Framework for session set-up with media authorization

Status of this Memo

   This document is an Internet-Draft and is in full conformance with
   all provisions of Section 10 of RFC2026 [1].

   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

   The distribution of this memo is unlimited. This memo is filed as
   <draft-ietf-rap-session-auth-00.txt>, and expires September 31, 2001.
   Please send comments to the authors.

Abstract

   Establishing multimedia streams must take into account requirements
   for end-to-end QoS, authorization of network resource usage and
   accurate accounting for resources used. During session set up,
   policies may be enforced to ensure that the media streams being
   requested lie within the bounds of the service profile established
   for the requesting host. Similarly, when a host requests resources
   to provide a certain QoS for a packet flow, policies may be enforced
   to ensure that the required resources lie within the bounds of the
   resource profile established for the requesting host.

   To prevent fraud and to ensure accurate billing, we describe various
   scenarios and mechanisms that provide the linkage required to verify
   that the resources being used to provide a requested QoS are in-line
   with the media streams requested (and authorized) for the session.

Contents

1. **Introduction**

   Establishing multimedia streams must take into account requirements
   for end-to-end QoS, authorization of network resource usage and
   accurate accounting for resources used. During session set up,
   policies may be enforced to ensure that the media streams being
   requested lie within the bounds of the service profile established
   for the requesting host. Similarly, when a host requests resources
   to provide a certain QoS for a packet flow, policies may be enforced
   to ensure that the required resources lie within the bounds of the
   resource profile established for the requesting host.

   Reference [5] defines a mechanism through which end hosts can use a
   session control protocol (SIP) to indicate that QoS requirements
   must be met in order to successfully set up a session. However, a
   separate protocol (e.g. RSVP) is used to request the resources
   required to meet the end-to-end QoS of the media stream. To prevent
   fraud and to ensure accurate billing, some linkage is required to
   verify that the resources being used to provide the requested QoS
   are in-line with the media streams requested (and authorized) for
   the session.

   This document describes such a linkage through use of a "token" that
   provides capabilities similar to that of a gate in [8] and of a
   ticket in the push model of [2]. The token is generated by a policy
   server (or a session manager) and is transparently relayed through
   the end host to the edge router where it is used as part of the
   policy-controlled flow admission process.

   In some environments, authorization of media streams can exploit the
   fact that pre-established relationships exist between elements of
   the network (e.g. session managers, edge routers, policy servers and
   end hosts). In other environments, however, such pre-established
   relationships may not exist either due to the complexity of creating
   these associations a priori (e.g. in a network with many elements),
   or due to the different business entities involved (e.g. service
   provider and access provider), or due to the dynamic nature of these
   associations (e.g. in a mobile environment).

   In this document, we describe these various scenarios and the
   mechanisms used for exchanging information between network elements
   in order to authorize the use of resources for a service and to co-
   ordinate actions between the session and resource management
   entities. Specific extensions to session control protocols (e.g. SIP
   [6], H.323), to resource reservation protocols (e.g. RSVP [7],
   YESSIR) and to policy managements protocols (e.g. COPS-SIP, COPS-
   RSVP [4]) required to realize these scenarios and mechanisms are
   beyond the scope of this document.

   For clarity, this document will illustrate the media authorization
   concepts using SIP for session signalling, RSVP for resource
   reservation and COPS for interaction with the policy servers. Note,
   however, that the framework could be applied to a multimedia
   services scenario using different signalling protocols.

2. Conventions used in this document

   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 [1].

