Diameter Quality of Service Application
draft-ietf-dime-diameter-qos-03.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on July 26, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).
Abstract

This document describes framework, messages and procedures for the Diameter QoS application. The Diameter QoS application allows network elements to interact with Diameter servers when allocating QoS resources in the network. In particular, two modes of operation - Pull and Push are defined.

Table of Contents

1. Introduction .............................................. 4
2. Terminology ............................................. 5
3. Framework ............................................... 7
   3.1. Network element functional model .................... 8
   3.2. Implications of Endpoint QoS Capabilities .......... 10
       3.2.1. Category ...................................... 10
       3.2.2. Interaction modes between authorizing entity and
               network element .................................. 10
   3.3. Schemes .............................................. 12
       3.3.1. Schemes for pull mode .......................... 12
       3.3.2. Schemes for push mode .......................... 15
   3.4. QoS Application Requirements ....................... 16
4. QoS Application Session Establishment and Management ...... 21
   4.1. Parties involved .................................... 21
   4.2. Session Establishment ................................. 21
       4.2.1. Session establishment for pull mode .............. 21
       4.2.2. Session establishment for push mode .............. 24
       4.2.3. Discovery and selection of peer Diameter QoS
               application node ................................. 27
   4.3. Session re-authorization ................................ 28
       4.3.1. Client-Side Initiated Re-Authorization ........... 28
       4.3.2. Server-Side Initiated Re-Authorization .......... 29
   4.4. Session Termination .................................. 31
       4.4.1. Client-Side Initiated Session Termination ........ 31
       4.4.2. Server-Side Initiated Session Termination ........ 32
5. QoS Application Messages .................................. 34
   5.1. QoS-Authorization Request (QAR) ...................... 34
   5.2. QoS-Authorization Answer (QAA) ...................... 35
   5.3. QoS-Install Request (QIR) ............................ 36
   5.4. QoS-Install Answer (QIA) ............................. 36
   5.5. Re-Auth-Request (RAR) ................................ 37
   5.6. Re-Auth-Answer (RAA) ................................ 37
6. QoS Application State Machine ............................... 39
   6.1. Supplemented states for push mode .................... 39
7. QoS Application AVPs ...................................... 41
   7.1. Reused Base Protocol AVPs ............................ 41
   7.2. QoS Application Defined AVPs ......................... 41
1. Introduction

This document describes framework, messages and procedures for the Diameter QoS Application. The Diameter QoS Application allows network elements (NEs) to interact with Diameter servers when allocating QoS resources in the network.

In particular, two modes of operation are defined. In the first, called "Pull Mode", the network element pro-actively sends a command to the Diameter server for QoS authorization based on some trigger (such as a QoS signaling protocol) that arrives along the data path. In the second, called "Push Mode", the Diameter server pro-actively sends a command to the network element(s) to install QoS authorization state. This could be triggered, for instance, by off-path signaling such as SIP-based call control.

A set of command codes pertinent to this QoS application are specified that allows a single Diameter application to support both Pull and Push modes based on the requirements of network technologies, deployment scenarios and end-host’s capabilities. In conjunction with parameters defined in [I-D.ietf-dime-qos-attributes] and in [I-D.ietf-dime-qos-parameters], this document depicts basic call flow procedures to establish, modify and terminate a Diameter QoS application session.
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].

The following terms are used in this document:

Diameter QoS Application Server

A Diameter QoS application server is a logical Diameter node that supports the protocol interaction for QoS authorization. The Diameter QoS application server resides in the authorizing entity (AE). In the Pull mode, it responds to a Diameter session initiated by a Diameter QoS application client; in the Push mode, it initiates a Diameter session to a Diameter QoS application client triggered by application signaling or local events.

Diameter QoS Application Client

A Diameter QoS application client is a logical Diameter node that supports the protocol interaction for QoS enforcement. The Diameter QoS client resides in the network element. In the Pull mode, it initiates a Diameter session to the Diameter QoS application server triggered by a QoS signaling or other events; in the Push mode, it responds to a Diameter session initiated by a Diameter QoS server.

Resource Requesting Entity

A resource requesting entity is a logical entity that supports the protocol interaction for QoS resources. The resource requesting entity resides in the end-host and is able to communicate with peer logical entities in Authorizing Entity or Network element to trigger the QoS authorization process.

Application Server

An application server is a network entity that exchanges signaling messages with an application endpoint. It may be a source of authorization for QoS-enhanced application flows. For example, a SIP server is one kind of application server.

Application Endpoint

An application endpoint is an entity in an end user device that exchanges signaling messages with application servers or directly with other application endpoints. Based on the result of this
signaling, the endpoint may make a request for QoS from the network. For example, a SIP User Agent is one kind of application endpoint.

Authorizing Entity

The authorizing entity acts as a Diameter server (and may collocate with a subscriber database) responsible for authorizing QoS requests for a particular application flow or aggregate. It may be a standalone entity or integrated with an application server. This entity corresponds to the Policy Decision Point (PDP) (see [RFC2753]).

AAA Cloud

An infrastructure of AAA entities (clients, agents, servers) based on a AAA protocol, which provides trusted secure connections between them. It offers authentication, authorization and accounting services to applications in flexible local and roaming scenarios. Diameter [RFC3588] and RADIUS [RFC2865] are both widely deployed AAA protocols.

Network Element (NE)

QoS aware router that acts as Diameter client that implements the Diameter QoS application in the context of this document. For almost all scenarios this entity triggers the protocol interaction described in this document. This entity corresponds to the Policy Enforcement Point (PEP) (see [RFC2753]).

Pull Mode

In this mode, the QoS authorization process is invoked by the QoS reservation request received from the endpoint. The Network Element then requests the QoS authorization decision from the Authorizing entity.

Push Mode

In this mode, the QoS authorization process is invoked by the request from Application Server or local policies in the Authorizing Entity. The Authorizing Entity then installs the QoS authorization decision to the Network Element directly.
3. Framework

The Diameter QoS application runs between a network element (acting as a Diameter client) and the resource authorizing entity (acting as a Diameter server). A high-level picture of the resulting architecture is shown in Figure 1.

Figure 1: An Architecture supporting QoS-AAA

Figure 1 depicts network elements through which media flows need to pass, a cloud of AAA servers, and an authorizing entity. Note that there may be more than one router that needs to interact with the AAA cloud along the path of a given application flow, although the figure only depicts one for clarity.

In some deployment scenarios, QoS aware network elements may request authorization through the AAA cloud based on an incoming QoS reservation request. The network element will route the request to a designated authorizing entity. The authorizing entity will return the result of the authorization decision. In other deployment scenarios, the authorization will be initiated upon dynamic application state, so that the request must be authenticated and authorized based on information from one or more application servers. After receiving the authorization request from the application server or the network element, the authorizing entity decides the appropriate mode (i.e. Push or Pull). The Push or Pull mode can be
dynamically determined based on the information received from the request of the application server and/or the information (e.g., policy) in the authorizing entity, or statically configured according to operator’s demand, or the messages between AE and NE. The Authorizing Entity may identify the access network through the use of some out-of-band signaling, such as SIP, Diameter, which may be sent from the application server to Authorizing Entity, and then select appropriate resource admission and control policies.

If defined properly, the interface between the routers and AAA cloud would be identical in both cases. Routers 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.

3.1. Network element functional model

Figure 2 depicts a logical operational model of resource management in a router.
Processing of incoming QoS reservation requests includes three actions: admission control, authorization and resource reservation.

