSPEC (see Appendix A.1).

QoS-NSIS:

The QoS-NSIS AVP is of type OctetString. It contains QoS parameter information. The format will be described in [I-D.ietf-nsis-qos-nslp] and [I-D.qspecteam-nsis-nslp-qspec]. Note that this work is still in progress. More specific packet format will be described in Appendix A.2 in a future version of

this document.

It is for further investigation whether a more generic formation for the QoS description in SDP, RSVP and NSIS can be compiled.

QoS-Flow-State

The QoS-Flow-State AVP is of type Enumerated and is used in both QAR and QAA messages. When included in a QAR message, it indicates the state of the flow identified by the User-Name and Session-Id AVPs. When included in a QAA message, it is instructions to the bearer control element with regard to the state to which the flow should be set. The supported values are

0 Open
1 Close
2 Maintain

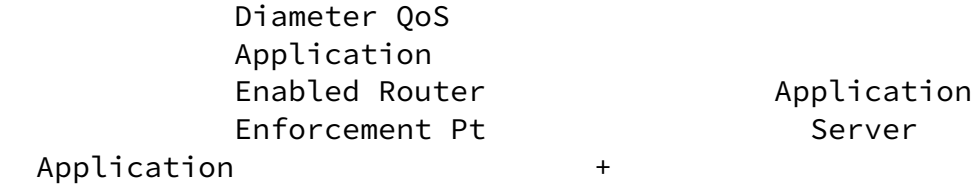
The QoS-Flow-State is an optional AVP. When not included in a QAA response, the default behavior is to immediately allow the flow of packets (Open).

5.6 Scenarios

This section illustrates the interworking of NSIS (in Figure 8) and RSVP (in Figure 9) in combination with the Diameter QoS application.

Figure 8 shows the interaction between NSIS, application layer signaling (e.g., SIP) and the Diameter QoS application. First, a service request is sent from the client to the application server. This response, for example, returns an authorization token to bind the application layer signaling exchange to the subsequent NSIS signaling session. The authorization token is attached to the NSIS signaling message and the message itself is intercepted by the first NSIS NSLP node. This router then needs to authorize the QoS request and delegates this responsibility to the Diameter QoS application. This type of authorization model is described in Section 3.6 of [I-D.ietf-nsis-qos-nslp]. The Diameter QoS Authorization Request (QAR), which includes authorization information and QoS information is, in this case, forwarded to the administrative domain of the application domain for verification. As a response, the authorization decision is returned with the Diameter QoS Answer message (QAA). Finally, the NSIS QoS NLP aware router acts as an enforcement point. If the authorization decision provided with the QAA message was successful then the NSIS signaling message is forwarded along the path. Otherwise, the QoS NSLP returns an error

message to the end host (such as 'Authorisation denied').



