Authentication, Authorization and
Accounting
Internet-Draft
Expires: March 9, 2006

F. Alfano
P. McCann
Lucent Technologies
H. Tschofenig
T. Tsenov
Siemens

September 5, 2005

Diameter Quality of Service Application
draft-alfano-aaa-qosprot-04.txt

Status of this Memo

Copyright Notice

Abstract

This document describes a Diameter application that performs Authentication, Authorization, and Accounting for Quality of Service (QoS) 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 consumed during the lifetime of the application flow. Clients that implement the Diameter QoS application contact an authorizing entity/application server that is located somewhere in the network, allowing for a wide variety of flexible deployment models.

Table of Contents

1. Introduction

To meet the Quality of Service needs of applications such as Voice-over-IP in a heavily loaded network, packets belonging to real-time application flows must be identified and segregated from other traffic to ensure that bandwidth, delay, and loss rate requirements are met. In addition, new flows should not be added to the network when it is at or near capacity, which would result in degradation of quality for all flows carried by the network.

In some cases, these goals can be achieved with mechanisms such as differentiated services and/or end-to-end congestion and admission control. However, when bandwidth is scarce and must be carefully managed, such as in cellular networks, or when applications and transport protocols lack the capability to perform end-to-end congestion control, explicit reservation techniques are required. In these cases, the endpoints will send reservation requests to edge and/or interior nodes along the communication path. In addition to verifying whether resources are available, the recipient of a reservation request must also authenticate and authorize the request, especially in an environment where the endpoints are not trusted. In addition, these nodes will generate accounting information about the resources used and attribute usage to the requesting endpoints. This will enable the owner of the network element to generate usage-sensitive billing records and to understand how to allocate new network capacity.

A variety of protocols could be used to make a QoS request, including RSVP [RFC2210], NSIS [I-D.ietf-nsis-qos-nslp], link-specific

signaling or even SIP/SDP [RFC2327]. This document aims to be agnostic to the used QoS signaling protocol and to the signaled QoS model.

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:

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 will 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 is that entity responsible for authorizing QoS requests for a particular application flow or aggregate. This may be a Diameter server (with a subscriber database) or an application server acting as a Diameter server.

AAA Cloud

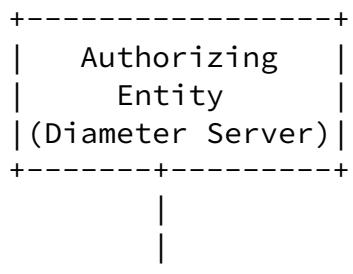
A network of AAA proxy/broker arrangements.

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]) from a functionality point of view.

3. Framework

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



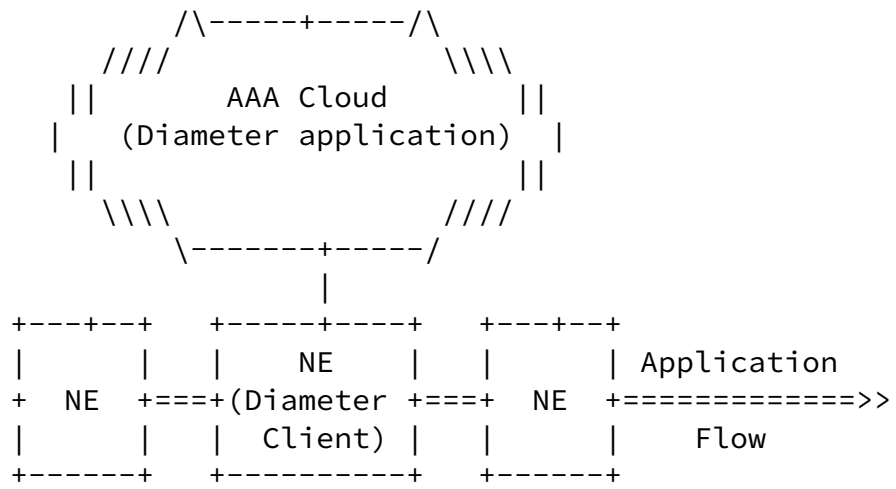


Figure 1: An Architecture supporting QoS-AAA

Figure 1 depicts network elements through which application 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. QoS aware network elements will request authorization from the AAA cloud based on an incoming QoS reservation request, which will route the request, for example, to the home network where the home authorizing entity will return the result of the authorization decision.

In more complex deployment models, the authorization will be based on dynamic application state, so that the request must be authenticated and authorized based on information from one or more application servers. 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.

+--+

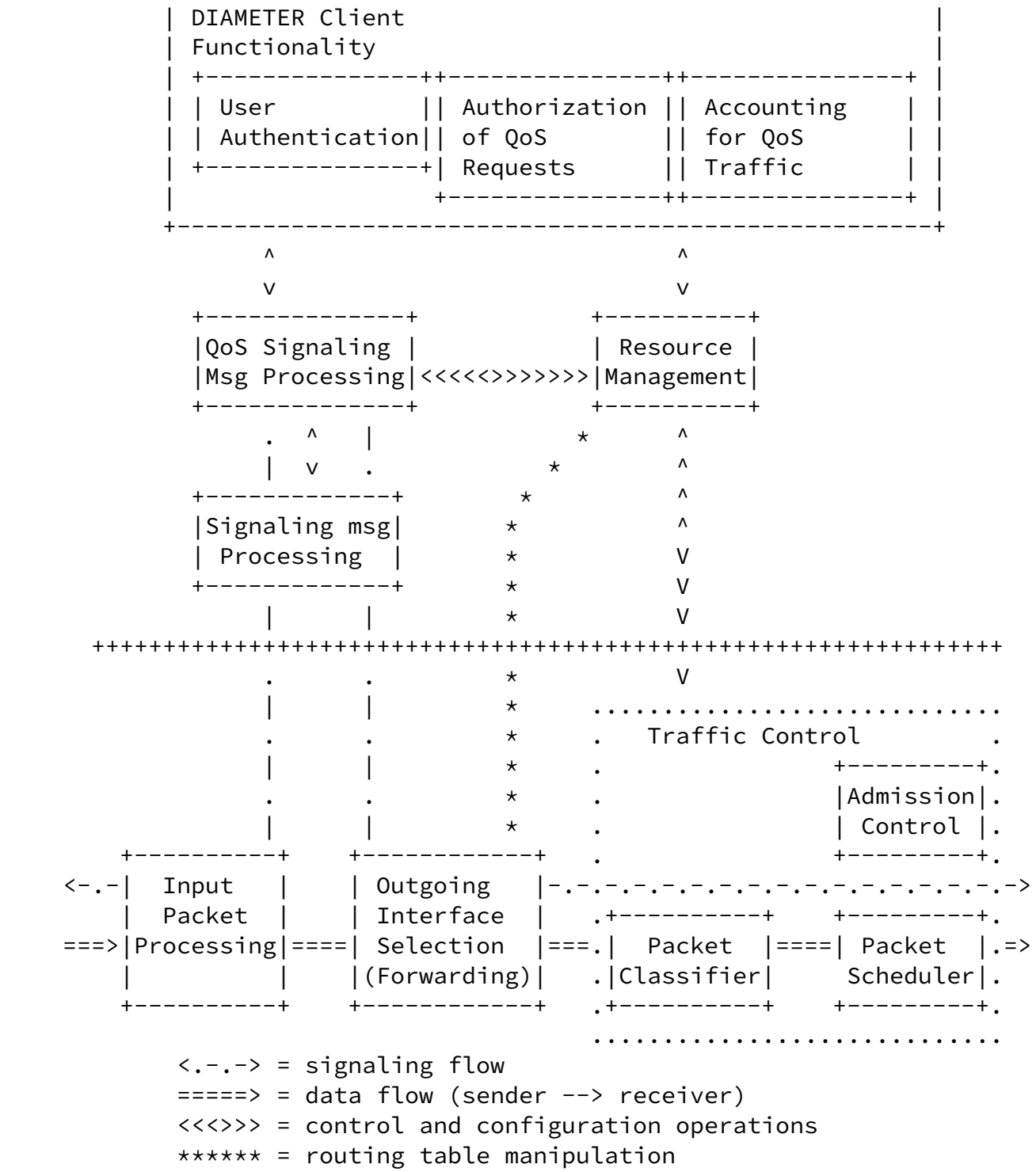


Figure 2: Network element functional model

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. Authorization models

Three fundamental models for authorizing QoS reservations exist: one two-party and two three party models. See [I-D.tschofenig-nsis-aaa-issues] and in [I-D.tschofenig-nsis-qos-authz-issues] for a more detailed discussion of authorization models and the impact for QoS reservations. From the Diameter QoS application's point of view these models differ in type of information that need to be carried. Here we focus on the 'Three party model' (Figure 3) and the Token based three party model' (Figure 4). With the 'Two party model' 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.