The admission control function provides information for available
resources and determines whether there are enough resources to fulfill the request. Authorization is performed by the Diameter client function which involves contacting an authorization entity through the AAA cloud shown in Section 3. If both checks are successful, the authorized QoS parameters are set in the packet classifier and the packet scheduler. Note that the parameters passed to the Traffic Control function may be different from requested QoS (depending on the authorization decision). Once the requested resource is granted, the Resource Management function provides accounting information to the Authorizing entity using the Diameter client function.

3.2. Implications of Endpoint QoS Capabilities

3.2.1. Category

The QoS capabilities of endpoints are varied, which can be categorized as follows:

- **Category 1 endpoint**: Has no QoS capability at both application and network levels. This type of endpoint may set up a connection through application signaling, but it is unable to specify any resource/QoS requirements either through application signaling or does not support network signaling at all.

- **Category 2 endpoint**: Only has QoS capability at the application level. This type of endpoint is able to set up a connection through application signaling with certain resource/QoS requirements (e.g., application attributes), but it is unable to specify any network level resource/QoS requirements (e.g., network QoS class) through network signaling e.g., RSVP or NSIS (or does not support network layer signaling at all).

- **Category 3 endpoint**: Has QoS capability at the network level. This type of endpoint may set up a connection through application signaling and translate service characteristics into network resource/QoS requirements (e.g., network QoS class) locally, and request the resources through network signaling, e.g., RSVP or NSIS.

3.2.2. Interaction modes between authorizing entity and network element

Different QoS mechanisms are employed in packet networks. Those QoS mechanisms can be categorized into two schemes: IntServ and DiffServ. In the IntServ scheme, network signaling (e.g., RSVP, NSIS, or link specific signaling) is commonly used to initiate a request from endpoint for desired QoS resource of media flow. In the DiffServ scheme, the QoS resources are provisioned based on some predefined QoS service classes instead of endpoint initiated per flow based QoS request.
It is obvious that the eligible QoS scheme is correlated to the endpoint’s capability in the context of QoS authorization. Since category 1 and 2 endpoints cannot initiate the QoS resource requests through the network signaling, the IntServ model is not applicable to them in general. Depending on network technology and operator’s demand, a category 3 endpoint may either make use of the network signaling for requesting the resource or not perform the request.

The diversity of QoS capabilities of endpoints and QoS schemes of network technology leads to the distinction on the interaction mode between QoS authorization system and underlying network elements. When the IntServ scheme is employed by category 3 endpoint, the authorization process is typically initiated by network element when a trigger such as the network signaling is received from the endpoint. In the DiffServ scheme, since the network element is unable to request the resource authorization on its own initiative, the authorization process is typically triggered upon either the request of application servers or policies defined by the operator.

As a consequence, two interaction modes are needed in support of different combinations of QoS schemes and endpoint’s QoS capabilities: Push mode and Pull mode.

- **Push mode**: The QoS authorization process is triggered by application servers or local network conditions (e.g., time of day on resource usage and QoS classes), and the authorization decisions are installed by the authorizing entity to the network element on its own initiative without explicit request. In order to support the push mode, the authorizing entity (i.e., Diameter server) should be able to initiate a Diameter authorization session to communicate with the network element (i.e., Diameter client) without any pre-established connection from the network element.

- **Pull mode**: The QoS authorization process is triggered by the network signaling received from end user equipments or by the local event in the network element according to pre-configured policies, and authorization decisions are produced upon the request of the network element. In order to support the pull mode, the network element (i.e., Diameter client) will initiate a Diameter authorization session to communicate with authorizing entity (i.e., Diameter server).

For category 1 and 2 endpoints, the Push mode is required, in particular, category 1 endpoint requires network initiated push mode and category 2 endpoint may use both them. For category 3 endpoint, either push mode or pull mode is doable.

The Push mode is applicable to certain networks, for example, Cable
network, DSL, Ethernet, Diffserv enabled IP/MPLS as defined by other SDOs, e.g., ETSI TISPAN and ITU-T. The Pull mode is more appropriate to IntServ enabled IP networks or certain wireless networks such as GPRS networks as defined by 3GPP/PP2. Some networks, e.g., WiMAX may require both Push and Pull modes.

3.3. Schemes

3.3.1. Schemes for pull mode

Three basic authorization schemes for pull mode exist: one two-party and two three-party schemes. The notation adopted here is in respect to the entity that performs the QoS authorization. The authentication of the QoS requesting entity might be done at the network element as part of the QoS signaling protocol, or by an off-path protocol run (on the application layer or for network access authentication) or the authorizing entity might be contacted with request for authentication and authorization of the QoS requesting entity. From the Diameter QoS application’s point of view these schemes differ in type of information that need to be carried. Here we focus on the ‘Three party scheme’ (see Figure 3) and the ‘Token-based three party scheme’ (see Figure 4). With the ‘two party scheme’ the QoS resource requesting entity is authenticated by the Network Element and the authorization decision is made either locally at the Network Element itself or offloaded to a trusted entity (most likely within the same administrative domain). In the former case no Diameter QoS protocol interaction is required.
With the 'three party scheme' a QoS reservation request that arrives at the Network Element is forwarded to the Authorizing Entity (e.g., in the user’s home network), where the authorization decision is made. A business relationship, such as a roaming agreement, between the visited network and the home network ensures that the visited network is compensated for the resources consumed by the user via the home network.
The 'Token-based Three Party scheme' is applicable to environments where a previous protocol interaction is used to request authorization tokens to assist the authorization process at the Network Element or the Authorizing Entity.

The QoS resource requesting entity may be involved in an application layer protocol interaction, for example using SIP, with the Authorizing Entity. As part of this interaction, authentication and authorization at the application layer might take place. As a result of a successful authorization decision, which might involve the user’s home AAA server, an authorization token is generated by the Authorizing Entity (e.g., the SIP proxy and an entity trusted by the SIP proxy) and returned to the end host for inclusion into the QoS signaling protocol. The authorization token will be used by a Network Element that receives the QoS signaling message to authorize the QoS request. Alternatively, the Diameter QoS application will be used to forward the authorization token to the user’s home network. The authorization token allows the authorization decision performed at the application layer protocol run to be associated with a corresponding QoS signaling session. Note that the authorization token might either refer to established state concerning the authorization decision or the token might itself carry the authorized parameters (protected by a digital signature or a keyed message...
digest to prevent tampering). In the latter case the authorization
token may contain several pieces of information pertaining to the
authorized application session, but at minimum it should contain:
- An identifier of the Authorizing Entity (for example, of an
  application server) that issued the authorization token,
- An identifier referring to a specific application protocol session
  for which the token was issued and
- A keyed message digest or digital signature protecting the content
  of the authorization token.

A possible structure for the authorization token and the policy
element carrying it are proposed in context of RSVP [RFC3520].

In the scenario mentioned above, where the QoS resource requesting
entity is involved in an application layer protocol interaction with
the Authorizing entity, it may be worthwhile to consider a token less
binding mechanism also. The application layer protocol interaction
may have indicated the transport port numbers at the QoS resource
requesting entity where it might receive media streams, for example
in SIP/SDP signalling these port numbers are advertised. The QoS
resource requesting entity may also use these port numbers in some IP
filter indications to the NE performing QoS reservation so that it
may properly tunnel the inbound packets. The NE performing QoS
reservation will forward the QoS resource requesting entity’s IP
address and the IP filter indications to the Authorizing entity in
the QoS authz. request. The Authorizing entity will use the QoS
resource requesting entity’s IP address and the port numbers in the
IP filter indication, which will match the port numbers advertised in
the earlier application layer protocol interaction, to identify the
right piece of policy information to be sent to the NE performing the
QoS reservation in the QoS authz. response.