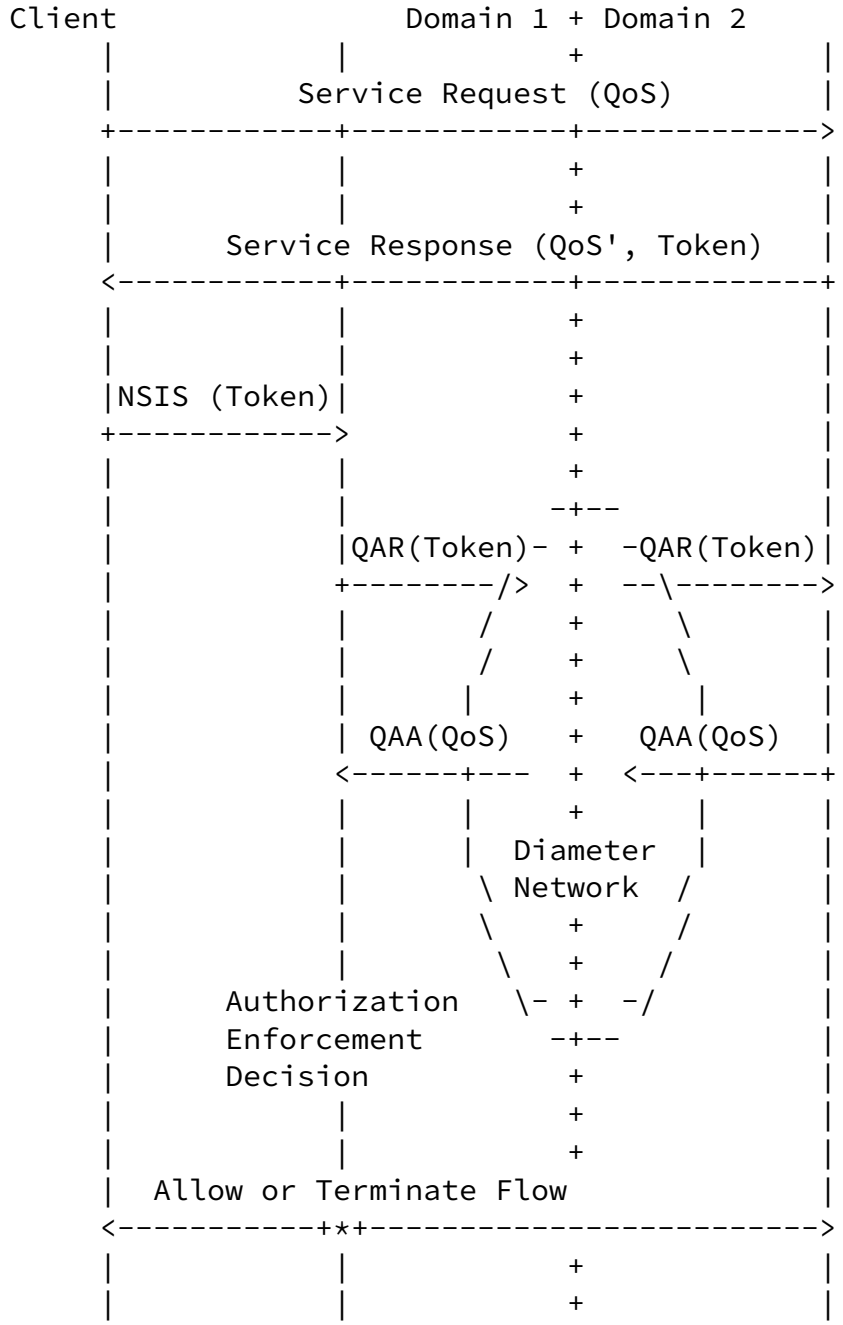


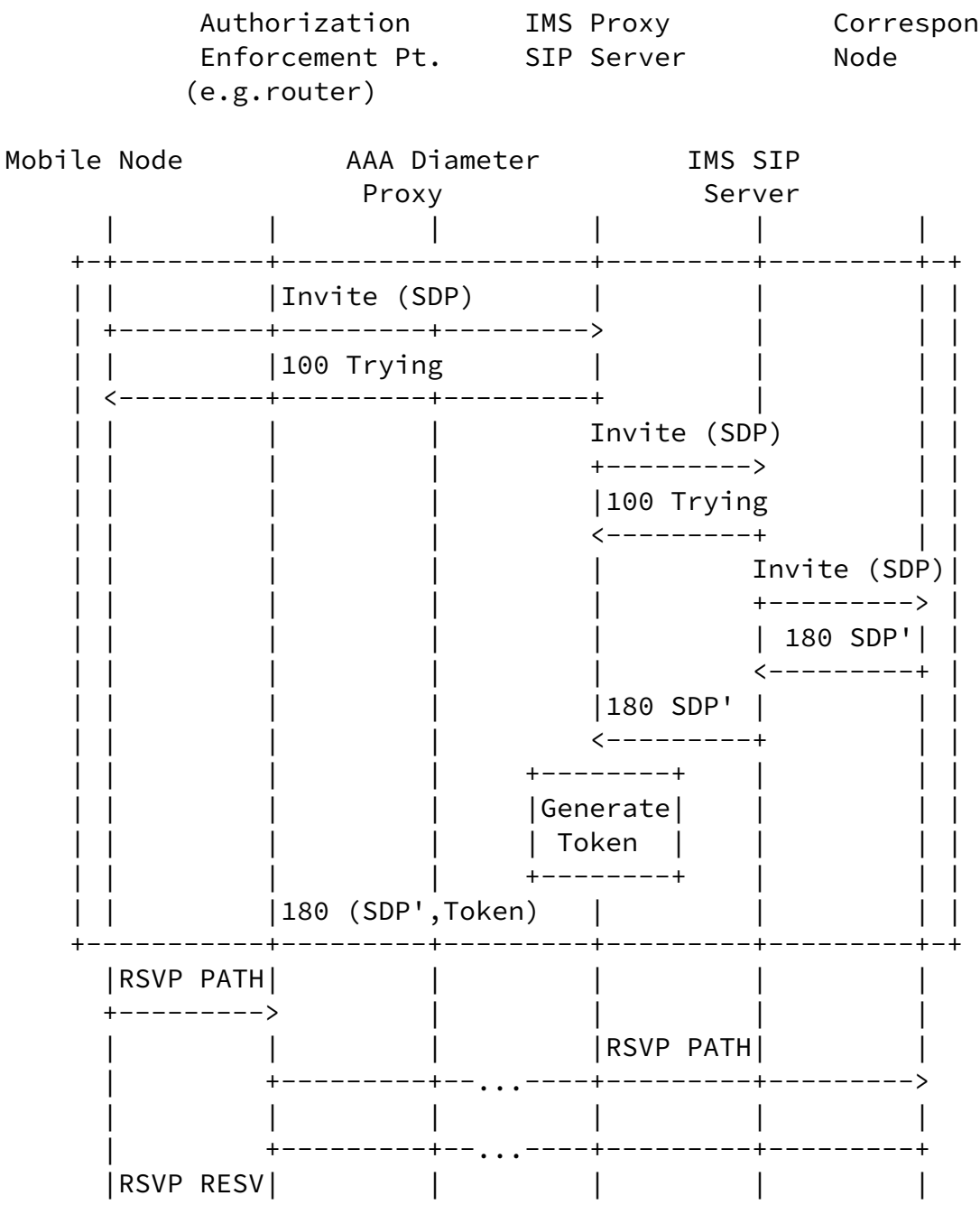
Figure 8: Message flow with NSIS and Diameter QoS Application

Figure 9 depicts the interaction between the SIP/RSVP aware end host in a scenario with application layer interaction. The basic

signaling exchange is similar to Figure 8 but a few differences

exist. First, the Diameter QoS application needs to carry RSVP and SDP specific payloads. Furthermore, the protocol specific mechanisms caused by RSVP (e.g., receiver initiated reservations) and SIP (such as [RFC2327] and [RFC3313]) need to be considered.