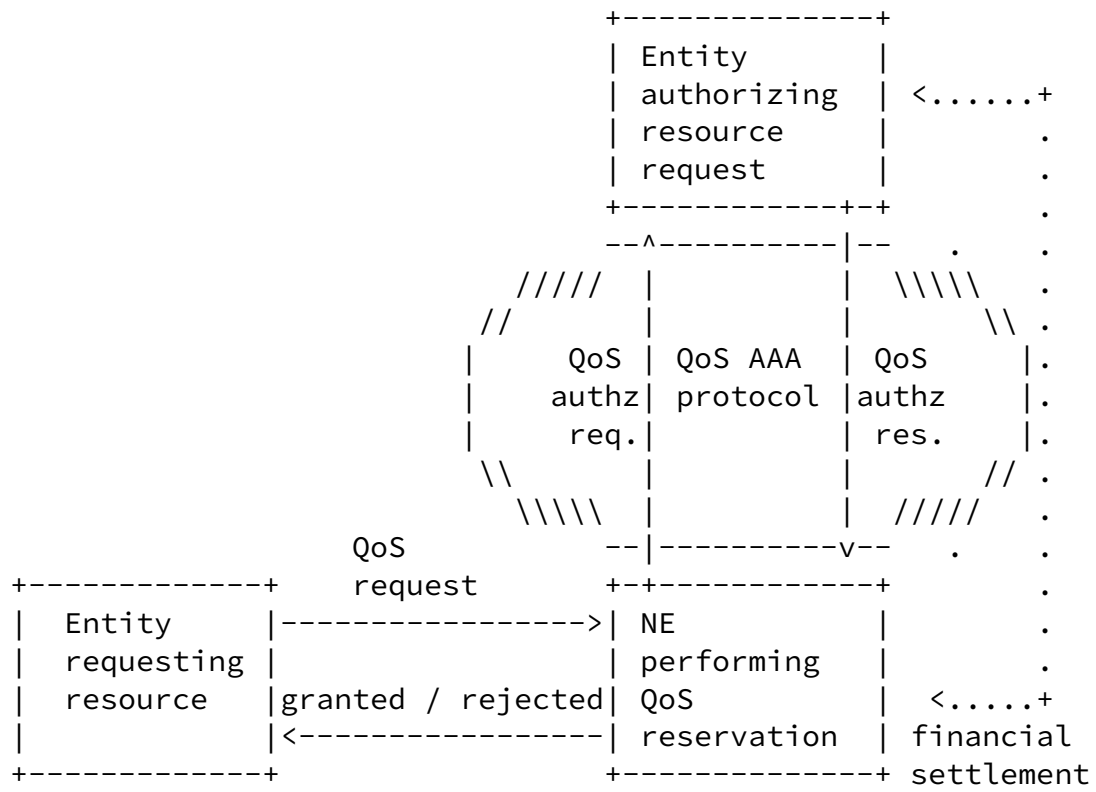


Figure 3: Three Party Model

With the 'Three party model' a QoS reservation request that hits the Network Element is forwarded to the Authorizing Entity (e.g., 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 consumed resources of the user via the home network.

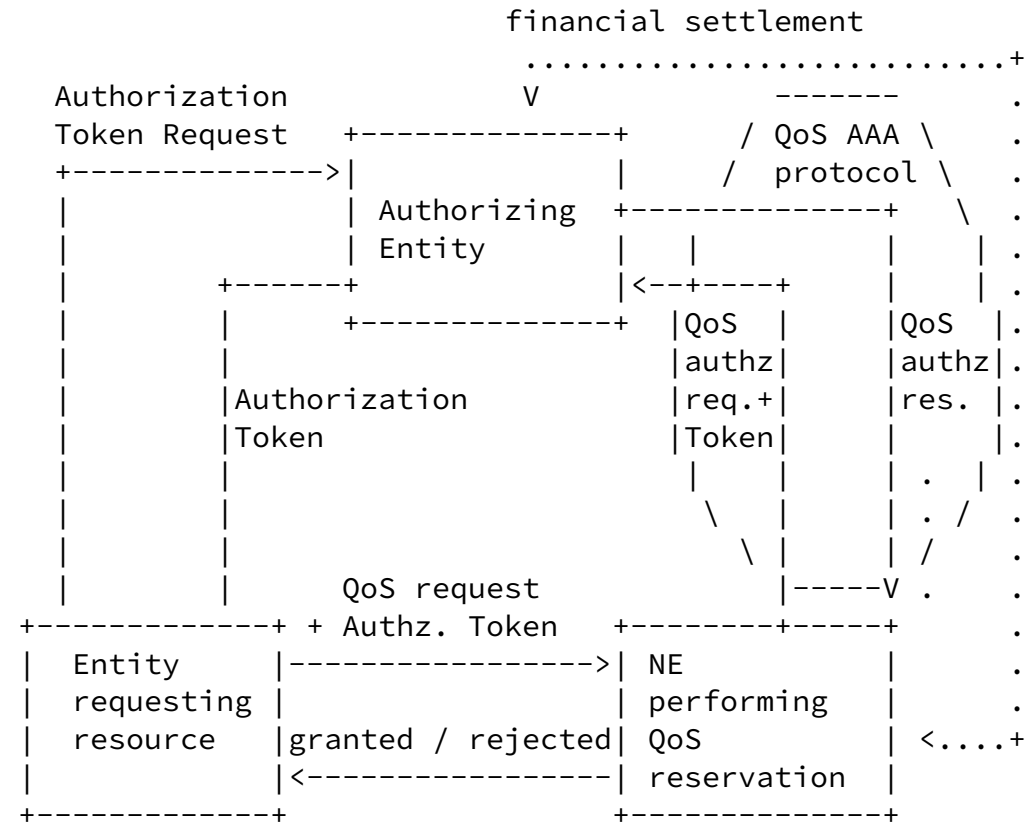


Figure 4: Token based Three Party Model

The 'Token based Three Party model' 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], with the OSP [ETSI-OSP] or as outlined in [I-D.ietf-sipping-trait-authz] and [I-D.tschofenig-sip-saml].

3.3. QoS authorization considerations

A QoS authorization 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 requirements 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.

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 MUST 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 MUST send accounting records for a particular application flow to the authorizing entity for that flow or to another entity identified by the authorizing 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 MUST 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 NASREQ [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., TLS handshake in GIST [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 (of 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.

4. Diameter QoS Authorization session establishment and management

4.1. Involved parties

Authorization models supported by this application include three parties:

- Resource requesting entity
- Network Elements (Diameter QoS clients)
- Authorizing Entity (Diameter QoS 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., Diameter QoS client) and the Authorizing Entity (i.e., Diameter QoS server).