3.3.2. Schemes for push mode

The push mode can be further divided into two types: endpoint
initiated and network initiated. In the former case, the
authorization process is triggered by application server upon
explicit QoS request from endpoints through application signaling,
e.g. SIP; in the latter case, the authorization process is triggered
by application server without explicit QoS request from endpoint.

In the endpoint initiated scheme, the QoS resource requesting entity
(i.e. endpoint) determines the required application level QoS and
sends the QoS request through application signaling message, the
Application Server will extract application level QoS information and
trigger the authorization process to Authorizing entity. In the
network initiated scheme, the Authorizing entity and/or Application
server should derive and determine the QoS requirement according to
application attribute, subscription and endpoint’s capability when the endpoint does not explicitly indicate the QoS attributes. The authorizing entity makes authorization decision based on application level QoS information, network policies, end user subscription and network resource availability etc., and installs the decision to network element directly.

![Diagram](attachment:image)

**Figure 5: Scheme for Push Mode**

### 3.4. QoS Application Requirements

A QoS application must meet a number of requirements applicable to a diverse set of networking environments and services. It should be compliant with different deployment scenarios with specific QoS signaling models and security issues. Satisfying the requirements listed below while interworking with QoS signaling protocols, a Diameter QoS application should accommodate the capabilities of the QoS signaling protocols rather than introducing functional requirements on them. A list of requirements for a QoS authorization application is provided here:
Inter-domain support

In particular, users may roam outside their home network, leading to a situation where the network element and authorizing entity are in different administrative domains.

Identity-based Routing

The QoS AAA protocol MUST route AAA requests to the Authorizing Entity, based on the provided identity of the QoS requesting entity or the identity of the Authorizing entity encoded in the provided authorization token.

Flexible Authentication Support

The QoS AAA protocol MUST support a variety of different authentication protocols for verification of authentication information present in QoS signaling messages. The support for these protocols MAY be provided indirectly by tying the signaling communication for QoS to a previous authentication protocol exchange (e.g., using network access authentication).

Making an Authorization Decision

The QoS AAA protocol MUST exchange sufficient information between the authorizing entity and the enforcing entity (and vice versa) to compute an authorization decision and to execute this decision.

Triggering an Authorization Process

The QoS AAA protocol MUST allow periodic and event triggered execution of the authorization process, originated at the enforcing entity or even at the authorizing entity.

Associating QoS Reservations and Application State

The QoS AAA protocol MUST carry information sufficient for an application server to identify the appropriate application session and associate it with a particular QoS reservation.

Dynamic Authorization

It MUST be possible for the QoS AAA protocol to push updates towards the network element(s) from authorizing entities.
Bearer Gating

The QoS AAA protocol MUST allow the authorizing entity to gate (i.e., enable/disable) authorized application flows based on, e.g., application state transitions.

Accounting Records

The QoS AAA protocol may define QoS accounting records containing duration, volume (byte count) usage information and description of the QoS attributes (e.g., bandwidth, delay, loss rate) that were supported for the flow.

Sending Accounting Records

The network element SHOULD be able to send accounting records for a particular QoS reservation state to an accounting entity.

Failure Notification

The QoS AAA protocol MUST allow the network element to report failures, such as loss of connectivity due to movement of a mobile node or other reasons for packet loss, to the authorizing entity.

Accounting Correlation

The QoS AAA protocol may support the exchange of sufficient information to allow for correlation between accounting records generated by the network elements and accounting records generated by an application server.

Interaction with other AAA Applications

Interaction with other AAA applications such as Diameter Network Access (NASREQ) application [RFC4005] is required for exchange of authorization, authentication and accounting information.

In deployment scenarios, where authentication of the QoS reservation requesting entity (e.g., the user) is done by means outside the Diameter QoS application protocol interaction the Authorizing Entity is contacted only with a request for QoS authorization. Authentication might have taken place already via the interaction with the Diameter NASREQ application or as part of the QoS signaling protocol (e.g., Transport Layer Security (TLS) handshake in the General Internet Signaling Transport (GIST) protocol, see [I-D.ietf-nsis-ntlp]).
Authentication of the QoS reservation requesting entity to the Authorizing Entity is necessary if a particular Diameter QoS application protocol run cannot be related (or if there is no intention to relate it) to a prior authentication. In this case the Authorizing Entity MUST authenticate the QoS reservation requesting entity in order to authorize the QoS request as part of the Diameter QoS protocol interaction.

The document refers to three types of sessions that need to be properly correlated.

QoS signaling session

The time period during which a QoS signaling protocol establishes, maintains and deletes a QoS reservation state at the QoS network element is referred as QoS signaling session. Different QoS signaling protocols use different ways to identify QoS signaling sessions. The same applies to different usage environments. Currently, this document supports three types of QoS session identifiers, namely a signaling session id (e.g., the Session Identifier used by the NSIS protocol suite), a flow id (e.g., identifier assigned by an application to a certain flow as used in the 3GPP) and a flow description based on the IP parameters of the flow's end points.

Diameter authorization session

The time period, for which a Diameter server authorizes a requested service (i.e., QoS resource reservation) is referred to as a Diameter authorization session. It is identified by a Session-Id included in all Diameter messages used for management of the authorized service (initial authorization, re-authORIZATION, termination), see [RFC3588].

Application layer session

The application layer session identifies the duration of an application layer service which requires provision of certain QoS. An application layer session identifier is provided by the QoS requesting entity in the QoS signaling messages, for example as part of the authorization token. In general, the application session identifier is opaque to the QoS aware network elements. It is included in the authorization request message sent to the Authorizing entity and helps it to correlate the QoS authorization request to the application session state information.

Correlating these sessions is done at each of the three involved
entities: The QoS requesting entity correlates the application with the QoS signaling sessions. The QoS network element correlates the QoS signaling session with the Diameter authorization sessions. The Authorizing entity SHOULD bind the information about the three sessions together. Note that in certain scenarios not all of the sessions are present. For example, the application session might not be visible to QoS signaling protocol directly if there is no binding between the application session and the QoS requesting entity using the QoS signaling protocol.
4. QoS Application Session Establishment and Management

4.1. Parties involved

Authorization models supported by this application include three parties:
- Resource requesting entity
- Network Elements (Diameter QoS application (DQA) client)
- Authorizing Entity (Diameter QoS application (DQA) server)

Note that the QoS resource requesting entity is only indirectly involved in the message exchange. This entity provides the trigger to initiate the Diameter QoS protocol interaction by transmitting QoS signaling messages. The Diameter QoS application is only executed between the Network Element (i.e., DQA client) and the Authorizing Entity (i.e., DQA server).

The QoS resource requesting entity may communicate with the Authorizing Entity using application layer signaling for negotiation of service parameters. As part of this application layer protocol interaction, for example using SIP, authentication and authorization might take place. This message exchange is, however, outside the scope of this document. The protocol communication between the QoS resource requesting entity and the QoS Network Element might be accomplished using the NSIS protocol suite, RSVP or a link layer signaling protocol. A description of these protocols is also outside the scope of this document and a tight coupling with these protocols is not desirable since this applications aims to be generic.