The message flow in Figure 9 also shows a QoS reservation in both direction - RSVP PATH/RESV messages signaling QoS information in both directions (from the Mobile Node to the Correspondent Node and vice versa). The authorization token handling of the Correspondent Node is omitted from the description.



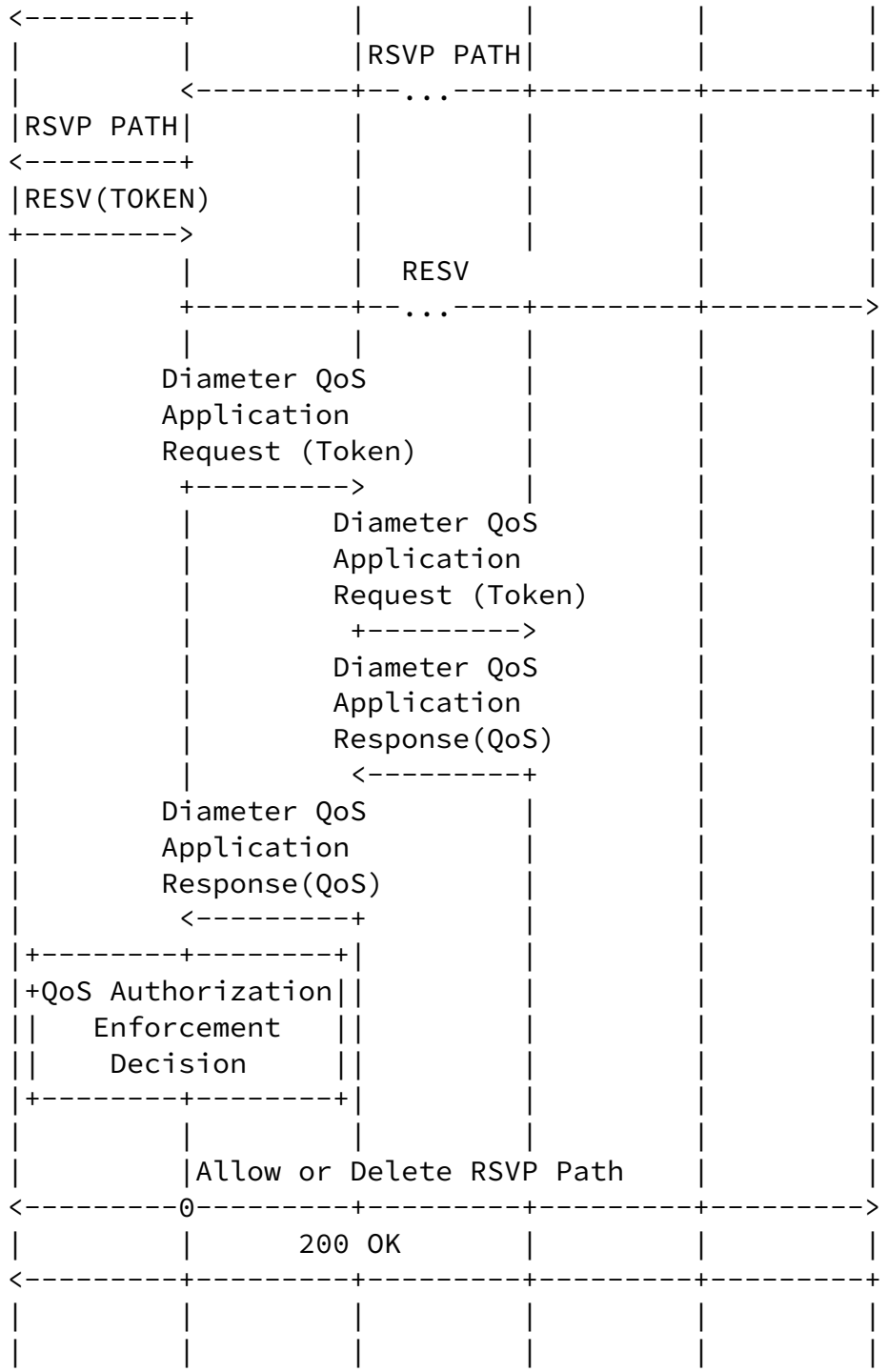


Figure 9: Message flow with RSVP and Diameter QoS Application

A future version of this document will describe scenarios with other authorization models.