[3](#). **Definition of terms**

Figure 1 introduces a generic model for session establishment, QoS
and policy enforcement.

```
                    +--------------------------------------+   +---+
                    | SCD - Service Control District       |   |   |
                    | +----------------------+ +--------+|  | I |
                    | |Session management    | |Policy  ||  | n |
                    | |server                | |Server  ||  | t |
                    | | +---------+ +------+  | |  +----+||<->| e |
                    | | |SIP Proxy| |PEP   |<-|-|->|PDP |||  | r |
                    | | +---------+ +------+  | |  +----+||  | - |
                    | +----------------------+ +--------+|  | c |
                    |                                    |  | o |
                    +------------------------------------+  | n |
                                                            | n |
                    +------------------------------------+  | e |
                    | RCD - Resource Control District    |  | c |
                    |                                    |  | t |
                    |                                    |  | i |
                    |   +------------+    +-------------+ |  | n |
      +----------+  |   |Edge Router |    |Policy Server| |  | g |
      | End      |  |   |            |    |             | |  |   |
      | Host     |  |   |+----------+|    |+----------+ | |  | N |
      |+--------+|  |   ||RSVP Agent||    ||PDP       | | |  | e |
      ||RSVP    ||<->|   |+----------+|<-->|+----------+ | |<->| t |
      ||Client  ||  |   |+----------+|    |             | |  | w |
      |+--------+|  |   || PEP      ||    |             | |  | o |
      ||SIP User||  |   |+----------+|    |             | |  | r |
      ||Agent   ||  |   +------------+    +-------------+ |  | k |
      |+--------+|  |                                    |  |   |
      +----------+  +------------------------------------+  +---+
```
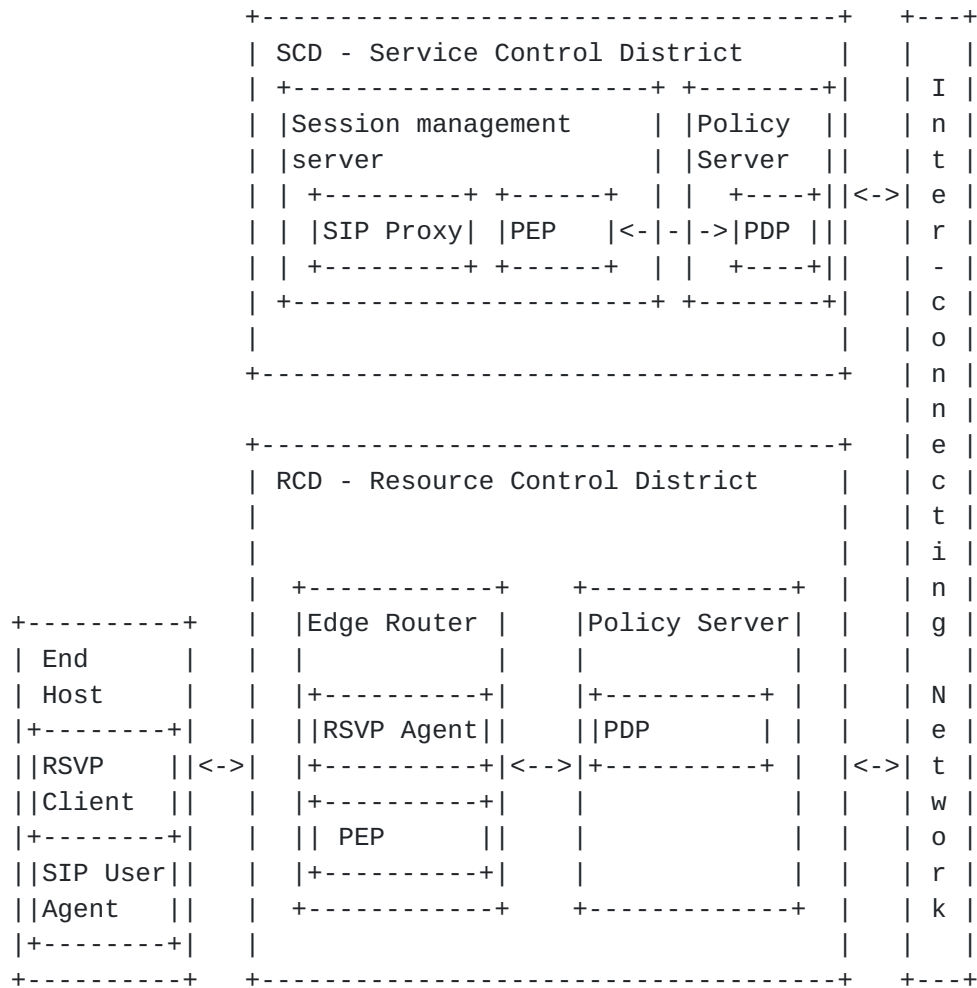
Figure 1: Generic media authorization network model

EH - End Host: The End Host is a device used by a subscriber to
access network services. The End Host includes a client for
requesting network services (e.g. through SIP) and a client for
requesting network resources (e.g. through RSVP).

ER - Edge Router: The Edge Router is a network element connecting
the end host to the rest of the Resource Control District. The Edge
Router contains a PEP to enforce policies related to resource usage
in the Resource Control District by the End Host. It also contains a

signalling agent (e.g. for RSVP) for handling resource reservation
requests from the End Host.