4.2. Session Establishment

The Pull and Push modes use a different set of command codes for session establishment. For other operations, such as session modification and termination, they use the same set of command codes.

The Pull mode or Push mode operation is invoked based on the trigger of QoS Authorization session. When a QAR with a new session ID is received, the Authorizing Entity operates in the pull mode; when other triggers are received, the Authorizing Entity operates in the push mode. Similarly, when a QIR with new session ID is received, the Network Element operates in the push mode; when other triggers are received, the Network Element operation in the pull mode.

4.2.1. Session establishment for pull mode

A request for a QoS reservation or local events received by a Network Element can trigger the initiation of a Diameter QoS authorization session. The Network Element generates a QoS-Authorization-Request
(QAR) message in which it maps required objects from the QoS signaling message to Diameter payload objects.

Figure 7 shows the protocol interaction between a resource requesting entity, a Network Element and the Authorizing Entity.

The Authorizing Entity’s identity, information about the application session and/or identity and credentials of the QoS resource requesting entity, requested QoS parameters, signaling session identifier and/or QoS enabled data flows identifiers MAY be encapsulated into respective Diameter AVPs and included into the Diameter message sent to the Authorizing Entity. The QAR is sent to a Diameter server that can either be the home server of the QoS requesting entity or an application server.

<table>
<thead>
<tr>
<th>QoS specific Input Data</th>
<th>Diameter QoS AVPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorizing entity ID (e.g., taken from authorization token or derived based on Network Access ID (NAI) [RFC2486] of the QoS requesting entity)</td>
<td>Destination-Host Destination-Realm</td>
</tr>
<tr>
<td>Authorization Token Credentials of the QoS requesting entity</td>
<td>QoS-Authz-Data User-Name</td>
</tr>
<tr>
<td>QoS parameters</td>
<td>QoS-Resources</td>
</tr>
</tbody>
</table>

Authorization processing starts at the Diameter QoS server when it receives the QAR. Based on the information in the QoS-Authentication-Data, User-Name and QoS-Resources AVPs the server determines the authorized QoS resources and flow state (enabled/disabled) from locally available information (e.g., policy information that may be previously established as part of an application layer signaling exchange, or the user’s subscription profile). The QoS-Resources AVP is defined in [I-D.ietf-dime-qos-attributes]. The authorization decision is then reflected in the response returned to the Diameter client with the QoS-Authorization-Answer message (QAA).
The Authorizing Entity keeps authorization session state and SHOULD save additional information for management of the session (e.g., Signaling-Session-Id, authentication data) as part of the session.
state information.

The final result of the authorization request is provided in the Result-Code AVP of the QAA message sent by the Authorizing Entity. In case of successful authorization (i.e., Result-Code = DIAMETER_LIMITED_SUCCESS, (see Section 7.1)), information about the authorized QoS resources and the status of the authorized flow (enabled/disabled) is provided in the QoS-Resources AVP of the QAA message. The QoS information provided via the QAA is installed by the QoS Traffic Control function of the Network Element. The value DIAMETER_LIMITED_SUCCESS indicates that the Authorizing entity expects confirmation via another QAR message for successful QoS resource reservation and for final reserved QoS resources (see below).

One important piece of information returned from the Authorizing Entity is the authorization lifetime (carried inside the QAA). The authorization lifetime allows the Network Element to determine how long the authorization decision is valid for this particular QoS reservation. A number of factors may influence the authorized session duration, such as the user’s subscription plan or currently available credits at the user’s account (see Section 8). The authorization duration is time-based as specified in [RFC3588]. For an extension of the authorization period, a new QoS-Authorization-Request/Answer message exchange SHOULD be initiated. Further aspects of QoS authorization session maintenance is discussed in Section 4.3, Section 4.4 and Section 8.

The indication of a successful QoS reservation and activation of the data flow is provided by the transmission of an QAR message, which reports the parameters of the established QoS state: reserved resources, duration of the reservation, and identification of the QoS enabled flow/QoS signaling session. The Diameter QoS server acknowledges the reserved QoS resources with the QA Answer (QAA) message where the Result-Code is set to ‘DIAMETER_SUCCESS’. Note that the reserved QoS resources reported in this QAR message MAY be different than those authorized with the initial QAA message, due to the QoS signaling specific behavior (e.g., receiver-initiated reservations with One-Path-With-Advertisements) or specific process of QoS negotiation along the data path.

4.2.2. Session establishment for push mode

The Diameter QoS server in the Authorizing Entity initiates a Diameter QoS authorization session upon the request for QoS reservation triggered by application layer signaling or by local events, and generates a QoS-Install-Request (QIR) message to Diameter QoS client in the NE in which it maps required objects to Diameter
payload objects.

Figure 9 shows the protocol interaction between the Authorizing Entity, a Network Element and a resource requesting entity.

The Network Element’s identity, information about the application session and/or identity and credentials of the QoS resource requesting entity, requested QoS parameters, signaling session identifier and/or QoS enabled data flows identifiers MAY be encapsulated into respective Diameter AVPs and included into the Diameter message sent from a Diameter QoS server in the Authorizing Entity to a Diameter QoS client in the NE. This requires that the Authorizing Entity has knowledge of specific information for allocating and identifying the Network Element that should be contacted and the data flow for which the QoS reservation should be established. This information can be statically configured or dynamically discovered, see Section 3.2.3 for details.

+----------------------------------|-------------------------------+
| QoS specific Input Data          | Diameter QoS AVPs             |
+----------------------------------|-------------------------------+
| Network Element ID (e.g., from    | Destination-Host             |
| static configuration             | Destination-Realm             |
| or dynamically discovered, see    |                               |
| Section 3.2.3 for details)       |                               |
+----------------------------------|-------------------------------+
| Authorization Token              | QoS-Authz-Data                |
| Credentials of                   | User-Name                     |
| the QoS requesting entity        |                               |
+----------------------------------|-------------------------------+
| QoS parameters                   | QoS-Resources                 |
+----------------------------------|-------------------------------+

Authorization processing starts at the Diameter QoS server when it receives the request from a resource requesting entity through application server (e.g., SIP Invite) or the trigger by local events (e.g., pre-configured timer). Based on the received information the server determines the authorized QoS resources and flow state (enabled/disabled) from locally available information (e.g., policy information that may be previously established as part of an application layer signaling exchange, or the user’s subscription profile). The authorization decision is then reflected in the QoS-Install-Request message (QIR) to the Diameter QoS client.
The Authorizing Entity keeps authorization session state and SHOULD save additional information for management of the session (e.g., Signaling-Session-Id, authentication data) as part of the session state information.
The final result of the authorization decision is provided in the QoS-Resources AVP of the QIR message sent by the Authorizing Entity. The QoS information provided via the QIR is installed by the QoS Traffic Control function of the Network Element.

One important piece of information from the Authorizing Entity is the authorization lifetime (carried inside the QIR). The authorization lifetime allows the Network Element to determine how long the authorization decision is valid for this particular QoS reservation. A number of factors may influence the authorized session duration, such as the user’s subscription plan or currently available credits at the user’s account (see Section 8). The authorization duration is time-based as specified in [RFC3588]. For an extension of the authorization period, a new QoS-Install-Request/Answer message or QoS-Authorization-Request/Answer message exchange SHOULD be initiated. Further aspects of QoS authorization session maintenance is discussed in Section 4.3, Section 4.4 and Section 8.