5.7 Security Considerations

This document describes a mechanism for performing authorization of a QoS reservation at a third party entity. Thereby, it is necessary to

understand the QoS signaling protocol to forward the necessary information to the backend AAA server. This functionality is particularly useful in roaming environments where the authorization decision is most likely provided at an entity where the user is known. To provide proper authorization authentication might be necessary at least for the generic third party model (described in Section 3.6 of [I-D.ietf-nsis-qos-nslp]. The concept of an authorization token based third party approach is also described in the same document. The impact of the existence of different authorization models is (with respect to this Diameter QoS application) the ability to carry different authentication and authorization information.

Further discussions on the authorization handling for QoS signaling protocols is available with [I-D.tschofenig-nsis-aaa-issues] and [I-D.tschofenig-nsis-qos-authz-issues].

5.8 Acknowledgments

The authors would like to thank Tseno Tsenov for his early implementation work of this proposal.

5.9 Open Issues

During our work on this document we identified the following open issues:

- The security functionality of RSVP has been analysed in [I-D.ietf-nsis-rsvp-sec-properties]. Some of the mechanisms proposed with [RFC3182] do not seem to be adquate for today's usage. Hence, there is the question which functionality should be supported by the Diameter QoS application.

- This Diameter QoS application can reuse a number of other Diameter applications. This is a big advantage over other approaches. This interaction and a list of useful attributes needs to be collected and described. This aspect is for further study.

- The NSIS group is currently working on QoS models. As soon as

results are available it is feasible to incorporate them into this Diameter application to build a complete solution for QoS signaling which uses a backend infrastructure.

- Several authorization models have been described in [I-D.ietf-nsis-qos-nslp]. Section 5.6 currently addresses only the third party approach using authorization tokens. Further work is needed to describe the details of a generic three party scenario.

- Section 3.3 describes the session termination functionality. Should a new command code for bearer gating purposes be introduced, i.e., what if the application server wants to temporarily disable the bearer without terminating the session with ASR?

- Section 3.2 raises the question of a re-authorizing capability for the Diameter application. The authors think that such a re-authorization capability would be desirable (e.g., using with the RAR/RAA message exchange). Note that it would require the bearer path signaling protocol (for example RSVP or NSIS) to support network-initiated re-auth, which might not always be in place. There should be a failure code for the case where the underlying bearer signaling protocol does not support it.

- The QoS-Filter-Rule is of type IPFilterRule and specifies which traffic has to experience QoS treatment. The definition of the IPFilterRule in [RFC3588] does not explicitly list the capability to support IPsec protected traffic. Such a flow identifier description is required with NSIS and [RFC2207].

6. References

6.1 Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", March 1997.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G. and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003, <reference.RFC.3588.xml>.

6.2 Informative References

[I-D.alfano-aaa-qosreq] Alfano, F., McCann, P., Towle, T., Ejzak, R. and H. Tschofenig, "Requirements for a QoS AAA Protocol", draft-alfano-aaa-qosreq-01 (work in progress), October 2003, <reference.I-D.alfano-aaa-qosreq.xml>.

[I-D.ietf-aaa-diameter-cc] Mattila, L., Koskinen, J., Stura, M., Loughney, J. and H. Hakala, "Diameter Credit-control Application", draft-ietf-aaa-diameter-cc-05 (work in progress), May 2004, <reference.I-D.ietf-aaa-diameter-cc.xml>.

[I-D.ietf-aaa-diameter-nasreq]

Calhoun, P., Zorn, G., Spence, D. and D. Mitton, "Diameter Network Access Server Application", draft-ietf-aaa-diameter-nasreq-16 (work in progress), June 2004, <reference.I-D.ietf-aaa-diameter-nasreq.xml>.

[I-D.ietf-aaa-diameter-sip-app]
Garcia-Martin, M., "Diameter Session Initiation Protocol (SIP) Application", draft-ietf-aaa-diameter-sip-app-02 (work in progress), April 2004, <reference.I-D.ietf-aaa-diameter-sip-app.xml>.

[I-D.ietf-aaa-eap]
Eronen, P., Hiller, T. and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", draft-ietf-aaa-eap-08 (work in progress), June 2004, <reference.I-D.ietf-aaa-eap.xml>.

[I-D.ietf-nsis-qos-nslp]
Bosch, S., Karagiannis, G. and A. McDonald, "NSLP for Quality-of-Service signaling", draft-ietf-nsis-qos-nslp-03 (work in progress), May 2004.

[I-D.ietf-nsis-rsvp-sec-properties]
Tschofenig, H. and R. Graveman, "RSVP Security Properties", draft-ietf-nsis-rsvp-sec-properties-04 (work in progress), February 2004, <reference.I-D.ietf-nsis-rsvp-sec-properties.xml>.

[I-D.qspecteam-nsis-nslp-qspec]
Ash, J., Bader, A. and C. Kappler, "QoS-NSLP Qspec Template", draft-qspecteam-nsis-nslp-qspec-00 (work in progress), May 2004, <reference.I-D.qspecteam-nsis-nslp-qspec.xml>.

[I-D.tschofenig-nsis-aaa-issues]
Tschofenig, H., "NSIS Authentication, Authorization and Accounting Issues", draft-tschofenig-nsis-aaa-issues-01 (work in progress), March 2003, <reference.I-D.tschofenig-nsis-aaa-issues.xml>.