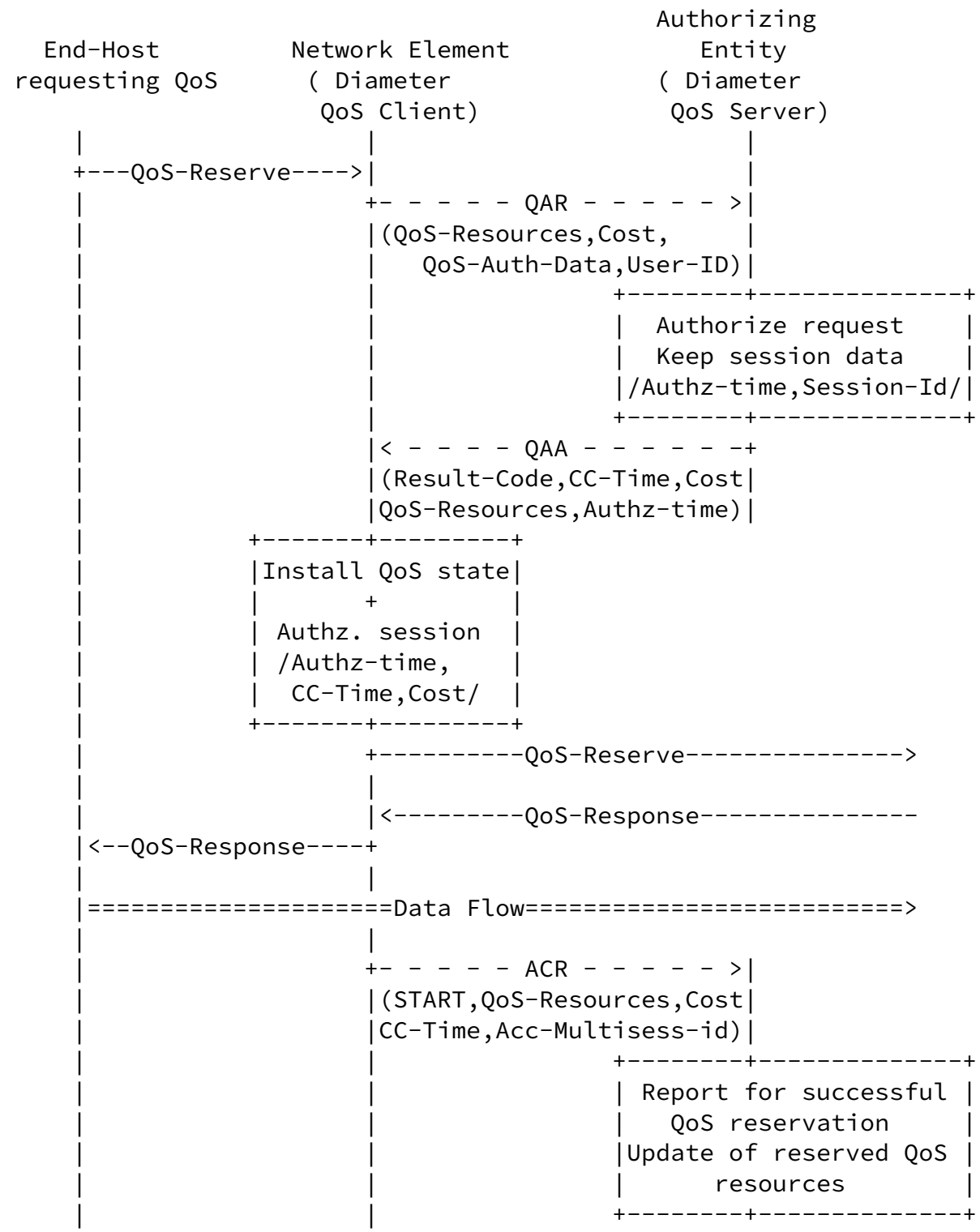
The QoS resource requesting entity may communicate with the Authorizing Entity using application layer signaling for negotiation of service parameters. As part of this application layer protocol interaction, for example using SIP, authentication and authorization might take place (see Figure 4). This message exchange is, however, outside the scope of this document. This protocol communication 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 desired since this applications aims to be generic.

4.2. Initial QoS authorization (Diameter QoS authorization session establishment)

Figure 5 shows the protocol interaction between a resource requesting entity, a Network Element and the Authorizing Entity.

A request for a QoS reservation received by a Network Element initiates a Diameter QoS authorization session. The Network Element generates a QoS-Authorization-Request message (QAR) in which it maps required objects from the QoS signaling message to Diameter AVPs. Authorizing Entity's identity (Destination-Host AVP), pointer to the application session and/or identity and credentials of the QoS resource requesting entity (QoS-Authentication-Data, User-Name-ID AVPs), requested QoS parameters (QSPEC AVP), signaling session identifier and/or QoS enabled data flows identifiers (Signaling-Session-Id and Flows AVPs) 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 in the realm of the QoS requesting entity or also be an application server.

When the Diameter QoS server receives the QAR authorization processing starts. Based on the information in the QoS-Authentication-Data, User-Name-ID and QoS-Authorized-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 authorization decision is then reflected in the response returned to the Diameter client with the QoS-Authorization-Answer message (QAA).


End-Host requesting QoS
Network Element (Diameter QoS Client)
Authorizing Entity (Diameter QoS Server)
---QoS-Reserve---->
- - - - - QAR - - - - - >
(QoS-Resources,Cost, QoS-Auth-Data,User-ID)
Authorize request
Keep session data
/Authz-time,Session-Id/
< - - - - - QAA - - - - - -+
(Result-Code,CC-Time,Cost
QoS-Resources,Authz-time)
Install QoS state
Authz. session /Authz-time, CC-Time,Cost/
----------QoS-Reserve---------->
<---------QoS-Response----------
<--QoS-Response----
==========Data Flow==========>
- - - - - ACR - - - - - >
(START,QoS-Resources,Cost
CC-Time,Acc-Multisess-id)
Report for successful QoS reservation
Update of reserved QoS resources

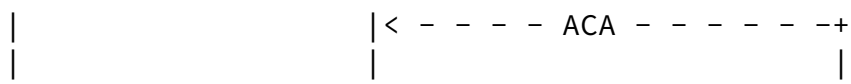


Figure 5: Initial QoS request authorization

The Authorizing Entity keeps authorization session state and SHOULD save additional information for management of the session (e.g., Acc-Multi-Session-Id, Signaling-Session-Id, authentication data) as part

of the session state information. A Signaling-session-Id (if present) SHOULD be used together with the generated Acc-Multi-Session-Id AVP for binding the authorization and the accounting session information in case of end host mobility (i.e., to correlate the Diameter sessions that are initiated for the same signaling session from different QoS NE).

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), information about the authorized QoS resources and the status of the authorized flow (enabled/disabled) is provided in the QoS-Authorization-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 (see Figure 2).

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 5). 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 4.5 and Section 5.

The indication of a successful QoS reservation and activation of the data flow, is done by the transmission of an Accounting Request (ACR) message, which reports the parameters of the established QoS state: reserved resources, duration of the reservation, identification of

the QoS enabled flow/QoS signaling session and accounting parameters. The Diameter QoS server acknowledges the reserved QoS resources with the Accounting Answer (ACA) message where the Result-Code is set to 'DIAMETER_SUCCESS'. Note that the reserved QoS resources reported in the ACR message MAY be less than those initially authorized with QAA message, due to the QoS signaling specific behavior (e.g., receiver-initiated reservations with One-Path-With-Advertisements) specific process of QoS negotiation along the data path.

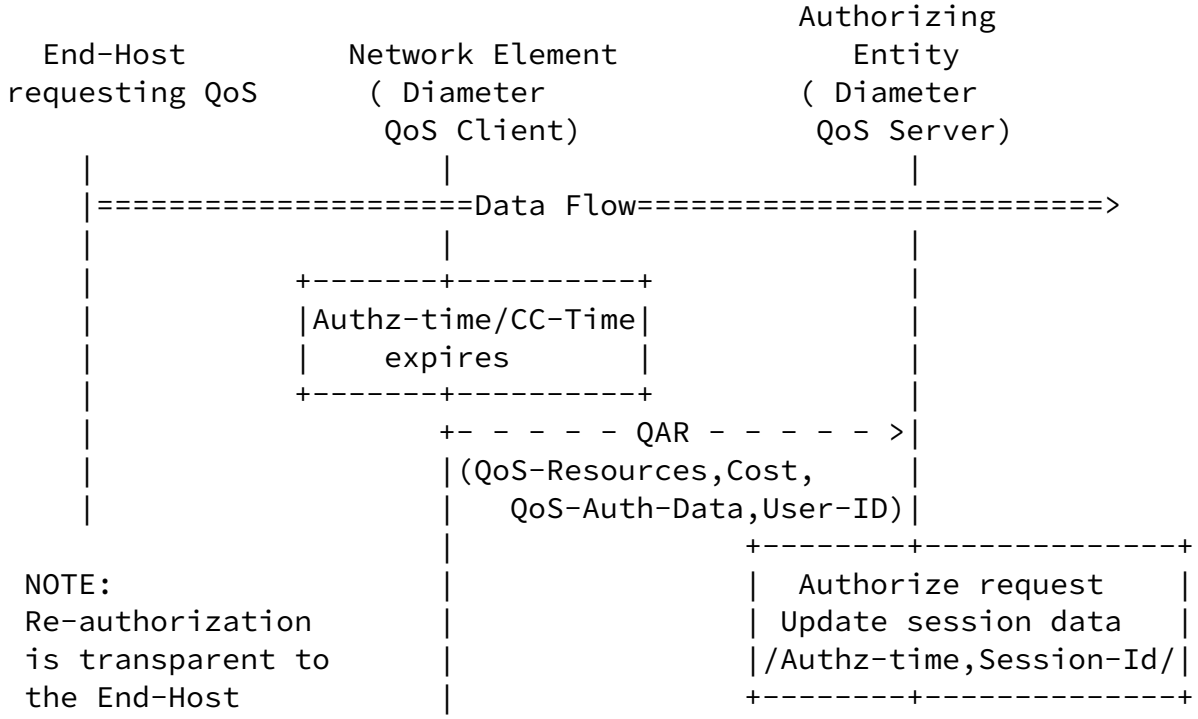
4.3. QoS authorization session re-authorization

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.