The indication of QoS reservation and activation of the data flow, can be provided by the QoS-Install-Answer message immediately. In the case of successful enforcement, the Result-Code (= DIAMETER_SUCCESS, (see Section 7.1)) information is provided in the QIA message. Note that the reserved QoS resources reported in the QIA message MAY be different than those initially authorized with the QIR message, due to the QoS signaling specific behavior (e.g., receiver-initiated reservations with One-Path-With-Advertisements) or specific process of QoS negotiation along the data path. When path coupled signaling is used for QoS reservation along the data path, QAR/QAA may be used to update the results of QoS reservation and enforcement following the establishment of data flows.

4.2.3. Discovery and selection of peer Diameter QoS application node

The Diameter QoS application node may obtain information of its peer nodes (e.g., FQDN, IP address) through static configuration or dynamic discovery as described in [RFC3588]. In particular, the Network Element shall perform the relevant operation for Pull mode; the Authorizing Entity shall perform the relevant operations for Push mode.

Upon receipt of a trigger to initiate a new Diameter QoS authorization session, the Diameter QoS application node selects and retrieves the location information of the peer node and based on some index information provided by the resource requesting entity. For instance, it can be the Authorization Entity’s ID stored in the authorization token, the end-host’s identity (e.g., NAI [RFC2486]) or globally routable IP address.
4.3. Session re-authorization

Client and server-side initiated re-authorizations are considered in the design of the Diameter QoS application. Whether the re-authorization events are transparent for the resource requesting entity or result in specific actions in the QoS signaling protocol is outside the scope of the Diameter QoS application. It is directly dependent on the capabilities of the QoS signaling protocol.

There are a number of options for policy rules according to which the NE (AAA client) contacts the Authorizing Entity for re-authorization. These rules depend on the semantics and contents of the QAA message sent by the Authorizing Entity:

a. The QAA message contains the authorized parameters of the flow and its QoS and sets their limits (presumably upper). With these parameters the Authorizing Entity specifies the services that the NE can provide and will be financially compensated for. Therefore, any change or request for change of the parameters of the flow and its QoS that do not conform to the authorized limits requires contacting the Authorizing Entity for authorization.

b. The QAA message contains authorized parameters of the flow and its QoS. The rules that determine whether parameters’ changes require re-authorization are agreed out of band, based on a Service Level Agreement (SLA) between the domains of the NE and the Authorizing Entity.

c. The QAA message contains the authorized parameters of the flow and its QoS. Any change or request for change of these parameters requires contacting the Authorizing entity for re-authorization.

d. In addition to the authorized parameters of the flow and its QoS, the QAA message contains policy rules that determine the NEs actions in case of change or request for change in authorized parameters.

Provided options are not exhaustive. Elaborating on any of the listed approaches is deployment/solution specific and is not considered in the current document.

In addition, the Authorizing Entity may use RAR to perform re-authorization with the authorized parameters directly when the re-authorization is triggered by service request or local events/policy rules.

4.3.1. Client-Side Initiated Re-Authorization

The Authorizing Entity provides the duration of the authorization session as part of the QoS-Authorization-Answer message (QAA). At
any time before expiration of this period, a new QoS-Authorization-Request message (QAR) MAY be sent to the Authorizing Entity. The transmission of the QAR MAY be triggered, such as, when the Network Element receives a QoS signaling message that requires modification of the authorized parameters of an ongoing QoS session, or authorization lifetime expires.

![Figure 10: Client-side initiated QoS re-authorization](image)

4.3.2. Server-Side Initiated Re-Authorization

The Authorizing Entity MAY initiate a QoS re-authorization by issuing a Re-Auth-Request message (RAR) as defined in the Diameter base protocol [RFC3588], which may include the parameters of the re-
authorized QoS state: reserved resources, duration of the reservation, identification of the QoS enabled flow/QoS signaling session for re-installation of the resource state by the QoS Traffic Control function of the Network Element.

A Network Element that receives such a RAR message with Session-Id matching a currently active QoS session acknowledges the request by sending the Re-Auth-Answer (RAA) message towards the Authorizing entity.

If RAR does not include any parameters of the re-authorized QoS state, the Network Element MUST initiate a QoS re-authorization by sending a QoS-Authorization-Request (QAR) message towards the Authorizing entity.
4.4. Session Termination

4.4.1. Client-Side Initiated Session Termination

The authorization session for an installed QoS reservation state MAY be terminated by the Diameter client by sending a Session-Termination-Request message (STR) to the Diameter server. This is a Diameter base protocol function and it is defined in [RFC3588]. Session termination can be caused by a QoS signaling messaging requesting deletion of the existing QoS reservation state or it can be caused as a result of a soft-state expiration of the QoS reservation state.
4.4.2. Server-Side Initiated Session Termination

At anytime during a session the Authorizing Entity MAY send an Abort-Session-Request message (ASR) to the Network Element. This is a Diameter base protocol function and it is defined in [RFC3588]. Possible reasons for initiating the ASR message to the Network Element are insufficient credits or session termination at the application layer. The ASR message results in termination of the authorized session, release of the reserved resources at the Network Element and transmission of an appropriate QoS signaling message indicating a notification to other Network Elements aware of the signaling session.
Figure 13: Server-Side Initiated Session Termination
5. QoS Application Messages

The Diameter QoS Application requires the definition of new mandatory AVPs and Command-codes (see Section 3 of [RFC3588]). Four new Diameter messages are defined along with Command-Codes whose values MUST be supported by all Diameter implementations that conform to this specification.

<table>
<thead>
<tr>
<th>Command-Name</th>
<th>Abbrev.</th>
<th>Code</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS-Authz-Request</td>
<td>QAR</td>
<td>[TBD]</td>
<td>Section 5.1</td>
</tr>
<tr>
<td>QoS-Authz-Answer</td>
<td>QAA</td>
<td>[TBD]</td>
<td>Section 5.2</td>
</tr>
<tr>
<td>QoS-Install-Request</td>
<td>QIR</td>
<td>[TBD]</td>
<td>Section 5.3</td>
</tr>
<tr>
<td>QoS-Install-Answer</td>
<td>QIA</td>
<td>[TBD]</td>
<td>Section 5.4</td>
</tr>
</tbody>
</table>

In addition, the following Diameter Base protocol messages are used in the Diameter QoS application:

<table>
<thead>
<tr>
<th>Command-Name</th>
<th>Abbrev.</th>
<th>Code</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Re-Auth-Request</td>
<td>RAR</td>
<td>258</td>
<td>RFC 3588</td>
</tr>
<tr>
<td>Re-Auth-Answer</td>
<td>RAA</td>
<td>258</td>
<td>RFC 3588</td>
</tr>
<tr>
<td>Abort-Session-Request</td>
<td>ASR</td>
<td>274</td>
<td>RFC 3588</td>
</tr>
<tr>
<td>Abort-Session-Answer</td>
<td>ASA</td>
<td>274</td>
<td>RFC 3588</td>
</tr>
<tr>
<td>Session-Term-Request</td>
<td>STR</td>
<td>275</td>
<td>RFC 3588</td>
</tr>
<tr>
<td>Session-Term-Answer</td>
<td>STA</td>
<td>275</td>
<td>RFC 3588</td>
</tr>
</tbody>
</table>

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, see [RFC3588].

The value of TBD MUST be used as the Application-Id in all QAR/QAA and QIR/QIA commands.