[I-D.tschofenig-nsis-qos-authz-issues]

Tschofenig, H., "QoS NSLP Authorization Issues", draft-tschofenig-nsis-qos-authz-issues-00 (work in progress), June 2003, <reference.I-D.tschofenig-nsis-qos-authz-issues.xml>.

[RFC2205] Braden, B., Zhang, L., Berson, S., Herzog, S. and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, September 1997, <reference.RFC.2205.xml>.

[RFC2207] Berger, L. and T. O'Malley, "RSVP Extensions for IPSEC Data Flows", RFC 2207, September 1997, <reference.RFC.2207.xml>.

[RFC2210] Wroclawski, J., "The Use of RSVP with IETF Integrated Services", RFC 2210, September 1997, <reference.RFC.2210.xml>.

[RFC2327] Handley, M. and V. Jacobson, "SDP: Session Description Protocol", RFC 2327, April 1998, <reference.RFC.2327.xml>.

[RFC2749] Herzog, S., Boyle, J., Cohen, R., Durham, D., Rajan, R. and A. Sastry, "COPS usage for RSVP", RFC 2749, January 2000, <reference.RFC.2749.xml>.

[RFC3182] Yadav, S., Yavatkar, R., Pabbati, R., Ford, P., Moore, T., Herzog, S. and R. Hess, "Identity Representation for RSVP", RFC 3182, October 2001, <reference.RFC.3182.xml>.

[RFC3313] Marshall, W., "Private Session Initiation Protocol (SIP) Extensions for Media Authorization", RFC 3313, January 2003, <reference.RFC.3313.xml>.

[RFC3520] Hamer, L-N., Gage, B., Kosinski, B. and H. Shieh, "Session Authorization Policy Element", RFC 3520, April 2003.

[RFC3521] Hamer, L-N., Gage, B. and H. Shieh, "Framework for Session Set-up with Media Authorization", RFC 3521, April 2003.

Authors' Addresses

Frank M. Alfano
Lucent Technologies
1960 Lucent Lane
Naperville, IL 60563
USA

Phone: +1 630 979 7209
EMail: falfano@lucent.com

Peter J. McCann
Lucent Technologies
1960 Lucent Lane
Naperville, IL 60563
USA

Phone: +1 630 713 9359
EMail: mccap@lucent.com

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

EMail: Hannes.Tschofenig@siemens.com

Appendix A. AVP Formats

This section provides a strawman proposal for the AVPs introduced by this document. Additionally, the content of the payload is described. Unlike the approach followed with RSVP (see [RFC2749])

where the entire RSVP message is encapsulated into a COPS message this approach only includes the relevant fields. This approach avoids a certain overhead of transmitting fields which are irrelevant for the AAA infrastructure, it keeps implementations simpler and it allows to reuse other Diameter AVPs. Finally, it helps to make this Diameter application less dependent on any particular QoS signaling protocol or a particular QoS model.

A.1 RSVP to Diameter QoS AVPs Mapping

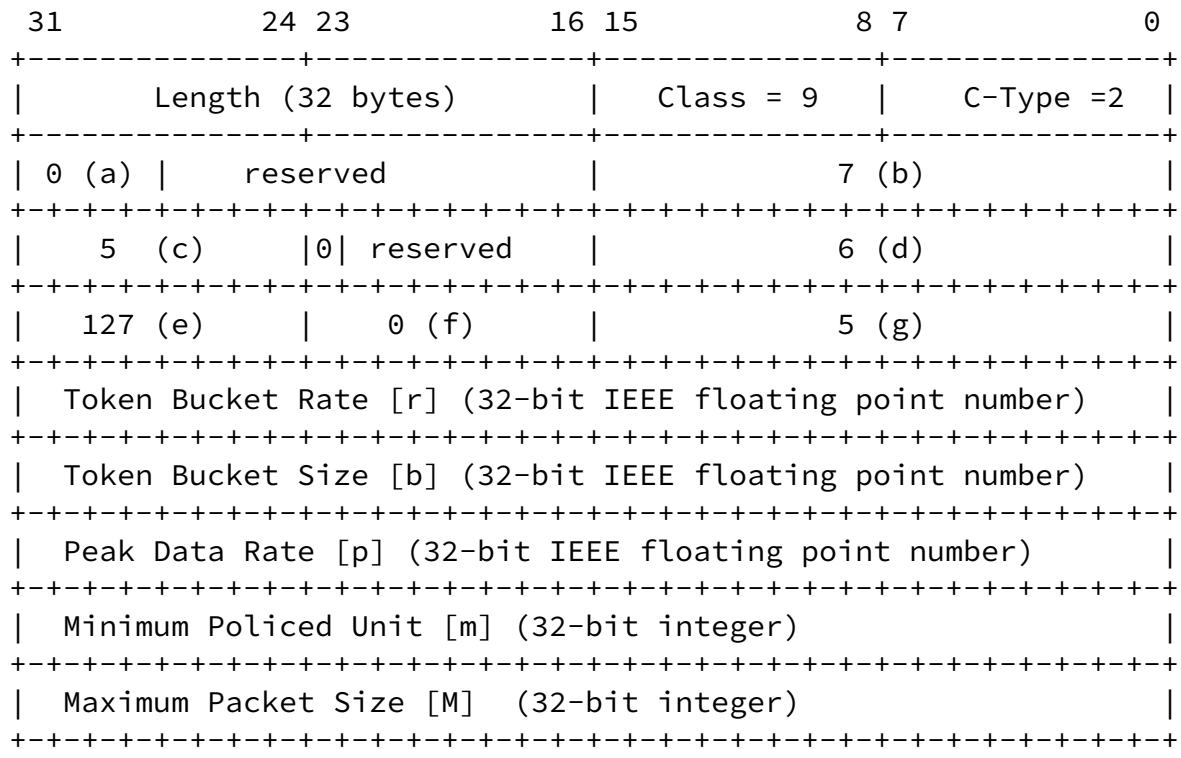
The following RSVP objects need to be mapped to the Diameter QoS AVPs: FLOWSPEC, FILTER_SPEC and POLICY_DATA. The FLOWSPEC defines a desired QoS, in a Resv message. FILTER_SPEC defines a subset of session data packets that should receive the desired QoS (specified by a FLOWSPEC object), in a Resv message. POLICY_DATA carries information about the user requesting QoS resources.

