Authentication, Authorization and Accounting
Internet Draft
Document: draft-alfano-aaa-qosreq-01.txt
Expires: April 2004

Frank M. Alfano
Peter J. McCann
Tom Towle
Richard Ejzak
Lucent Technologies
Hannes Tschofenig
Siemens
October 2003

Requirements for a QoS AAA Protocol

Status of this Memo

Abstract

This document describes requirements for a protocol that would perform Authentication, Authorization, and Accounting for Quality-of-Service reservations. Such a protocol would be used by entities to authenticate a user's reservation request, to ensure that the reservation is authorized and to provide accounting functionality.

The requirements covered in this document primarily address the communication of AAA protocols and not the QoS signaling protocols, although they have to provide some degree of interworking. Therefore, we list a minimal set of requirements on supported QoS signaling protocols.

Table of Contents

1. Introduction

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

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

1.1 QoS Signaling

A variety of protocols can be used to signal QoS information and to make a reservation, such as RSVP, NSIS, SIP/SDP or link-layer specific mechanisms.

RSVP [2] is the existing IETF-defined QoS signaling protocol. The Next Steps in Signaling (NSIS) working group [3] is currently developing a general signaling model based on two-layer architecture.

In the meantime, deployments such as 3rd generation cellular networks are defining their own reservation procedures: these include link-layer specific means, such as the PDP Context Activation procedures of 3GPP [4,5] or the service instance establishment procedures of 3GPP2 [6]. This list can easily be extended.

In other areas QoS signaling mechanisms are often tightly coupled to the application signaling. In the 3GPP/3GPP2 IP Multimedia Core Network subsystems the Session Initiation Protocol (SIP) [7] and Session Description Protocol (SDP) [8] are essentially being used to request resource reservations from the network. Special purpose protocols are used for communication between the SIP servers and network elements.

1.2 Architecture

This draft describes requirements on a AAA protocol for QoS reservations stemming from the new (primarily wireless) network deployments in light of recent efforts to revisit QoS signaling within the IETF. The goal is to meet these requirements of network operators while at the same time supporting a variety of QoS signaling protocols and avoiding the need for monolithic, vertically integrated applications (such as e.g., a SIP proxy server in every router). A high-level picture of the resulting architecture is shown in Figure 1.

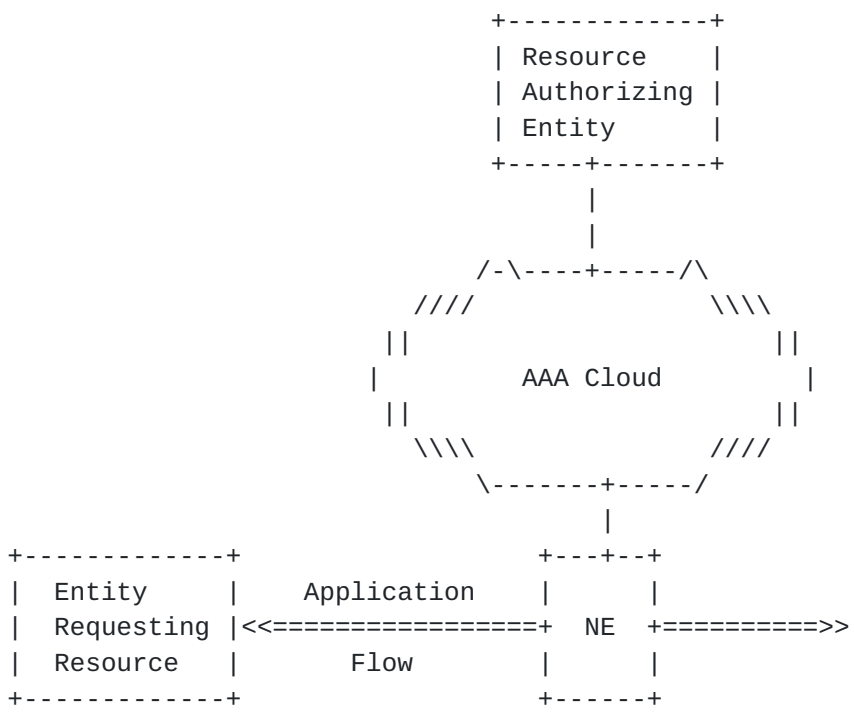

Figure 1: Architecture

Figure 1 depicts an entity requesting a resource, a network element (NE) through which application flows need to pass (i.e., an entity which enforces the QoS reservation), a cloud of AAA servers and an entity authorizing the QoS request. In many cases, the authentication terminates at the user's home network where a database containing subscriber records is located. This is often the entity that executes the authorization decision. Finally, there might be an interaction with an application signaling protocol.