The value of zero (0) SHOULD be used as the Application-Id in all STR/STA, ASR/ASA, and RAR/RAA commands, because these commands are defined in the Diameter base protocol and no additional mandatory AVPs for those commands are defined in this document.

5.1. QoS-Authorization Request (QAR)

The QoS-Authorization-Request message (QAR) indicated by the Command-Code field (see Section 3 of [RFC3588]) set to TBD and ‘R’ bit set in the Command Flags field is used by Network elements to request quality of service related resource authorization for a given flow.

The QAR message MUST carry information for signaling session
identification, Authorizing Entity identification, information about
the requested QoS, and the identity of the QoS requesting entity. In
addition, depending on the deployment scenario, an authorization
token and credentials of the QoS requesting entity SHOULD be
included.

The message format, presented in ABNF form [RFC2234], is defined as
follows:

\[\text{<QoS-Request> ::= < Diameter Header: XXX, REQ, PXY >}
\text{< Session-Id >}
\text{ { Auth-Application-Id }}
\text{ { Origin-Host }}
\text{ { Origin-Realm }}
\text{ { Destination-Realm }}
\text{ { Auth-Request-Type }}
\text{ { Destination-Host }}
\text{ { User-Name }}
\text{* [ QoS-Resources ]}
\text{ [ QoS-Authz-Data ]}
\text{ [ Bound-Auth-Session-Id ]}
\text{* [ AVP ]}\]

5.2. QoS-Authorization Answer (QAA)

The QoS-Authorization-Answer message (QAA), indicated by the Command-
Code field set to TBD and ‘R’ bit cleared in the Command Flags field
is sent in response to the QoS-Authorization-Request message (QAR).
If the QoS authorization request is successfully authorized, the
response will include the AVPs to allow authorization of the QoS
resources and transport plane gating information.

The message format is defined as follows:

\[\text{<QoS-Answer> ::= < Diameter Header: XXX, PXY >}
\text{< Session-Id >}
\text{ { Auth-Application-Id }}
\text{ { Auth-Request-Type }}
\text{ { Result-Code }}
\text{ { Origin-Host }}
\text{ { Origin-Realm }}
\text{* [ QoS-Resources ]}
\text{ [ Acc-Multisession-Id ]}
\text{ [ Session-Timeout ]}
\text{ [ Authz-Session-Lifetime ]}
\text{ [ Authz-Grace-Period ]}\]
5.3. QoS-Install Request (QIR)

The QoS-Install Request message (QIR), indicated by the Command-Code field set to TBD and ‘R’ bit set in the Command Flags field is used by Authorizing entity to install or update the QoS parameters and the flow state of an authorized flow at the transport plane element.

The message MUST carry information for signaling session identification or identification of the flow to which the provided QoS rules apply, identity of the transport plane element, description of provided QoS parameters, flow state and duration of the provided authorization.

The message format is defined as follows:

\[
\text{<QoS-Install-Request>} ::= \text{< Diameter Header: XXX, REQ, PXY >}
\]
\[
\text{< Session-Id >}
\]
\[
\text{< Auth-Application-Id >}
\]
\[
\text{< Origin-Host >}
\]
\[
\text{< Origin-Realm >}
\]
\[
\text{< Destination-Realm >}
\]
\[
\text{< Auth-Request-Type >}
\]
\[
\text{< Destination-Host >}
\]
\[
\text{< QoS-Resources >}
\]
\[
\text{< Session-Timeout >}
\]
\[
\text{< Authz-Session-Lifetime >}
\]
\[
\text{< Authz-Grace-Period >}
\]
\[
\text{< Authz-Session-Volume >}
\]
\[
\text{< AVP >}
\]

5.4. QoS-Install Answer (QIA)

The QoS-Install Answer message (QIA), indicated by the Command-Code field set to TBD and ‘R’ bit cleared in the Command Flags field is sent in response to the QoS-Install Request message (QIR) for confirmation of the result of the installation of the provided QoS reservation instructions.

The message format is defined as follows:
<QoS-Install-Answer> ::= < Diameter Header: XXX, PXY >
< Session-Id >
{ Auth-Application-Id }
{ Origin-Host }
{ Origin-Realm }
{ Result-Code }
* [ QoS-Resources ]
* [ AVP ]

5.5. Re-Auth-Request (RAR)

The Re-Auth-Request message (RAR), indicated by the Command-Code field set to 258 and the ‘R’ bit set in the Command Flags field, is sent by the Authorizing Entity to the Network Element in order to initiate the QoS re-authorization from DQA server side.

If the RAR command is received by the Network Element without any parameters of the re-authorized QoS state, the Network Element MUST initiate a QoS re-authorization by sending a QoS-Authorization-Request (QAR) message towards the Authorizing entity.

The message format is defined as follows:

<Re-Auth-Request> ::= < Diameter Header: 258, REQ, PXY >
< Session-Id >
{ Auth-Application-Id }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
{ Auth-Request-Type }
{ Destination-Host }
* [ QoS-Resources ]
{ Session-Timeout }
{ Authz-Session-Lifetime }
{ Authz-Grace-Period }
{ Authz-Session-Volume }
* [ AVP ]

5.6. Re-Auth-Answer (RAA)

The Re-Auth-Answer message (RAA), indicated by the Command-Code field set to 258 and the ‘R’ bit cleared in the Command Flags field, is sent by the Network Element to the Authorizing Entity in response to the RAR command.

The message format is defined as follows:
<Re-Auth-Answer> ::= < Diameter Header: 258, PXY >
    < Session-Id >
    { Auth-Application-Id }
    { Origin-Host }
    { Origin-Realm }
    { Result-Code }
    * [ QoS-Resources ]
    * [ AVP ]
6. QoS Application State Machine

The QoS application reuses the authorization state machine defined in Section 8.1 of the Base Protocol ([RFC3588]) with its own messages as defined in Section 5 and QoS AVPs as defined in Section 7.

6.1. Supplemented states for push mode

In addition to the reused state machines, the following states are supplemented to first 2 state machines in which the session state is maintained on the Server, and MUST be supported in any QoS application implementations in support of server initiated push mode (see (Section 4.2.2)).

The following states are supplemented to the state machine on the server:

<table>
<thead>
<tr>
<th>State</th>
<th>Event</th>
<th>Action</th>
<th>New State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle</td>
<td>An application or local event triggers an initial QoS request to the server</td>
<td>Send</td>
<td>Pending</td>
</tr>
<tr>
<td></td>
<td>QIR initial request</td>
<td>QIR initial request</td>
<td></td>
</tr>
<tr>
<td>Pending</td>
<td>Received QIA with a failed Result-Code</td>
<td>Cleanup</td>
<td>Idle</td>
</tr>
<tr>
<td>Pending</td>
<td>Received QIA with Result-Code = SUCCESS</td>
<td>Update</td>
<td>Open</td>
</tr>
<tr>
<td>Pending</td>
<td>Error in processing received QIA with Result-Code = SUCCESS ASR</td>
<td>Send</td>
<td>Discon</td>
</tr>
</tbody>
</table>

The following states are supplemented to the state machine on the client:
### CLIENT, STATEFUL

<table>
<thead>
<tr>
<th>State</th>
<th>Event</th>
<th>Action</th>
<th>New State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle</td>
<td>QIR initial request received and successfully processed</td>
<td>Send Open</td>
<td>QIR initial reply, reserve resources</td>
</tr>
<tr>
<td>Idle</td>
<td>QIR initial request received but not successfully processed</td>
<td>Send Idle</td>
<td>QIR initial reply with Result-Code != SUCCESS</td>
</tr>
</tbody>
</table>
7. QoS Application AVPs

Each of the AVPs identified in the QoS-Authorization-Request/Answer and QoS-Install-Request/Answer messages and the assignment of their value(s) is given in this section.