A.1.1 RSVP Objects for the QoS-RSVP AVP

The QoS-Flow-state AVP has to carry QoS specific information. This section describes payloads which are relevant for the transport of RSVP QoS specific payloads.

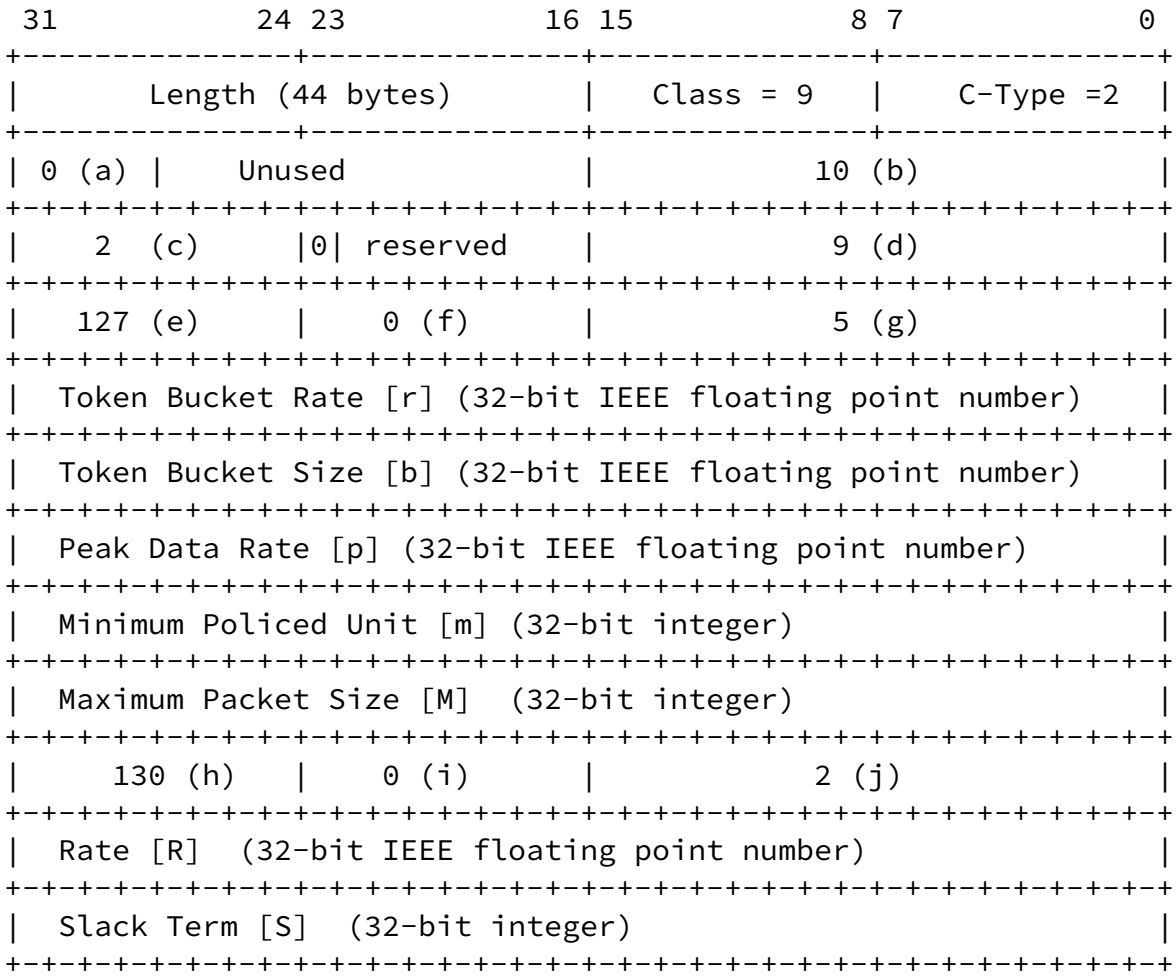
The subsequently listed RSVP objects are taken from [RFC2210] and [RFC2205]. For completeness we list these attributes in this section.