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 when the Network Element receives a QoS signaling message with the semantic of modifying an ongoing authorized QoS session or when authorization lifetime expires or by an accounting event (see Section 5)(Figure 6)


End-Host requesting QoS
Network Element (Diameter QoS Client)
Authorizing Entity (Diameter QoS Server)
Data Flow
Authz-time/CC-Time expires
QAR
(QoS-Resources,Cost, QoS-Auth-Data,User-ID)
Authorize request
Update session data
/Authz-time,Session-Id/
NOTE:
Re-authorization is transparent to the End-Host

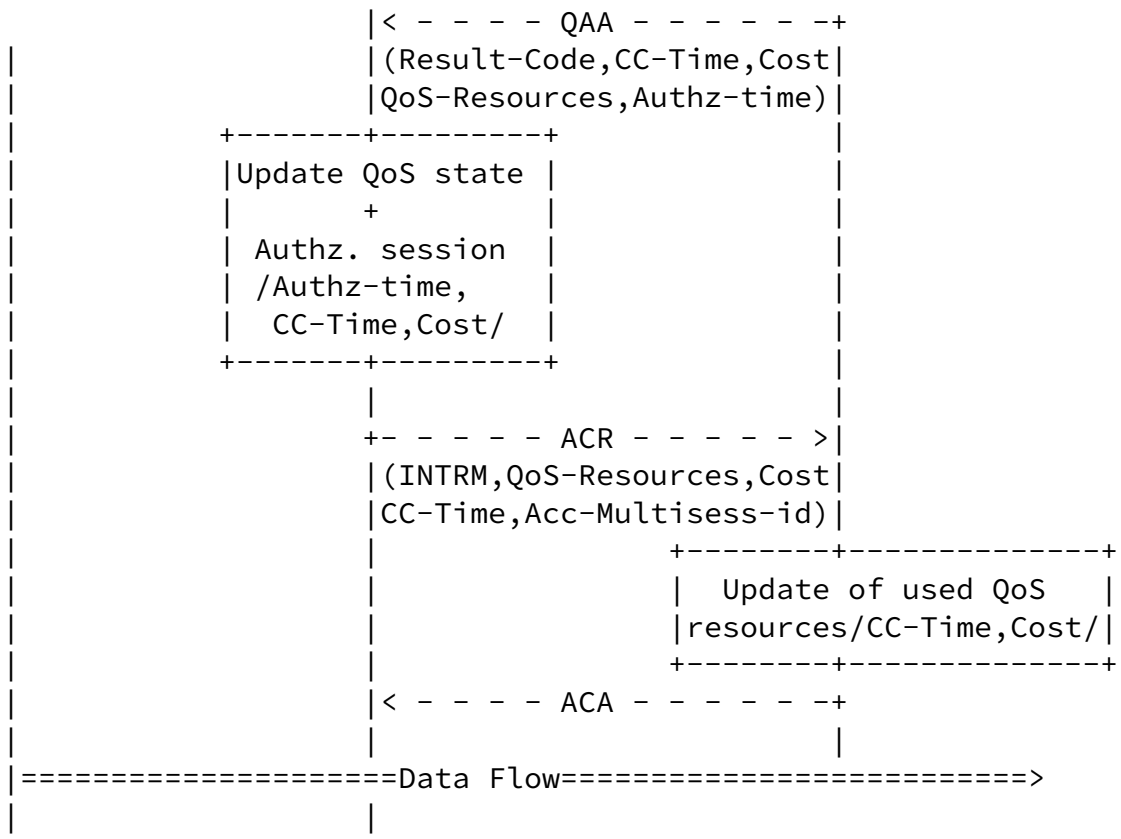


Figure 6: QoS request re-authorization

4.3.2. Server-side initiated Re-Authorization

The Authorizing Entity MAY optionally initiate a QoS re-authorization by issuing a Re-Auth-Request message (RAR) as defined in the Diameter

base protocol [BASE]. A Network Element client 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 and MUST initiate a QoS reservation re-authorization by sending a QoS-Authorization-Request (QAR) message towards the Authorizing entity.

4.4. Server-side initiated QoS parameter provisioning

The Authorizing Entity is enabled to update installed QoS parameters and flow state at the Network Element by sending a QoS-Install Request message (QIR). Network Elements MUST apply the updates and

respond with an QoS-Install Answer message (QIA). This functionality, for example, allows to update already authorized flow status of an established QoS reservation due to a change at the application layer session (Figure 7).

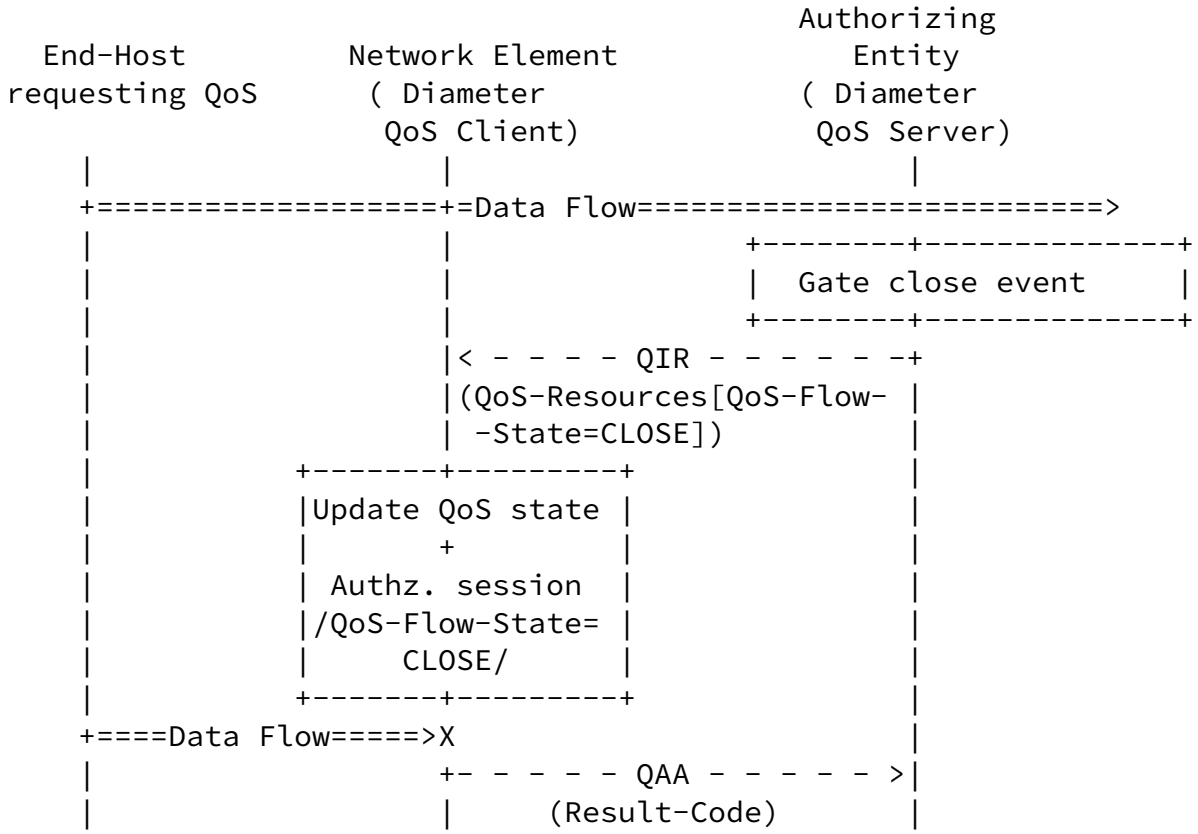


Figure 7: Server-side initiated QoS parameter provisioning

The Authorizing Entity MAY initiate QoS authorization session establishment and QoS reservation state installation (prior to a request from a Network Element). Such function requires that the Authorizing Entity has knowledge of specific information identifying the Network Element that should be contacted and the data flow for

which the QoS reservation should be established.