7.1. Reused Base Protocol AVPs

The QoS application uses a number of session management AVPs, defined in the Base Protocol ([RFC3588]).

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>AVP Code</th>
<th>Reference [RFC3588]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Origin-Host</td>
<td>264</td>
<td>Section 6.3</td>
</tr>
<tr>
<td>Origin-Realm</td>
<td>296</td>
<td>Section 6.4</td>
</tr>
<tr>
<td>Destination-Host</td>
<td>293</td>
<td>Section 6.5</td>
</tr>
<tr>
<td>Destination-Realm</td>
<td>283</td>
<td>Section 6.6</td>
</tr>
<tr>
<td>Auth-Application-Id</td>
<td>258</td>
<td>Section 6.8</td>
</tr>
<tr>
<td>Result-Code</td>
<td>268</td>
<td>Section 7.1</td>
</tr>
<tr>
<td>Auth-Request-Type</td>
<td>274</td>
<td>Section 8.7</td>
</tr>
<tr>
<td>Session-Id</td>
<td>263</td>
<td>Section 8.8</td>
</tr>
<tr>
<td>Authz-Lifetime</td>
<td>291</td>
<td>Section 8.9</td>
</tr>
<tr>
<td>Authz-Grace-Period</td>
<td>276</td>
<td>Section 8.10</td>
</tr>
<tr>
<td>Session-Timeout</td>
<td>27</td>
<td>Section 8.13</td>
</tr>
<tr>
<td>User-Name</td>
<td>1</td>
<td>Section 8.14</td>
</tr>
</tbody>
</table>

The Auth-Application-Id AVP (AVP Code 258) is assigned by IANA to Diameter applications. The value of the Auth-Application-Id for the Diameter QoS application is TBD.

7.2. QoS Application Defined AVPs

This document reuses the AVPs defined in Section 4 of [I-D.ietf-dime-qos-attributes].

This section lists the AVPs that are introduced specifically for the QoS application. The following new AVPs are defined: Bound-Auth-Session-Id and the QoS-Authz-Data AVP.

The following table describes the Diameter AVPs newly defined in this document for usage with the QoS Application, their AVP code values, types, possible flag values, and whether the AVP may be encrypted.
QoS-Authz-Data

The QoS-Authz-Data AVP (AVP Code TBD) is of type OctetString. It is a container that carries application session or user specific data that has to be supplied to the Authorizing entity as input to the computation of the authorization decision.

Bound-Authentication-Session-Id

The Bound-Authentication-Session AVP (AVP Code TBD) is of type UTF8String. It carries the id of the Diameter authentication session that is used for the network access authentication (NASREQ authentication session). It is used to tie the QoS authorization request to a prior authentication of the end host done by a co-located application for network access authentication (Diameter NASREQ) at the QoS NE.
8. Accounting

A Network Element may start an accounting session by sending an Accounting-Request message (ACR) after successful QoS reservation and activation of the data flow (see Figure 7 and Figure 9). After every successful re-authorization procedure (see Figure 10 and Figure 11), the Network element may initiate an interim accounting message exchange. After successful session termination (see Figure 12 and Figure 13), the Network element may initiate a final exchange of accounting messages for terminating of the accounting session and reporting final records for the usage of the QoS resources reserved. It should be noted that the two sessions (authorization and accounting) have independent management by the Diameter base protocol, which allows for finalizing the accounting session after the end of the authorization session.

The detailed QoS accounting procedures are out of scope in this document.
9. Examples

9.1. Example call flow for pull mode

This section presents an example of the interaction between the end host and Diameter QoS application entities using Pull mode. The application layer signaling is, in this example, provided using SIP. Signaling for a QoS resource reservation is done using the QoS NSLP. The authorization of the QoS reservation request is done by the Diameter QoS application (DQA).

```
End-Host                              SIP Server              Correspondent
requesting QoS                        (DQA Server)          Node

|........................................|.......................|
|........................................|.......................|
|........Application layer SIP signaling.......|...............|
|........Application layer SIP signaling.......|...............|
|........Application layer SIP signaling.......|...............|

|......Invite (SDP)   |              |
|......100 Trying    |              |
|......Invite (SDP)   |              |
|......180 SDP’       |              |
|......Authorize session parameters |
|......180 (Session parameters) +---------|
|......+---------|
|......Authorize |QoS resources|
|......QAA        |

|........QoS NSLP Reserve +------------|
|QAR                        |
| POLICY_DATA>v             |
| v                        |
| QSPEC>                   |
| Destination-Host,        |
| QoS-Authz-Data           |
| QoS-Resources            |
| Authorize                |
|  QoS resources           |
| QAA                      |
| (Result-Code,            |
| QoS-Resources,           |
| Authz-Lifetime)          |
```

Sun, et al.       Expires July 26, 2008       [Page 44]
The communication starts with SIP signaling between the two endpoints and the SIP server for negotiation and authorization of the requested service and its parameters (see Figure 26). As a part of the process, the SIP server verifies whether the user at Host A is authorized to use the requested service (and potentially the ability...
to be charged for the service usage). Negotiated session parameters are provided to the end host.

Subsequently, Host A initiates a QoS signaling message towards Host B. It sends a QoS NSLP Reserve message, in which it includes description of the required QoS (QSPEC object) and authorization data for negotiated service session (part of the POLICY_DATA object). Authorization data includes, as a minimum, the identity of the authorizing entity (e.g., the SIP server) and an identifier of the application service session for which QoS resources are requested.

A QoS NSLP Reserve message is intercepted and processed by the first QoS aware Network Element. The NE uses the Diameter QoS application to request authorization for the received QoS reservation request. The identity of the Authorizing Entity (in this case the SIP server that is co-located with a Diameter server) is put into the Destination-Host AVP, any additional session authorization data is encapsulated into the QoS-Authz-Data AVP and the description of the QoS resources is included into QoS-Resources AVP. These AVPs are included into a QoS Authorization Request message, which is sent to the Authorizing entity.

A QAR message will be routed through the AAA network to the Authorizing Entity. The Authorizing Entity verifies the requested QoS against the QoS resources negotiated for the service session and replies with QoS-Authorization answer (QAA) message. It carries the authorization result (Result-Code AVP) and the description of the authorized QoS parameters (QoS-Resources AVP), as well as duration of the authorization session (Authorization-Lifetime AVP).

The NE interacts with the traffic control function and installs the authorized QoS resources and forwards the QoS NSLP Reserve message further along the data path. Moreover, the NE may serve as a signaling proxy and process the QoS signaling (e.g. initiation or termination of QoS signaling) based on the QoS decision received from the authorizing entity.

9.2. Example call flow for push mode

This section presents an example of the interaction between the end-host and Diameter QoS application entities using Push Mode. The application layer signaling is, in this example, provided using SIP. Signaling for a QoS resource reservation is done using the QoS NSLP. The authorization of the QoS reservation request is done by the Diameter QoS application (DQA).
...Application layer SIP signaling........|.................|
. Invite(SDP offer)|
. +-----------------+-----------------+|
. 100 Trying |
. <---.-.-.--.-.--.-.--.-.--.-.--.-.-.--.+|
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
. |
The communication starts with SIP signaling between the two end points and the SIP server for negotiation and authorization of the requested service and its parameters (see Figure 27). As a part of the process, the SIP server verifies whether the user at Host A is authorized to use the requested service (and potentially the ability to be charged for the service usage). The DQA server is triggered to authorize the QoS request based on session parameters (i.e., SDP offer), initiate a Diameter QoS authorization session and install authorized QoS state to the Network Element via QIR message.