Note that the entity authorizing the QoS reservation request might be a AAA server, an application server or another entity. These entities are collectively referred as the "Resource Authorizing Entity" in Figure 1.

The term "AAA Cloud" is used to refer to the network of AAA proxies and brokers. Furthermore, there might be more than one network element that needs to interact with the AAA infrastructure although Figure 1 depicts only one for clarity. Similarly, a given user might support different authentication methods; he might have more than one home network; or, he might use different means of authorization.

The remainder of this document is organized as follows:

Section 3 defines some terms that are used in subsequent discussion.

Section 4 describes some generic requirements for a QoS signaling protocol.
Section 5 gives generic requirements for a QoS AAA protocol.
Section 6 gives requirements specific to Authentication.
Section 7 gives requirements specific to Authorization.
Section 8 gives requirements specific to Accounting.
Section 9 discusses the relationship of a QoS AAA protocol to other AAA applications.
Section 10 gives an example use scenario.
Finally, Section 11 outlines some security considerations.

2. Keywords

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 [9].

3. Terminology

Accounting Rules
An accounting rule is a collection of data that identifies one or more IP flows and provides related information. An accounting rule defines the accounting treatment such as on-line (i.e., pre-paid) or off-line accounting. The data may also identify, for example, volume or time based accounting, rating information, termination actions for on-line accounting (e.g., drop or re-route packets), record correlation identifiers, etc.

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. This may be a AAA server (with a subscriber database) or an application server or some other entity.

Network Element

A network element is a network entity such as an IP router on the path between two endpoints, through which IP packets belonging to application flows pass. Typically only a small subset of the network elements along a path communicates with the AAA infrastructure for the purpose of QoS authorization. In a typical service provider scenario, the first-hop router will be required to play this role. A motivation of this architectural simplification is referred to as the New Jersey Turnpike Model and is described in detail in Section 4 of [11]. Network elements are responsible for enforcing the result of the authorization process.

Subscriber Database

A Subscriber Database holds information related to network users such as information about their subscribed service. A user might, for example, have a subscription for a 'gold' service that authorizes him for higher QoS parameters than 'normal' users.

Termination Actions

On-line accounting allows the on-line accounting authorization entity to terminate flows in real time. A termination action defines the action to be taken by the network element for the case where a flow has been terminated. For example flow packets might be dropped, might be redirected, or might be allowed to continue but not be counted.

QoS signaling protocol

A protocol used to carry QoS information between two end points and intercepted by entities along the path. The QoS signaling protocols discussed in this context follow the data path (i.e., they are path-coupled).

QoS AAA protocol

The QoS AAA protocol runs between a network element (acting as a AAA client) and the resource authorizing entity (acting as a AAA server). For example, upon receipt of a QoS request from the resource requesting entity, the network element might copy authentication credentials and QoS flow information into a AAA message which is forwarded to the resource authorizing entity, possibly via one or more proxy AAA servers. The authorizing entity returns an authorization decision (yes/no) for the flow, and accounting data would be sent to the authorizing entity while the flow is active.

4. Generic Requirements on a QoS Signaling Protocol

While the details of a particular QoS signaling protocol are outside the scope of this document, we do list here some generic requirements that any QoS signaling protocol must meet in order to act as a front end for a QoS AAA protocol.

4.1 Identification of Resource Authorizing Entity

The QoS signaling protocol MUST carry information sufficient to identify the resource authorizing entity. Note that the network element and the resource authorizing entity will often be in different administrative domains.

4.2 User Authentication/Authorization

The QoS signaling protocol MUST carry information to allow the authorizing entity to compute the authorization decision. In most cases this information will allow the authorizing entity to authenticate the user. Note that authentication is not necessarily required since authorization can also be accomplished for an anonymous user.

Section 5.7.1 of [13] points to these requirements for the NSIS area. RSVP extended the admission control procedure by adding user authentication as described in [14]. Additional authorization capability has been added with the help of authorization tokens as described in [15] and [16].

It is important to provide cryptographic authentication or to protect the authorization information (e.g., tokens) appropriately to counter identity spoofing and attacks against the authorization information (e.g., replay attacks). These attacks might lead to fraud as described in [17].

4.3 Support for different authorization scenarios

[11] and [12] describe a two and a three party approach for computing the authorization decision. The QoS signaling protocol SHOULD support these general authorization scenarios. This wide range of authorization scenarios is required to make the QoS AAA protocol applicable in all deployment environments.