4.5. Session Termination

4.5.1. Client-side initiated session termination

A QoS authorization session MAY be terminated by the Diameter client by sending a Session-Termination-Request message (STR) to the Diameter server. This is a Base Diameter protocol functionality and it is defined in [RFC3588]. Session termination can be caused by a QoS signaling messaging requesting to delete an existing QoS reservation state or it can be caused as a result of a loss of bearer report. After a successful termination of the authorization session, final accounting messages MUST be exchanged (Figure 8).

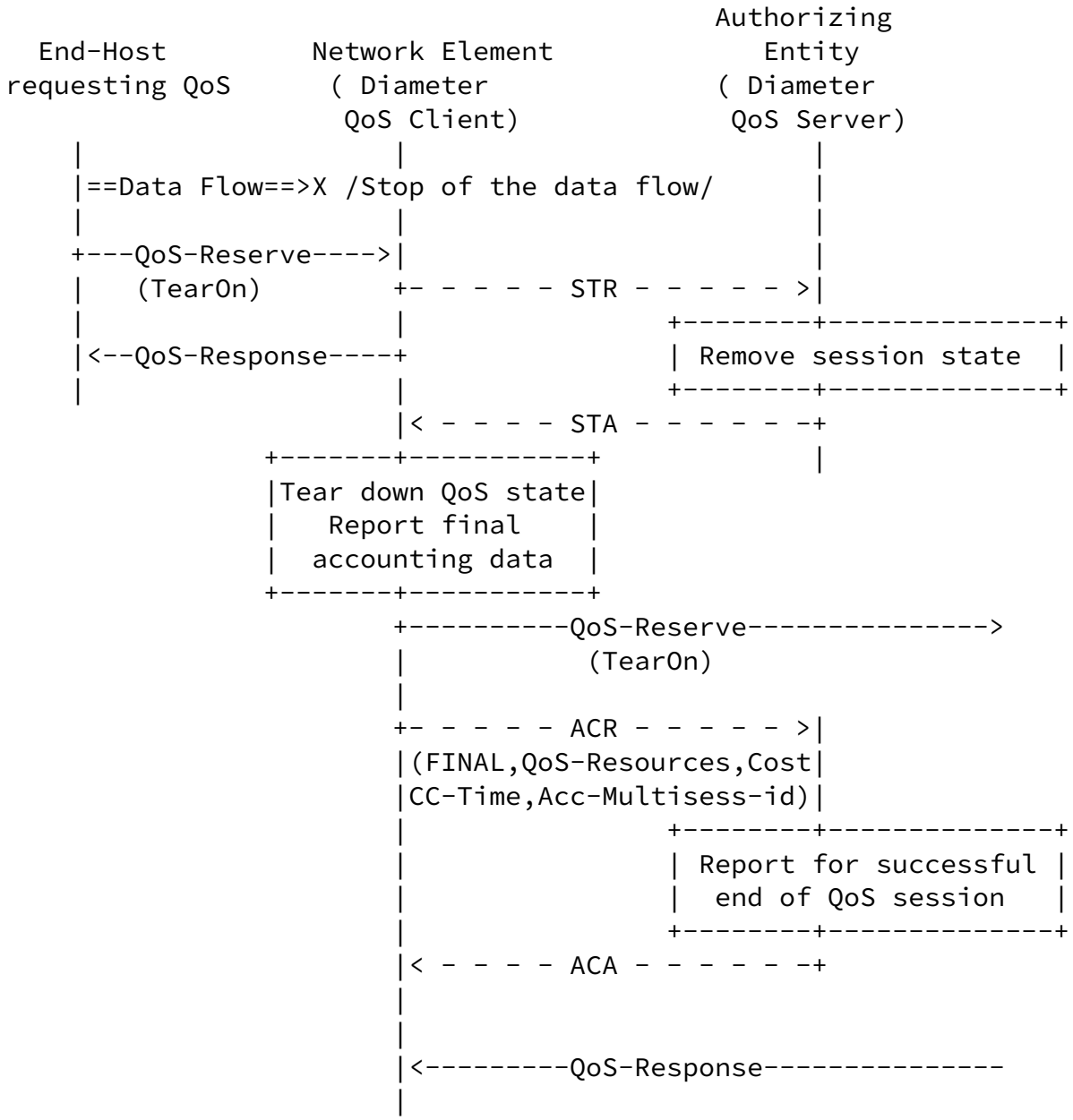


Figure 8: Client-side initiated session termination

4.5.2. 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 Base Diameter protocol functionality 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. A final accounting message exchanges MUST be

triggered as a result of this ASR message exchange (Figure 9).

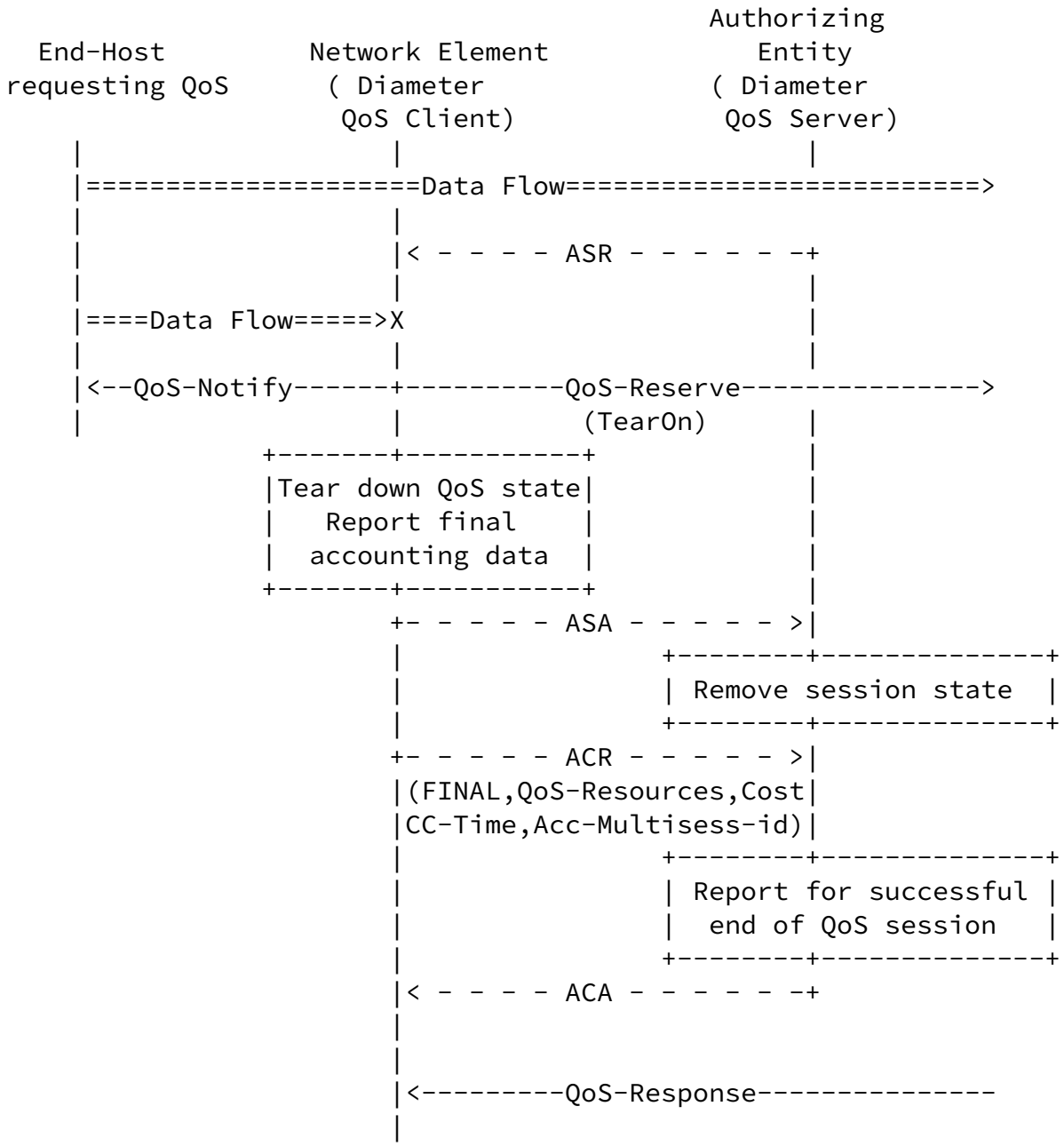


Figure 9: Server-side initiated session termination

5. Accounting

The Diameter QoS application provides accounting for usage of reserved QoS resources. Diameter QoS accounting has built-in support for online, duration based accounting. This accounting is based on the notion that the routers making the QoS Authorization Request (Diameter QoS clients) are in the best position to determine the cost of those resources. This cost represents the financial settlement that will be ultimately demanded by the router if the Resource Authorizing Entity authorizes the reservation.