The DQA server may obtain the info of peer DQA client from pre-configured information or query the DNS based on Host A’s identity or IP address (In this case a DQA server is co-located with a SIP server and a DQA client is co-located with a Network element). The identity of Network Element is put into the Destination-Host AVP, the description of the QoS resources is included into QoS-Resources AVP, as well as duration of the authorization session (Authorization-Lifetime AVP). The NE interacts with the traffic control function and reserves the authorized QoS resources accordingly, for instance, the NE may serve as a signaling proxy and process the QoS signaling (e.g. initiation or termination of QoS signaling) based on the QoS decision received from the authorizing entity.

With successful QoS authorization, the SDP offer in SIP Invite is forwarded to Host B. Host B sends back a 18x (ringing) message towards Host A and processes the SDP. Once Host B accepts the call, it sends back a 200 OK, in which it includes description of the accepted session parameters (i.e. SDP answer).

The DQA server may verifies the accepted QoS against the pre-authorized QoS resources, and sends a Diameter RAR message to the DQA client in the network element for activating the installed policies and commit the resource allocation. With successful QoS enforcement, the 200 OK is forwarded towards Host A.

Note that the examples above show a sender-initiated reservation from the end host towards the corresponding node and a receiver-initiated reservation from the correspondent node towards the end host.
10. IANA Considerations

This section contains the namespaces that have either been created in this specification or had their values assigned to existing namespaces managed by IANA.

10.1. AVP Codes

IANA is requested to allocate two AVP codes to the following:

<table>
<thead>
<tr>
<th>AVP Code</th>
<th>Attribute Name</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>to be assigned</td>
<td>QoS-Authz-Data</td>
<td>Section 6.4</td>
</tr>
<tr>
<td>to be assigned</td>
<td>Bound-Auth-Session-Id</td>
<td>Section 6.4</td>
</tr>
</tbody>
</table>

10.2. AVP specific values

IANA is requested to allocate the following sub-registry values.

Sub-registry: Auth-Application-Id  AVP Values (code 258)

<table>
<thead>
<tr>
<th>AVP Values</th>
<th>Attribute Name</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>to be assigned</td>
<td>DIAMETER-QOS-NOSUPPORT</td>
<td>Section 5</td>
</tr>
<tr>
<td>to be assigned</td>
<td>DIAMETER-QOS-SUPPORT</td>
<td>Section 5</td>
</tr>
</tbody>
</table>

Sub-registry: Acct-Application-Id  AVP Values (code 259)

<table>
<thead>
<tr>
<th>AVP Values</th>
<th>Attribute Name</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>to be assigned</td>
<td>DIAMETER-QOS-NOSUPPORT</td>
<td>Section 5</td>
</tr>
<tr>
<td>to be assigned</td>
<td>DIAMETER-QOS-SUPPORT</td>
<td>Section 5</td>
</tr>
</tbody>
</table>

10.3. AVP flags

There are no new AVP flags defined for either the QoS-Authz-Data AVP or the Bound-Ath-Session-ID AVP.

10.4. Application IDs

IANA is requested to allocate the following application ID using the next value from the 7-16777215 range.
10.5. Command Codes

IANA is requested to allocate command code values for the following from the range 289-299.

<table>
<thead>
<tr>
<th>Code Value</th>
<th>Name</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>to be assigned</td>
<td>QoS-Authz-Request (QAR)</td>
<td>Section 5.1</td>
</tr>
<tr>
<td>to be assigned</td>
<td>QoS-Authz-Answer  (QAA)</td>
<td>Section 5.2</td>
</tr>
<tr>
<td>to be assigned</td>
<td>QoS-Install-Request (QIR)</td>
<td>Section 5.3</td>
</tr>
<tr>
<td>to be assigned</td>
<td>QoS-Install-Answer (QIA)</td>
<td>Section 5.4</td>
</tr>
</tbody>
</table>
11. Security Considerations

This document describes a mechanism for performing authorization of a QoS reservation at a third party entity. Therefore, it is necessary that the QoS signaling application to carry sufficient information that should be forwarded 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 can be authorized, such as in the home realm.

QoS signaling application MAY re-use the authenticated identities used for the establishment of the secured transport channel for the signaling messages, e.g., TLS or IPsec between the end host and the policy aware QoS NE. In addition, a collocation of the QoS NE with, for example, the Diameter NASREQ application (see [RFC4005]) may allow the QoS authorization to be based on the authenticated identity used during the network access authentication protocol run. If a co-located deployment is not desired then special security protection is required to ensure that arbitrary nodes cannot reuse a previous authentication exchange to perform an authorization decision.

Additionally, QoS authorization might be based on the usage of authorization tokens that are generated by the Authorizing Entity and provided to the end host via application layer signaling.

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.
12. Acknowledgements

The authors would like to thank John Loughney and Allison Mankin for their input to this document. In September 2005 Robert Hancock, Jukka Manner, Cornelia Kappler, Xiaoming Fu, Georgios Karagiannis and Elwyn Davies provided a detailed review. Robert also provided us with good feedback earlier in 2005. Jerry Ash provided us review comments late 2005/early 2006. Rajith R provided some inputs to the document early 2007.
13. Contributors

The authors would like to thank Tseno Tsenov (tseno.tsenov@gmail.com) and Frank Alfano (falfano@lucent.com) for starting the Diameter Quality of Service work within the IETF, for your significant draft contributions and for being the driving force for the first few draft versions.

[Editor’s Note: A bit of history needs to be included here.]
14. References

14.1. Normative References

[I-D.ietf-dime-qos-attributes]
Korhonen, J., Tschofenig, H., Arumaithurai, M., and M. Jones, "Quality of Service Attributes for Diameter",

[I-D.ietf-dime-qos-parameters]
Korhonen, J. and H. Tschofenig, "Quality of Service Parameters for Usage with the AAA Framework",


14.2. Informative References

[I-D.ietf-nsis-ntlp]

[I-D.ietf-nsis-qos-nslp]
Manner, J., "NSLP for Quality-of-Service Signaling",


[RFC2486] Aboba, B. and M. Beadles, "The Network Access Identifier",...


Authors’ Addresses

Dong Sun (editor)
Alcatel-Lucent
600-700 Mountain Ave
Murray Hill, NJ  07974
USA
Phone: +1 908 582 2617
Email: dongsun@alcatel-lucent.com

Peter J. McCann
Motorola Labs
1301 E. Algonquin Rd
Schaumburg, IL  60196
USA
Phone: +1 847 576 3440
Email: pete.mccann@motorola.com

Hannes Tschofenig
Nokia Siemens Networks
Linnoitustie 6
Espoo  02600
Finland
Phone: +358 (50) 4871445
Email: Hannes.Tschofenig@nsn.com
URI:  http://www.tschofenig.com

Tina Tsou
Huawei
Shenzhen,
P.R.C
Email: tena@huawei.com
Avri Doria
Lulea University of Technology
Arbetsvetenskap
Lulea, SE-97187
Sweden

Email: avri@ltu.se

Glen Zorn

Email: glenzorn@comcast.net