   PDP - Policy Decision Point: The PDP is a logical entity located in
   the Policy Server that is responsible for authorizing or denying
   access to services and/or resources.

   PEP - Policy Enforcement Point: The PEP is a logical entity that
   enforces policy decisions made by the PDP. Note that other PEPs may
   reside in other network elements not shown in the model of Figure 1,
   however they will not be discussed in this document.

   PS - Policy Server: The Policy Server is a network element that
   includes a PDP. Note that there may be a PS in the Service Control
   District to control use of services and there may be a separate PS
   in the Resource Control District to control use of resources along
   the packet forwarding path. Note also that network topology may
   require multiple Policy Servers within either district, however they
   provide consistent policy decisions to offer the appearance of a
   single PDP in each district.

   RCD - Resource Control District: The Resource Control District is a
   logical grouping of elements that provide connectivity along the
   packet forwarding paths to and from an End Host. The RCD contains ER
   and PS entities whose responsibilities include management of
   resources along the packet forwarding paths.

   SCD - Service Control District: The Service Control District is a
   logical grouping of elements that offer applications and content to
   subscribers of their services. The Session Management Server resides
   in the SCD along with a PS.

   SMS - Session Management Server: The Session Management Server is a
   network element providing session management services (e.g.
   telephony call control). The Session Management Server contains a
   PEP to enforce policies related to use of services by the End Host.
   It also contains a signalling agent or proxy (e.g. for SIP) for
   handling service requests from the End Host.

4. The Coupled Model

   In some environments, a pre-established trust relationship exists
   between elements of the network (e.g. session managers, edge
   routers, policy servers and end hosts). We refer to this as the
   "coupled model", indicating the tight relationship between entities
   that is presumed. The key aspects of this scenario are the
   following:

   - Policy decisions, including media authorization, are made by a
      single Policy Server.

   - The Edge Router, Session Manager and Policy Server involved in
      establishing the session are known a priori. For example, the End
      Host may be configured to use a Session Manager associated with
      the Edge Router to which the EH is connected.

   - There are pre-defined trust relationships between the SMS and the
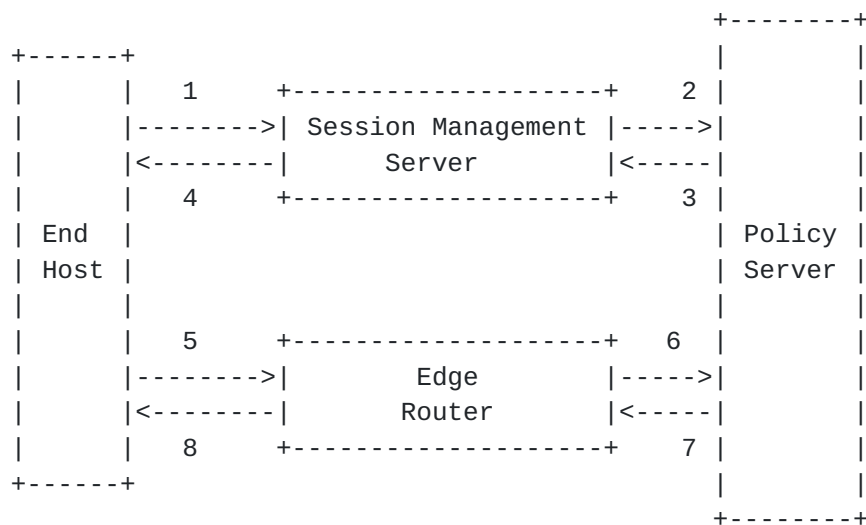   PS and between the ER and the PS.

```
                                            +--------+
    +------+                                |        |
    |      |    1     +-------------------+    2 |        |
    |      |-------->| Session Management |----->|        |
    |      |<--------|      Server        |<-----|        |
    |      |    4     +-------------------+    3 |        |
    | End  |                                | Policy |
    | Host |                                | Server |
    |      |                                |        |
    |      |    5     +-------------------+    6 |        |
    |      |-------->|       Edge         |----->|        |
    |      |<--------|       Router       |<-----|        |
    |      |    8     +-------------------+    7 |        |
    +------+                                |        |
                                            +--------+
```

   Figure 2: The Coupled Model

4.1   Coupled Model Message Flows

   In this model, it is assumed that there is one Policy Server serving
   both the Service Control and Resource Control districts and that
   there are pre-defined trust relationships between the PS and SMS and
   between the PS and ER. Communications between these entities are
   then possible as described below:

  1. The End Host issues a session set-up request (e.g. SIP INVITE) to
     the Session Manager indicating, among other things, the media
     streams to be used in the session. As part of this step, the End
     Host may authenticate itself to the Session Manager.