In the Diameter QoS application, the router MAY send a Cost-Information AVP ([RFC4006]) in the QAR. If the Cost-Information AVP includes a Cost-Unit AVP ([RFC4006]) then the Cost-Unit SHOULD be "minute". The Cost-Information AVPs represent the cost to allocate the resources requested in the QoS-Authorization-Resources AVP included in the same QAR message. The QAR MAY optionally contain a Tariff-Time-Change AVP ([RFC4006]) which is the time at which the cost will change, a second Cost-Information AVP, which is the cost of the reserved resources after the tariff time change, and a second Tariff-Time-Change, which is the time at which the tariff would change again. Either all three or none of these AVPs MUST be present in the QAR.

The Resource Authorizing Entity returns a CC-Time AVP ([RFC4006]) in the QAA message which is the total authorized gate-on time for the service. If the QAR included two Tariff-Time-Change AVPs, the current time plus the CC-Time AVP returned in the QAA MUST NOT exceed the second Tariff-Time-Change AVP from the QAR. Based on information in the Cost-Information AVPs, the Resource Authorizing Entity can use the CC-Time AVP to guarantee that the total cost of the session will not exceed a certain threshold, which allows, for example, support of prepaid users.

Each ACR message contains a triplet of QoS-Authorization-Resources

AVP, Cost-Information AVP, and CC-Time AVP. This represents the total time consumed at the given cost for the given resources. Note that an ACR message MUST be sent separately for each interval defined by the Tariff-Time-Change AVPs and the expiration of the CC-Time returned in the QAA (Figure 6).

The Network Element starts an accounting session by sending an Accounting-Request message (ACR) after successful QoS reservation and activation of the data flow (Figure 5). After every successful re-authorization procedure the Network element MUST initiate an interim accounting message exchange (Figure 6). After successful session termination the Network element MUST initiate a final exchange of accounting messages for terminating of the accounting session and

reporting final records for the usage of reserved QoS resources (Figure 8).

6. Diameter QoS authorization application Messages

The Diameter QoS Application requires the definition of new mandatory AVPs and Command-codes [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.

Command-Name	Abbrev.	Code	Reference
QoS-Authz-Request	QAR	[TBD]	Section 6.1
QoS-Authz-Answer	QAA	[TBD]	Section 6.2
QoS-Install-Request	QIR	[TBD]	Section 6.3
QoS-Install-Answer	QIA	[TBD]	Section 6.4

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

Command-Name	Abbrev.	Code	Reference
Accounting-Request	ACR	271	RFC 3588
Accounting-Request	ACR	271	RFC 3588

Accounting-Answer	ACA	271	RFC 3588
Re-Auth-Request	RAR	258	RFC 3588
Re-Auth-Answer	RAA	258	RFC 3588
Abort-Session-Request	ASR	274	RFC 3588
Abort-Session-Answer	ACA	274	RFC 3588
Session-Term-Request	STR	275	RFC 3588
Session-Term-Answer	STA	275	RFC 3588

Diameter nodes conforming to this specification MAY advertise support by including the value of TBD (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/QAA and QIR/QIA 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 commands are defined in the Diameter base protocol and no additional mandatory AVPs for those commands are defined in this document.

6.1. QoS-Authorization Request (QAR)

The QoS-Authorization-Request message (QAR) indicated by the Command-Code field set to TDB (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 is defined as follows:

```
 <QoS-Request> ::= < Diameter Header: XXX, REQ, PXY >
                     < Session-Id >
                     { Auth-Application-Id }
                     { Origin-Host }
                     { Origin-Realm }
                     { Destination-Realm }
                     { Auth-Request-Type }
                     [ Destination-Host ]
                     [ User-Name ]
                   *  [ QoS-Authorization-Resources ]
                     [ QoS-Authentication-Data ]
                     [ Cost-Information ]
                     [ Acc-Multisession-Id ]
                     [ Bound-Auth-Session-Id ]
                   *  [ AVP ]
```

6.2. QoS-Authorization Answer (QAA)

The QoS-Authorization-Answer message (QAA), indicated by the Command-Code field set to TBD (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 as well as accounting and transport plane gating information.

The message format is defined as follows:


```
 <QoS-Answer> ::= < Diameter Header: XXX, PXY >
                  < Session-Id >
                  { Auth-Application-Id }
                  { Auth-Request-Type }
                  { Result-Code }
                  { Origin-Host }
                  { Origin-Realm }
```

```
                    *  [ QoS-Authorization-Resources ]
                       [ CC-Time ]
                       [ Acc-Multisession-Id ]
                       [ Session-Timeout ]
                       [ Authz-Session-Lifetime ]
                       [ Authz-Grace-Period ]
                    *  [ AVP ]
```

6.3. QoS-Install Request (QIR)

The QoS-Install Request message (QIR), indicated by the Command-Code field set to TDB (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:

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

6.4. QoS-Install Answer (QAA)

The QoS-Install Answer message (QAA), indicated by the Command-Code field set to TBD (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-Authorization-Resources ]
                       * [ AVP ]
```

6.5. Accounting Request (ACR)

The Accounting Request message (ACR), indicated by the Command-Code field set to 271 and 'R' bit set in the Command Flags field is used by Network Element to report parameters of the authorized and established QoS reservation.

The message MUST carry accounting information authorized QoS resources and its usage, e.g., QoS-Authorized-Resources, CC-Time, CC-Cost, Acc-Multi-Session-Id.

The message format is defined as follows:

```
<Accounting-Request> ::= < Diameter Header: XXX, REQ, PXY >
                         < Session-Id >
                         { Acct-Application-Id }
                         { Destination-Realm }
                         [ Destination-Host ]
                         [ Accounting-Record-Type ]
                         [ Accounting-Record-Number ]
                       * [ QoS-Authorization-Resources ]
                         [ Cost-Information ]
                         [ CC-Time ]
                         [ Acc-Multi-Session-Id ]
                       * [ AVP ]
```

6.6. Accounting Answer (ACA)

The Accounting Answer message (ACA), indicated by the Command-Code field set to 271 and 'R' bit cleared in the Command Flags field is sent in response to the Accounting Request message (ACR) as an acknowledgment of the ACR message and MAY carry additional management information for the accounting session, e.g. Acc-Interim-Interval AVP.

The message format is defined as follows:

```
<Accounting-Answer> ::= < Diameter Header: XXX, PXY >
                        < Session-Id >
                        { Acct-Application-Id }
                        [ Result-Code ]
                        [ Accounting-Record-Type ]
                        [ Accounting-Record-Number ]
                        [ Acc-Multi-Session-Id ]
                      * [ AVP ]
```

7. Diameter QoS Authorization 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. Diameter Base Protocol AVPs

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

Attribute Name	AVP Code	Reference [RFC3588]
Origin-Host	264	Section 6.3
Origin-Realm	296	Section 6.4
Destination-Host	293	Section 6.5
Destination-Realm	283	Section 6.6
Auth-Application-Id	258	Section 6.8
Result-Code	268	Section 7.1
Auth-Request-Type	274	Section 8.7
Session-Id	263	Section 8.8
Authz-Lifetime	291	Section 8.9
Authz-Grace-Period	276	Section 8.10
Session-Timeout	27	Section 8.13
User-Name	1	Section 8.14
QoS-Filter-Rule	407	Section 6.9 [RFC4005]

Some of the listed AVPs require definition and assignment of additional values which is described here:

Auth-Application-Id AVP

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 (TBD).

7.2. Credit Control application AVPs

The Diameter QoS application provides accounting for usage of reserved QoS resources. Diameter QoS accounting has built-in support for online, duration based accounting. For this purpose it re-uses a number of AVPs defined in Diameter Credit Control application. [RFC4006].

Attribute Name	AVP Code	Reference [RFC4006]
Cost-Information AVP	423	Section 8.7
Unit-Value AVP	445	Section 8.8
Currency-Code AVP	425	Section 8.11
Cost-Unit AVP	424	Section 8.12
CC-Time AVP	420	Section 8.21
Tariff-Time-Change AVP	451	Section 6.20

Usage of the listed AVPs is described in Section 5

7.3. Accounting AVPs

The Diameter QoS application uses Diameter Accounting and accounting AVPs as defined in Section 9 of [RFC3588]. Additional description of the usage of some of them in QoS authorization context is provided:

Attribute Name	AVP Code	Reference [RFC3588]
Acct-Application-Id	259	Section 6.9
Accounting-Record-Type	480	Section 9.8.1
Accounting-Interim-Interval	85	Section 9.8.2
Accounting-Record-Number	485	Section 9.8.3
Accounting-Realtime-Required	483	Section 9.8.7
Acc-Multi-Session-ID	50	Section 9.8.5

The following AVP needs further explanation:

Acct-Application-Id AVP

The Acct-Application-Id AVP (AVP Code 259)is assigned by IANA to Diameter applications. The value of the Acct-Application-Id for the Diameter QoS application is TBD (TBD).

Acc-Multisession-ID

Acc-Multi-Session-ID AVP (AVP Code 50) SHOULD be used to link multiple accounting sessions together, allowing the correlation of accounting information. This AVP MAY be returned by the Diameter server in a QoS-Authorization-Answer message (QAA), and MUST be used in all accounting messages for the given session.

7.4. Diameter QoS Application Defined AVPs

This section defines the Quality of Service AVPs that are specific to the Diameter QoS application and MAY be included in the Diameter QoS application messages. Unlike the approach followed with RSVP (see [RFC2749]), where the entire RSVP message is encapsulated into a COPS message, only the relevant fields SHOULD be included. This approach

avoids a certain overhead of transmitting fields which are irrelevant for the AAA infrastructure. It keeps implementations simpler and it allows the reuse of other Diameter AVPs.

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
Signaling-Session-Id	TBD	7.4	Unsigned32	M	P		V	Y
Flow-ID	TBD	7.4	Unsigned32	M	P		V	Y
SPI	TBD	7.4	Unsigned32	M	P		V	Y
QoS-Flow-State	TBD	7.4	Enumerated	M	P		V	Y
IND-Flow	TBD	7.4	Grouped	M	P		V	Y
Flows	TBD	7.4	Grouped	M	P		V	Y
QSPEC	TBD	7.4	OctetString	M	P		V	Y

QoS-Auth -Resources	TBD	7.4	Grouped	M	P		V	Y	
QoS-Auth-Data Bound-Auth -Session-Id	TBD	7.4	UTF8String	M	P		V	Y	

Signaling-Session-ID

Signaling-Session-ID AVP (AVP Code TBD) is of type Unsigned32 and contains a copy of the QoS signaling session identifier, which is a unique identifier of the QoS signaling session that in NSIS case remains unchanged for the duration of the session.

Flow-ID

The Flow-ID AVP (AVP Code TBD) is of type Unsigned32 and contains identifier of an IP flow.

SPI

The SPI AVP (AVP Code TBD) is of type Unsigned32 and extends the QoS-Filter-Rule AVP to support IPsec protected traffic.

QoS-Flow-State

The QoS-Flow-State AVP (AVP Code TBD) is of type Enumerated. It gives an indication by the Authorizing entity how the flow MUST be treated. When included in a QAA message, it is instructions to the QoS network element with regard to the state to which the flow should be set. The supported values are:

0 Open - Enable the transport plane service, for which the signaling is done
1 Close - Disable the transport plane service
2 Maintain - Current state (enabled/disabled) of the transport plane service is maintained

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

IND-Flows

The IND-Flows AVP (AVP Code TBD) is of type Grouped and specifies IP Flows via their flow identifiers and filter-rule.

```
IND-Flows ::= <AVP Header>
              [Flow-Id]
              [QoS-Filter-Rule]
        [0-1] [SPI]
        [0-1] [QoS-Flow-State]
```

Flows

The Flows AVP (AVP Code TBD) is of type Grouped and contains all the individual flows that receive the same QoS specified in the included QSPEC.

```
Flows    ::= < AVP Header: XXX >
       [1+]* [ IND-Flows ]
```

QSPEC

The QSPEC AVP (AVP Code TBD) is of type OctetString and contains QoS parameter information. Description format is taken from QoS NSLP Qspec template, which is expected to cover all present QoS

description methods [I-D.ietf-nsis-qspec].

QoS-Authorization-Resources

The QoS-Auth-Resources AVP (AVP Code TBD) is of type Grouped and includes description of the resources that have been requested by the user or authorized by the application server for a particular

QoS request. More than one MAY be included into a message.