4.4 Providing Authorization Information

The QoS signaling protocol MUST carry sufficient information between the authorizing entity and the enforcing entity (and vice versa) to compute an authorization decision and to execute it.

This information might include flow identification, QoS objects for determining the authorization (in the direction to the authorizing entity) as well as for provisioning (in the direction from the authorizing entity to the enforcing entity) and price information. Flow information can be used for determining the authorization decision in those case where it meaningful.

In many cases it MUST be possible to determine the price of the QoS reservation and to communicate the price to the user (or at least to provide sufficient information to allow the user to compute the price). As described in [11] one or both end-points may need to know the price information.

4.5 Reauthorization

The QoS signaling protocol MUST allow the network to trigger a reauthorization procedure at any time to support periodic and event triggered authorization.

4.6 Integrity and Replay Protection

The QoS signaling protocol MUST be integrity and replay protected.

To support this requirement each signaling message would, for example, carry a keyed message digest to ensure that only valid requests are granted by the network. This is especially important when a user is being held responsible for charges associated with a QoS session. Prior to providing integrity and replay protection it is necessary to dynamically establish session keys. This is particularly important in a mobile environment as described in Section 7 of [11].

Integrity and replay protection is required for NSIS as described in [17] (see Section 4.2 and 4.3 of [17]).

4.7 Confidentiality Protection

The QoS signaling protocol MUST provide confidentiality protection in those cases where authorization information is vulnerable to replay attacks. As an example, single-use authorization tokens may rely on the use of a secure channel. An adversary who is able to eavesdrop authorization tokens might be able to reuse them. They only provide a proof of possession and do not serve the purpose of cryptographic authentication where a liveness guarantee has to be provided by the parties executing the protocol.

5. Generic Requirements on a QoS AAA Protocol

In this section we list some high-level requirements that must be met by a QoS AAA protocol.

5.1 Inter-domain Support

The QoS AAA protocol MUST support inter-domain operation. 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. This implies the existence of a roaming agreement between the two networks. In general, one or both end-points involved in a communication may be roaming, meaning that the network elements along the data path may belong to multiple administrative domains, none of which are the home domain of either end-point.

5.2 Identity-based Routing

The QoS AAA protocol MUST route AAA requests to the authorizing entity based on the identity information given in the QoS signaling protocol.

6. Requirements for QoS Authentication

In this section we list some QoS AAA requirements specific to authentication and authorization.

6.1 Flexible Authentication Support

The QoS AAA protocol MUST support verification of authentication information present in QoS signaling messages. The QoS AAA protocol MUST support a variety of different authentication protocols. Different QoS architectures are likely to have a different security infrastructure with different requirements.

The PacketCable architecture, for example, heavily utilizes Kerberos whereas the 3GPP architecture makes use of the UMTS AKA algorithm.

7. Requirements for QoS Authorization

In this section we list some QoS AAA requirements specific to authorization.

7.1 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.

This information might include flow identification, QoS objects for determining the authorization as well as for provisioning and price information.

The flow identification provided to the QoS AAA protocol MUST allow flow information to be under-specified ("wild carded"). This might be the case for aggregates and when endpoints are unknown at the time of initial resource authorization.

7.2 Triggering an Authorization Process

The QoS AAA protocol MUST allow periodic and event triggered execution of the authorization process.

The trigger for re-authorization might be originated at the enforcing entity or even at the authorizing entity. In any case it should be possible to carry information with the QoS AAA protocol to allow the enforcing or some other trusted entity to determine when to trigger authorization. For example, a time-based trigger, a volume-based trigger or even triggers based on consumed financial resources might lead to a reauthorization procedure.

7.3 Associating QoS Reservations and Application State

The QoS AAA protocol MUST carry information sufficient for an application server to identify the appropriate application session. This allows an application session to be associated with a particular QoS reservation.

Note that if flow information is sufficient to identify an application session then no separate identifier is required. Although this is not true for NSIS other QoS signaling protocols use different identifiers.

7.4 Dynamic Authorization

The QoS AAA protocol MUST support dynamic authorization; that is, it MUST be possible to push updates towards the network element(s) from authorizing entities.

This requirement would support runtime application state transitions or even a change in the subscriberÆs profile that would lead to a different authorization state for a specific QoS reservation.

7.5 Bearer Gating

The QoS AAA protocol MUST allow the authorizing entity to gate authorized application flows.