  2. The Session Manager, possibly after waiting for negotiation of
     the media streams to be completed, sends a policy decision
     request (e.g. COPS-SIP REQ) to the Policy Server in order to
     determine if the session set-up request should be allowed to
     proceed.

  3. The Policy Server sends a decision (e.g. COPS-SIP DEC) to the
     Session Manager, possibly after modifying the parameters of the
     media to be used. Included in this response is a "token" that can
     subsequently be used by the Policy Server to identify the session
     and the media it has authorized.

  4. The Session Manager sends a response to the End Host (e.g. SIP
     200 or 183) indicating that session set-up is complete or is
     progressing. Included in this response is a description of the
     negotiated media along with the token from the Policy Server.

  5. The End Host issues a request (e.g. RSVP PATH) to reserve the
     resources necessary to provide the required QoS for the media
     stream. Included in this request is the token from the Policy
     Server provided via the Session Manager.

  6. The Edge Router intercepts the reservation request and sends a
     policy decision request (e.g. COPS-RSVP REQ) to the Policy Server
     in order to determine if the resource reservation request should
     be allowed to proceed. Included in this request is the token from
     the Policy Server provided by the End Host. The Policy Server
     uses this token to correlate the request for resources with the
     media authorization previously provided to the Session Manager.

  7. The Policy Server sends a decision (e.g. COPS-RSVP DEC) to the
     Edge Router, possibly after modifying the parameters of the
     resources to be reserved.

  8. The Edge Router, possibly after waiting for end-to-end
     negotiation for resources to be completed, sends a response to
     the End Host (e.g. RSVP RESV) indicating that resource
     reservation is complete or is progressing.

4.2 **Coupled Model Authorization Token**

   In the Coupled Model, the Policy Server is the only network entity
   that needs to interpret the contents of the token. Therefore, in
   this model, the contents of the token are implementation dependent.
   Since the End Host is assumed to be untrusted, the Policy Server
   should take measures to ensure that the integrity of the token is
   preserved in transit; the exact mechanisms to be used are also
   implementation dependent.

4.3 **Coupled Model Protocol Impacts**

   The use of a media authorization token in the Coupled Model requires
   the addition of new fields to several protocols:

   - Resource reservation protocol. A new protocol field or object
     must be added to the resource reservation protocol to
     transparently transport the token from the End Host to the Edge
     Router. The content and internal structure (if any) of this
     object should be opaque to the resource reservation protocol.

   - Policy management protocol. A new protocol field or object must
     be added to the policy management protocol to transparently
     transport the token from the Policy Server to the Session
     Management Server and from the Edge Router to the Policy Server.
     The content and internal structure (if any) of this object should
     be opaque to the policy management protocol.

   - Session management protocol. A new protocol field or object must
     be added to the session management protocol to transparently
     transport the media authorization token from the Session
     Management Server to the End Host. The content and internal
     structure (if any) of this object should be opaque to the session
     management protocol.

5. The Associated Model <<using One Policy Server>>

   In this scenario, there are multiple instances of the Session
   Management Servers, Edge Routers and Policy Servers. This leads to a
   network of sufficient complexity that it precludes distributing
   knowledge of network topology to all network entities. The key
   aspects of this scenario are the following:

   - Policy decisions, including media authorization, are made by a
      the same Policy Server for both the Session Manager and the Edge
      Router. Basically, the SCD and RCD outsource policy decisions to
      the same policy server. However, the Policy Server may change on
      per-transaction basis.

   - The Edge Router, Session Manager and Policy Server involved in
      establishing the session are not known a priori. For example, the
      End Host may be dynamically configured to use one of a pool of
      Session Managers and each of the Session Managers may be
      statically configured to use one of a pool of Policy Servers.

      In another example, the End Host may be mobile and continually
      changing the Edge Router that its point of attachment uses to
      communicate with the rest of the network.