The RSVP FLOWSPEC object, including the RSVP object header, for requesting Controlled-Load Service is described below:



(a) - Message format version number (0)
(b) - Overall length (7 words not including header)
(c) - Service header, service number 5 (Controlled-Load)
(d) - Length of controlled-load data, 6 words not including per-service header
(e) - Parameter ID, parameter 127 (Token Bucket TSpec)
(f) - Parameter 127 flags (none set)
(g) - Parameter 127 length, 5 words not including per-service header

The RSVP FLOWSPEC object, including the RSVP object header, for requesting Guaranteed Service is described below:



(a) - Message format version number (0)
(b) - Overall length (9 words not including header)
(c) - Service header, service number 2 (Guaranteed)
(d) - Length of per-service data, 9 words not including per-service header
(e) - Parameter ID, parameter 127 (Token Bucket TSpec)
(f) - Parameter 127 flags (none set)
(g) - Parameter 127 length, 5 words not including parameter header
(h) - Parameter ID, parameter 130 (Guaranteed Service RSpec)
(i) - Parameter 130 flags (none set)
(j) - Parameter 130 length, 2 words not including parameter header

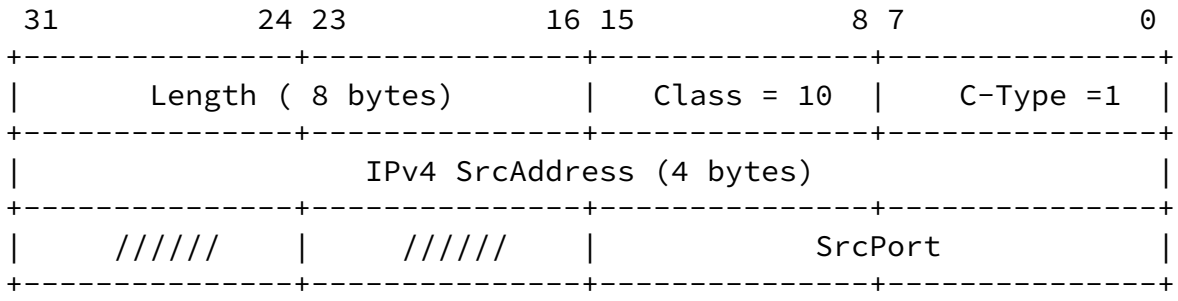
A.1.2 RSVP Objects for the Filter-Rule AVP

The RSVP FLOWSPEC needs to be associated with the FILTER_SPEC to describe which traffic should experience QoS treatment. The subsequent attributes list relevant payloads used in RSVP for this purpose. These objects need to be carried in the Filter-Rule AVP.

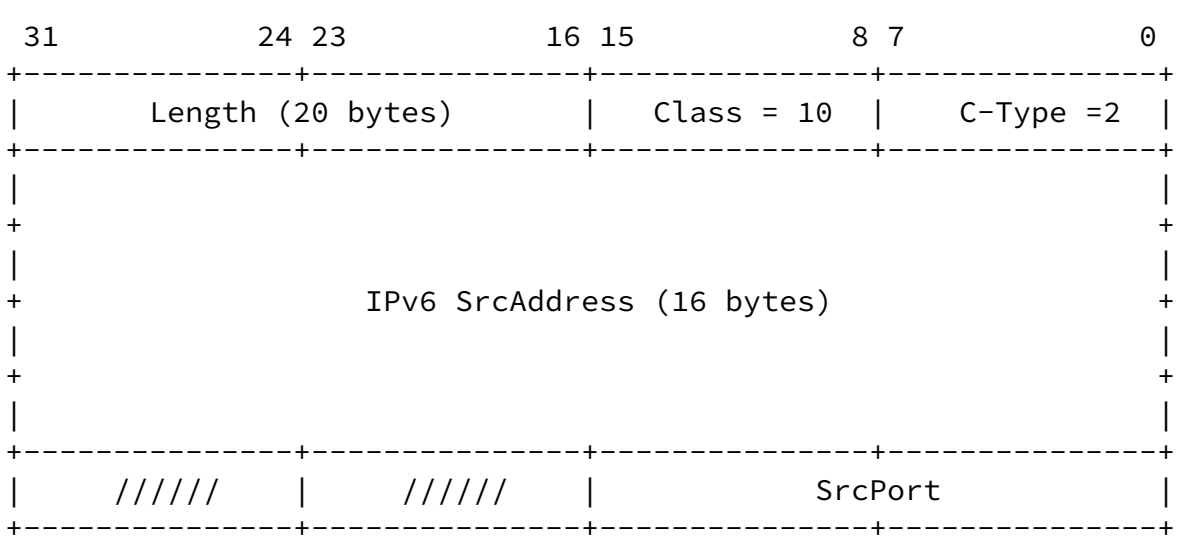
The subsequent attributes are reused from RSVP and show the

attributes that have to be supported.