```
QoS-Auth-Resources ::= < AVP Header: XXX >
                 [0-1]  [ Signaling-Session-ID ]
                 [0-1]* [ Flows ]
                   [1]  [ QSPEC ]
                 [0-1]  [ QoS-Flow-State ]
```

Included QoS-Flow-State AVP SHOULD be overwritten by any included QoS-Flow-State AVPs specified for the individual flows.

QoS-Authentication-Data

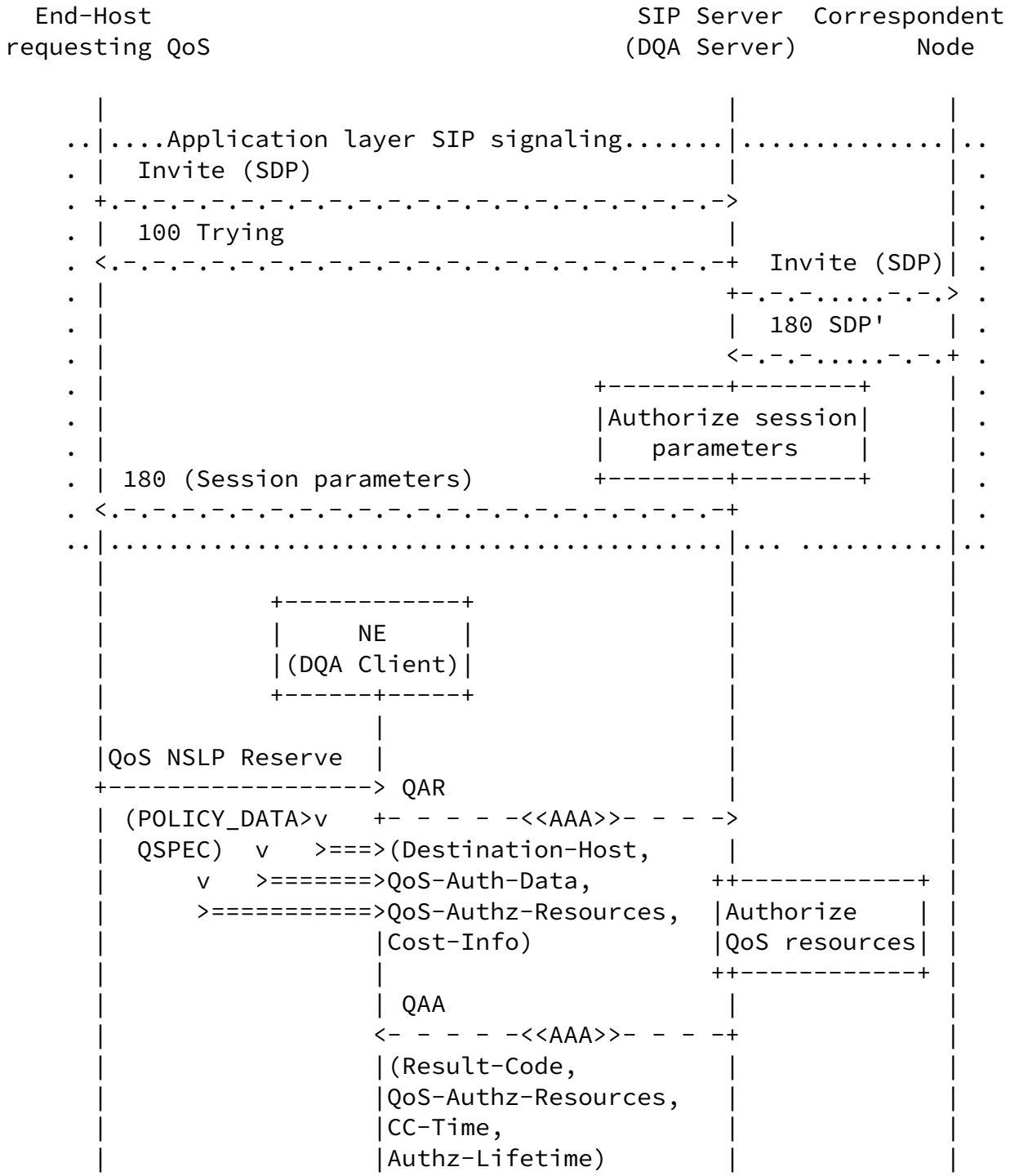
The QoS-Authentication-Data AVP (AVP Code TBD) is of type OctetString. It is a container that carries application session or user specific data that allows to the Authorizing entity in computation of the authorization decision.

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 priory authentication of the end host done by a collocated NASREQ application at the QoS NE.

8. Examples

This section presents an example of the interaction between the application layer signaling and the QoS signaling along the data path. 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).



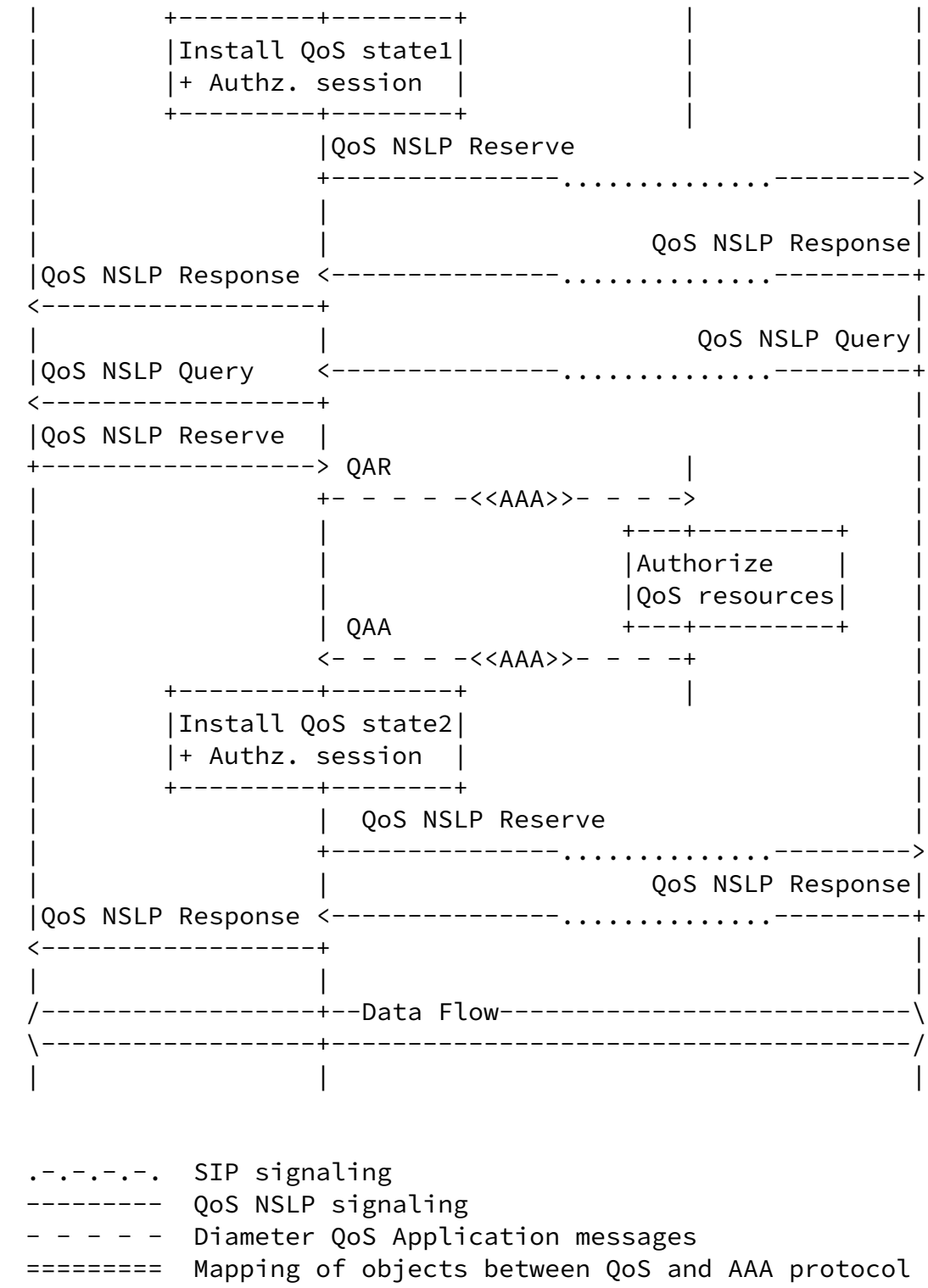


Figure 26: Example for a token-based QoS authorization

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 (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 get 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 our 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-Authentication AVP and the description of the QoS resources is included into QoS-Authorized-Resources AVP. In addition, the NE rates the requested QoS resources and announces the charging rate into the Cost-Information AVP. These AVPs are included into a QoS Authorization Request message, which is sent to the Authorizing entity.

A Diameter 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-Authorized-Resources AVP), as well as duration of the authorization session (Authorization-Lifetime AVP) and duration of the time (CC-Time) for which the end-user should be charged with the rate announced in the QAR message. 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.

If the data communication might be necessary in both directions, from Host A to Host B and vice versa, a separate QoS signaling

communication is required for the reverse direction (with path-coupled signaling). This message exchange is not shown in this example.

9. Security Considerations

This document describes a mechanism for performing authorization of a QoS reservation at a third party entity. Therefore, it is necessary 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 ([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. 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].

10. Acknowledgements

The authors would like to thank John Loughney and Allison Mankin for their input to this document.

11. Open Issues

Open issues related to this draft are listed at the issue tracker available at: http://www.tschofenig.com:8080/diameter-qos/

12. References

12.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

12.2. Informative References

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

[I-D.ietf-nsis-ntlp]
Schulzrinne, H. and R. Hancock, "GIMPS: General Internet Messaging Protocol for Signaling", draft-ietf-nsis-ntlp-07 (work in progress), July 2005.

[I-D.ietf-nsis-qos-nslp]
Bosch, S., "NSLP for Quality-of-Service signalling", draft-ietf-nsis-qos-nslp-07 (work in progress), July 2005.

[I-D.ietf-nsis-qspec]
Ash, J., "QoS-NSLP QSPEC Template", draft-ietf-nsis-qspec-05 (work in progress), July 2005.

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

[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.

[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.

[I-D.tschofenig-sip-saml]
Tschofenig, H., "Using SAML for SIP", draft-tschofenig-sip-saml-04 (work in progress), July 2005.

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

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

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

[RFC2753] Yavatkar, R., Pendarakis, D., and R. Guerin, "A Framework for Policy-based Admission Control", RFC 2753, January 2000.

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

[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.

[RFC4005] Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter Network Access Server Application", RFC 4005, August 2005.

[RFC4006] Hakala, H., Mattila, L., Koskinen, J-P., Stura, M., and J. Loughney, "Diameter Credit-Control Application", RFC 4006, August 2005.

[RFC4027] Josefsson, S., "Domain Name System Media Types", RFC 4027, April 2005.

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, Bavaria 81739
Germany

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

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

Email: tseno.tsenov@mytum.de

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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