   - There are pre-defined trust relationships between the SMS and the
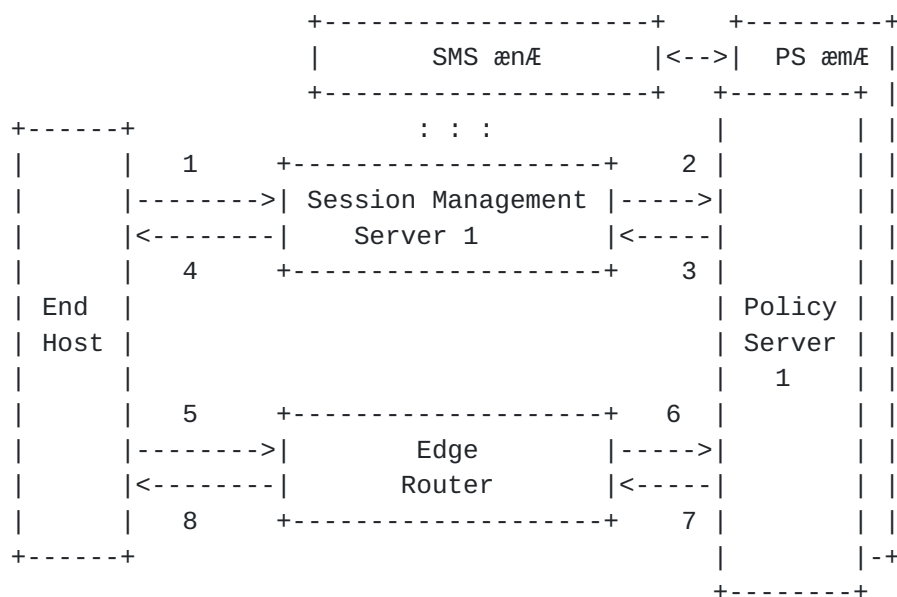   PS and between the ER and the PS.

```
                        +---------------------+    +---------+
                        |      SMS ænÆ         |<-->|  PS æmÆ |
                        +---------------------+    +--------+ |
    +------+                  : : :                    |      | |
    |      |    1     +-------------------+    2 |      | |
    |      |--------->| Session Management |----->|      | |
    |      |<---------|     Server 1       |<-----|      | |
    |      |    4     +-------------------+    3 |      | |
    | End  |                                    | Policy | |
    | Host |                                    | Server | |
    |      |                                    |   1    | |
    |      |    5     +-------------------+    6 |      | |
    |      |--------->|       Edge         |----->|      | |
    |      |<---------|      Router        |<-----|      | |
    |      |    8     +-------------------+    7 |      | |
    +------+                                     |      |-+
                                                 +--------+
```

   Figure 3: The Associated Model using One Policy Server

5.1   **Associated Model Message Flows <<using One Policy Server>>**

   In this model, it is assumed that a Policy Server can make decisions
   for both the Service Control and Resource Control districts and that
   there are pre-defined trust relationships between the PS and SMS and
   between the PS and ER. Communications between these entities are
   then possible as described below:

   1. The End Host issues a session set-up request (e.g. SIP INVITE) to
      the Session Manager indicating, among other things, the media
      streams to be used in the session. As part of this step, the End
      Host may authenticate itself to the Session Manager.

   2. The Session Manager, possibly after waiting for negotiation of
      the media streams to be completed, sends a policy decision
      request (e.g. COPS-SIP REQ) to the Policy Server in order to
      determine if the session set-up request should be allowed to
      proceed.

   3. The Policy Server sends a decision (e.g. COPS-SIP DEC) to the
      Session Manager, possibly after modifying the parameters of the
      media to be used. Included in this response is a "token" that can
      subsequently be used by the Policy Server to identify the session
      and the media it has authorized.

   4. The Session Manager sends a response to the End Host (e.g. SIP
      200 or 183) indicating that session set-up is complete or is
      progressing. Included in this response is a description of the
      negotiated media along with the token from the Policy Server.

   5. The End Host issues a request (e.g. RSVP PATH) to reserve the
      resources necessary to provide the required QoS for the media
      stream. Included in this request is the token from the Policy
      Server provided via the Session Manager.