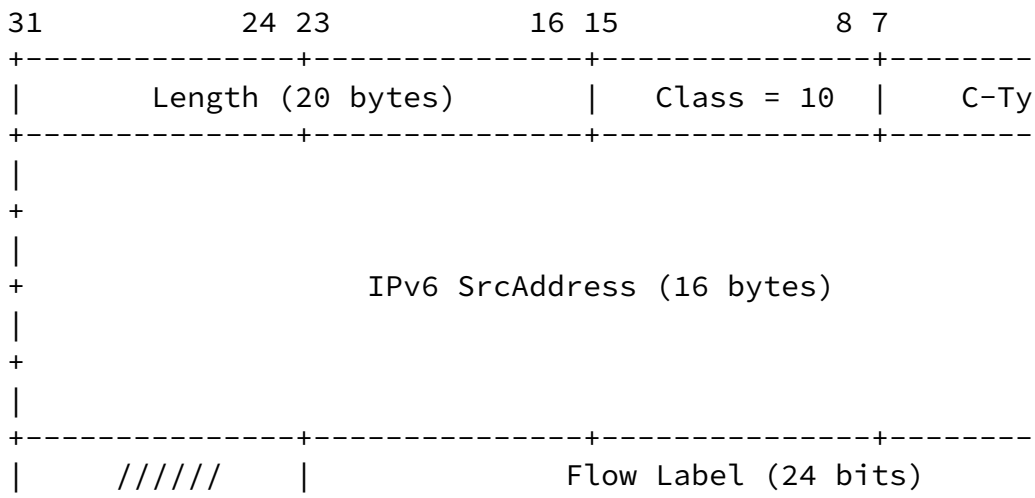
The IPv4 FILTER_SPEC object has the following structure:



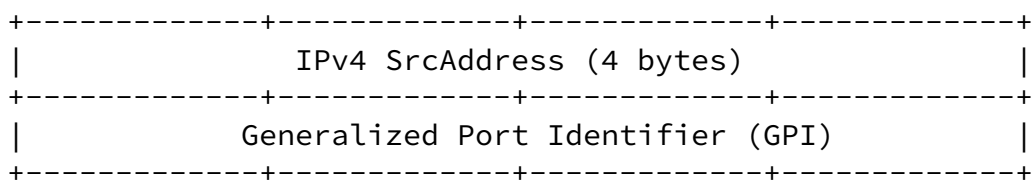
The IPv6 FILTER_SPEC object has the following structure:



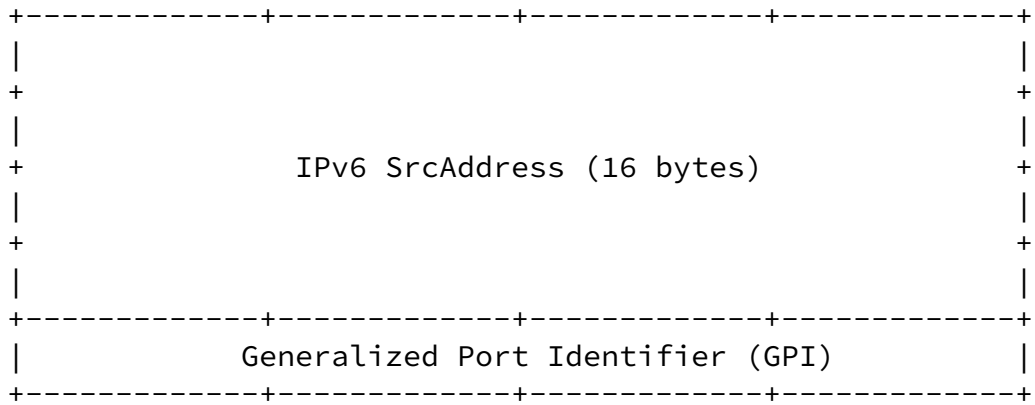
The IPv6 Flow-label FILTER_SPEC has the following structure:



The IPv4/GPI FILTER_SPEC object, which was introduced with [RFC2207] has the following structure:



The IPv6/GPI FILTER_SPEC object, which was introduced with [RFC2207] has the following structure:



The Generalized Port Identifier (GPI) contains the SPI.

A.1.3 RSVP Objects for the QoS-Auth-Resources

User authentication/authorization capabilities have been added to RSVP with [RFC3182]. Additionally, a token-based authorization mechanism has been proposed with [RFC3520] and [RFC3521] which should also supported by this Diameter application. A future version of this document will map these objects to QoS-Auth-Resources AVP (or related attributes). Please also see the open issue in Section 5.9.

A.2 NSIS to Diameter QoS AVPs Mapping

A future version of this document will contain payload descriptions of objects introduced by the NSIS protocol suite. Relevant parameters can be found in [I-D.ietf-nsis-qos-nslp] and in the area of QoS models (see [I-D.qspecteam-nsis-nslp-qspec] for ongoing work).

A.3 SIP to Diameter QoS AVPs Mapping

QoS authorization with the Diameter QoS Application requires that also SIP specific mechanisms are exchanged via Diameter. A future version of this document will describe the mapping of SDP payloads [RFC2327] to this Diameter application.

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of

such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

Copyright Statement

Acknowledgment

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