Even though a user might received an authorization for a given flow, some applications may want to toggle the flow on or off based on application state transitions. This control is called bearer gating. Unlike revocation functionality, gating leaves state information about the QoS reservation in place and it is only temporarily suspended.

8. Requirements for QoS Accounting

In this section we list some QoS AAA requirements specific to accounting.

8.1 Accounting Records

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

8.2 Accounting Rules

The QoS AAA protocol MUST allow the authorizing entity to transfer accounting rules that are applicable to specific flows. These rules would define the on-line ("pre-paid") versus off-line ("post-paid") nature of the accounting as well as convey other associated parameters such as record identifiers, rating information, usage quota, on-line termination actions, etc.

The QoS AAA protocol MUST allow for accounting rules to be provided at authorization time as well as to be pushed later as dynamic updates.

8.3 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.

8.4 Failure Notification

The QoS AAA protocol MUST allow the network element to report failures to the authorizing entity. These failures (such as loss of connectivity due to movement of a mobile node or other reasons for packet loss) primarily address problems in the data path and do not cover problems with the QoS AAA protocol.

8.5 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.

For example, an application server might create and pass an accounting correlation identifier to the network element. This correlation identifier would then be stored for inclusion in subsequent accounting records. This would allow the home network to link the accounting information of the network element with those of the application server.

9. Interaction with other AAA Applications

It is likely that an endpoint attached to a first-hop network element was authenticated and authorized for basic, best-effort Internet access prior to requesting any special QoS from the network. If the subscriber database for basic network access is the same as the one containing a QoS subscription, it may be expeditious to define some interactions between the AAA protocol used for basic access (e.g., NASREQ [10]) and the one outlined here for QoS. For example, it may be useful to return some QoS-related attributes to the first-hop network element at the time the endpoint is granted basic, best-effort access. This would allow for some future QoS requests to be granted based on the cached profile, rather than requiring a round-trip to the home subscriber database. This gives rise to the following requirement:

The QoS AAA protocol MUST define a QoS profile that can be re-used in other AAA applications.

Still, it must be possible to execute the QoS AAA protocol independently of other AAA protocols applications.

Also, it may be useful to allow application servers to push QoS authorization information to a network element prior to any explicit request from the endpoint. This could support application endpoints that do not support an explicit QoS signaling mechanism. In this case, the authorization may be pushed via the home AAA server, which presumably knows to which NAS the endpoint is currently attached. Alternatively, the QoS AAA protocol may define some sort of redirection facility that would allow application servers to send AAA messages directly to selected network elements such as a NAS. This operation could be considered a special case of dynamic authorization where no explicit request for QoS was made prior to the authorization:

The QoS AAA protocol MUST support dynamic authorization initiated by the authorizing entity.

10. Scenarios

This section provides a few example scenarios:

An application in a mobile node wants to open a video session with a video server. The mobile node and the video server negotiate the resources to be used for the session and for which the application will be financially responsible. When resource negotiation has completed, the video server stores the resource information and assigns a session identifier to the information that can be used as the primary key for later information queries. This identifier has to be known to both parties - the mobile node and the video server.

The mobile node starts to use a QoS signaling protocol. The signaling message will hit a network element (most likely the first hop router) in the visited network. The video server and the network element will verify that the mobile node has not requested more resources than what were negotiated and for which the application has agreed to be financially responsible. To link the application protocol session with this particular resource request, the mobile node passes the session identifier received from the video server to the network element via the QoS signaling protocol. The network element makes a request to the video server (or some other centralized node) as identified in the session identifier. The video server passes the relevant QoS state information to the network element in an answer message, associating the origin host information from the request with the state information stored by the video server. (This can then be used later for pushing information to the network element.) All accounting messages from a network entity include an accounting correlation id.

10.1 Bearer Gating

The video server can control the flow of packets on the network element by sending packet flow gating information in the answer message delivered for resource authorization. If the flow of packets is not immediately enabled, some event at the video server will trigger the server to enable the flow. The video server sends a request containing flow gating information to the network element to allow the flow of packets. The network element returns the state of the packet flow in the response message to the video server.

10.2 Loss of Connectivity

The network element determines connectivity to the end host has been lost. The video server needs this information in order to take corrective action, charge appropriately, and/or release resources associated with the session. The network element informs the video server of the loss of connectivity in a request message containing state information of the network element. The video server acknowledges the request in an answer message. The video server may then issue a session abort request message to other network functional entities.