   6. The Edge Router intercepts the reservation request and inspects
      the token to learn which Policy Server authorized the media. It
      then sends a policy decision request (e.g. COPS-RSVP REQ) to that
      Policy Server in order to determine if the resource reservation
      request should be allowed to proceed. Included in this request is
      the token from the Policy Server provided by the End Host. The
      Policy Server uses this token to correlate the request for
      resources with the media authorization previously provided to the
      Session Manager.

   7. The Policy Server sends a decision (e.g. COPS-RSVP DEC) to the
      Edge Router, possibly after modifying the parameters of the
      resources to be reserved.

8. The Edge Router, possibly after waiting for end-to-end
      negotiation for resources to be completed, sends a response to

      the End Host (e.g. RSVP RESV) indicating that resource
      reservation is complete or is progressing.

5.2   Associated Model Authorization Token <<using One Policy Server>>

   Since the ER does not know which SMS and PS are involved in session
   establishment, the token must include:

   - A correlation identifier. This is information that the Policy
      Server can use to correlate the resource reservation request with
      the media authorized during session set up. The Policy Server is
      the only network entity that needs to interpret the contents of
      the correlation identifier therefore, in this model, the contents
      of the correlation identifier are implementation dependent. Since
      the End Host is assumed to be untrusted, the Policy Server should
      take measures to ensure that the integrity of the correlation
      identifier is preserved in transit; the exact mechanisms to be
      used are also implementation dependent.

   - The identity of the authorizing entity. This information is used
      by the Edge Router to determine which Policy Server should be
      used to solicit resource policy decisions.

   In some environments, an Edge Router may have no means for
   determining if the identity refers to a legitimate Policy Server
   within its domain. In order to protect against redirection of
   authorization requests to a bogus authorizing entity, the token
   should also include:

   - An authentication signature. This signature is calculated over
      all other fields of the token using an agreed mechanism. The Edge
      Router must be able to verify the signature using credentials of
      the signer to confirm a trust relationship. The mechanism used by
      the Edge Router is beyond the scope of this document.

5.3   Associated Model Protocol Impacts <<using One Policy Server>>

   The use of a media authorization token in this version of the
   Associated Model requires the addition of new fields to several
   protocols:

   - Resource reservation protocol. A new protocol field or object
      must be added to the resource reservation protocol to
      transparently transport the token from the End Host to the Edge
      Router. The content and internal structure of this object must be

specified so that the Edge Router can distinguish between the
elements of the token described in [Section 5.2](#).

   - Policy management protocol. A new protocol field or object must
      be added to the policy management protocol to transparently
      transport the token -- or at least the correlation identifier --
      from the Edge Router to the Policy Server. The content and
      internal structure of this object should be opaque to the policy
      management protocol.

   - Session management protocol. A new protocol field or object must
      be added to the session management protocol to transparently
      transport the media authorization token from the Session
      Management Server to the End Host. The content and internal
      structure of this object should be opaque to the session
      management protocol.

6. The Associated Model <<using Two Policy Servers>>

   In this scenario, there are multiple instances of the Session
   Management Servers, Edge Routers and Policy Servers. This leads to a
   network of sufficient complexity that it precludes distributing
   knowledge of network topology to all network entities. The key
   aspects of this scenario are the following:

   - Policy decisions, including media authorization, are made by
      Policy Servers.

   - There is a PS in the Resource Control District that is separate
      from the PS in the Session Control District.

   - The Edge Router, Session Manager and Policy Servers involved in
      establishing the session are not known a priori. For example, the
      End Host may be dynamically configured to use one of a pool of
      Session Managers or the End Host may be mobile and continually
      changing the Edge Router that it uses to communicate with the
      rest of the network.

   - There is a pre-defined trust relationship between the SMS and the
      SCD PS.

   - There is a pre-defined trust relationship between the ER and the
      RCD PS.