11. Security Considerations

The QoS AAA protocol whose requirements are given in this draft assumes that a trust relationship exists between the authorizing entity and the network element. This trust relationship does not need to be pre-existing at the protocol startup but could also be dynamically established. The relationship may be direct or it may be indirect via a AAA cloud consisting of brokers and proxies. Each link in this chain of relationships MUST be secured to prevent spoofed authorizations.

This relationship implies that the bearer element should grant service based on the decision of the authorizing entity, presumably because the used resources will be paid for. The establishment of a trust relationship between the involved networks therefore also implies the setup of a financial settlement.

The authentication outlined in Section 6 MUST be cryptographically strong and protected against replay and other attacks. Various threats against a QoS signaling protocol (and on the AAA infrastructure) are described in [17].

Once QoS resources have been authorized, it may be possible for an unauthorized party to subvert them for its own use. Steps MUST be taken to prevent an adversary from injecting or spoofing data packets, which could then receive preferred treatment (i.e., steal

other user's QoS resources). Although beyond the scope of this document cryptographic protection of the data traffic should be considered either at the network or at the link layer.

Among other things, Section 9 implies to off-load some authorization decisions from the user's home network to the visted network. Making the user's profile available to entities outside the home network might raise some privacy concerns.

12. Reference

[1] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

[2] Braden, R., Zhang, L., Berson, S., Herzog, S., Jamin, S., "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, September 1997.

[3] Hancock, R., Freytsis, I., Karagiannis, G., Loughney, J., and Van den Bosch, S., "Next Steps in Signaling: Framework", Internet Draft, Internet Engineering Task Force, September 2003. Work in progress.

[4] 3GPP TS 29.208, "End-to-end Quality of Service (QoS) Signaling Flows", April 2003.

[5] 3GPP TS 29.207, "Policy control over Go interface", March 2003.

[6] 3GPP2 C.S0017-0 (also TIA IS-707-A), "Data Service Options for Spread Spectrum Systems."

[7] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and Schooler, E., "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[8] Handley, M., Jacobson, V., Perkins, C., "SDP: Session Description Protocol", Internet Draft, Internet Engineering Task Force, September 2003. Work In Progress.

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

[10] Calhoun, P., Zorn, G., Spence, D., Mitton, D., "Diameter Network Access Server Application", Internet Draft, Internet Engineering Task Force, October, 2003. Work In Progress.

[11] H. Tschofenig, M. Buechli, S. Van den Bosch and H. Schulzrinne: "NSIS Authentication, Authorization and Accounting Issues",

Internet Draft, Internet Engineering Task Force, March 2003. Work in progress.

[12] H. Tschofenig, M. Buechli, S. Van den Bosch, H. Schulzrinne and T. Chen: "QoS NSLP Authorization Issues", Internet Draft, Internet Engineering Task Force, June 2003. Work in progress.

[13] M. Brunner: "Requirements for QoS signaling protocols", Internet Draft, Internet Engineering Task Force, August 2003. Work in progress.

[14] Yadav, S., Yavatkar, R., Pabbati, R., Ford, P., Moore, T., Herzog, S., Hess, R.: "Identity Representation for RSVP", RFC 3182, October, 2001.

[15] L. Hamer, B. Gage, and H. Shieh: "Framework for session set-up with media authorization," RFC 3521, Internet Engineering Task Force, April 2003.

[16] L. Hamer, B. Gage, B. Kosinski, and H. Shieh: "Session Authorization Policy Element", RFC 3520, Internet Engineering Task Force, April 2003.

[17] Tschofenig, H. and D. Kroeselberg: "Security Threats for NSIS", Internet Draft, Internet Engineering Task Force, June 2003.

13. Author's Addresses

Frank M. Alfano
Lucent Technologies
Rm 9C-226L
1960 Lucent Lane
Naperville, IL 60563
Phone: +1 630 979 7209
Email: falfano@lucent.com

Peter J. McCann
Lucent Technologies
Rm 9C-226R
1960 Lucent Lane
Naperville, IL 60563
Phone: +1 630 713 9359
Email: mccap@lucent.com

Thomas T. Towle
Lucent Technologies
Rm 9C-229
1960 Lucent Lane
Naperville, IL 60563
Phone: +1 630 979 7303
Email: ttowle@lucent.com

Richard Ejzak
Lucent Technologies
Rm 7H-245
1960 Lucent Lane
Naperville, IL 60563
Phone: +1 630 979 7036
Email: ejzak@lucent.com

Hannes Tschofenig
Siemens AG
Otto-Hahn-Ring 6
81739 Munich
Germany
EMail: Hannes.Tschofenig@siemens.com

Intellectual Property Statement

Full Copyright Statement