   - There is a pre-defined trust relationship between the RCD and SCD
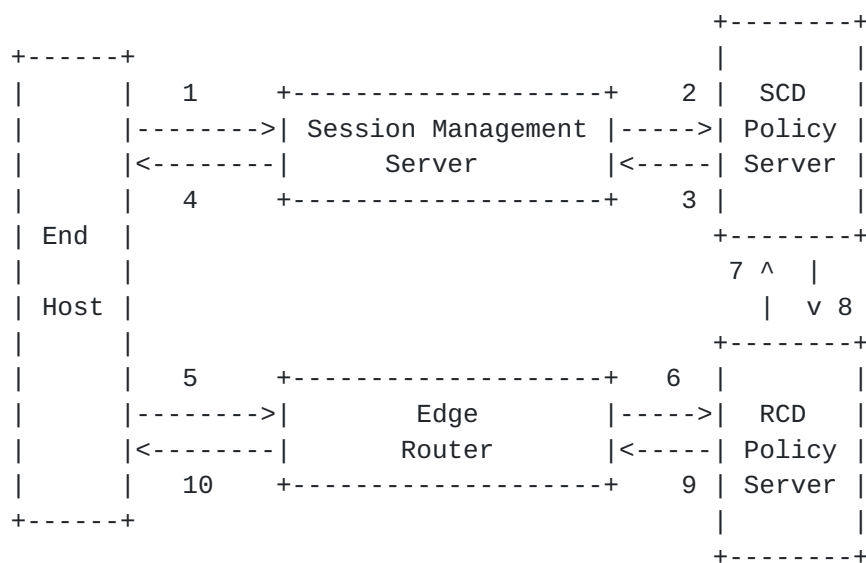   Policy Servers.


```
                                            +--------+
        +------+                            |        |
        |      |   1      +-------------------+    2 |  SCD   |
        |      |--------->| Session Management |----->| Policy |
        |      |<---------|      Server        |<-----| Server |
        |      |   4      +-------------------+    3 |        |
        | End  |                            +--------+
        |      |                              7 ^  |
        | Host |                              |  v 8
        |      |                            +--------+
        |      |   5      +-------------------+  6  |        |
        |      |--------->|        Edge        |----->|  RCD   |
        |      |<---------|       Router       |<-----| Policy |
        |      |  10      +-------------------+   9 | Server |
        +------+                            |        |
                                            +--------+
```

   Figure 4: The Associated Model using Two Policy Servers

6.1   Associated Model Message Flows <<using Two Policy Servers>>

In this model, it is assumed that there is one Policy Server for the
Service Control District and a different Policy Server for the
Resource Control District. There are pre-defined trust relationships
between the SCD PS and SMS, between the RCD PS and ER and between
the RCD and SCD Policy Servers. Communications between these
entities are then possible as described below:

1. The End Host issues a session set-up request (e.g. SIP INVITE) to
   the Session Manager indicating, among other things, the media
   streams to be used in the session. As part of this step, the End
   Host may authenticate itself to the Session Manager.

2. The Session Manager, possibly after waiting for negotiation of
   the media streams to be completed, sends a policy decision
   request (e.g. COPS-SIP REQ) to the SCD Policy Server in order to
   determine if the session set-up request should be allowed to
   proceed.

3. The SCD Policy Server sends a decision (e.g. COPS-SIP DEC) to the
   Session Manager, possibly after modifying the parameters of the
   media to be used. Included in this response is a "token" that can
   subsequently be used by the SCD Policy Server to identify the
   session and the media it has authorized.

4. The Session Manager sends a response to the End Host (e.g. SIP
   200 or 183) indicating that session set-up is complete or is
   progressing. Included in this response is a description of the
   negotiated media along with the token from the SCD Policy Server.

5. The End Host issues a request (e.g. RSVP PATH) to reserve the
   resources necessary to provide the required QoS for the media
   stream. Included in this request is the token from the SCD Policy
   Server provided via the Session Manager.

6. The Edge Router intercepts the reservation request and sends a
   policy decision request (e.g. COPS-RSVP REQ) to the RCD Policy
   Server in order to determine if the resource reservation request
   should be allowed to proceed. Included in this request is the
   token from the SCD Policy Server provided by the End Host.

7. The RCD Policy Server uses this token to learn which SCD Policy
   Server authorized the media. It then sends an authorization
   request (e.g. DIAMETER AA-Request) to that SCD Policy Server in
   order to determine if the resource reservation request should be
   allowed to proceed. Included in this request is the token from
   the SCD Policy Server provided by the End Host.

   8. The SCD Policy Server uses this token to correlate the request
      for resources with the media authorization previously provided to
      the Session Manager. The SCD Policy Server sends a decision (e.g.
      DIAMETER AA-Answer) to the RCD Policy Server on whether the
      requested resources are within the bounds authorized by the SCD
      Policy Server.

   9. The RCD Policy Server sends a decision (e.g. COPS-RSVP DEC) to
      the Edge Router, possibly after modifying the parameters of the
      resources to be reserved.

   10. The Edge Router, possibly after waiting for end-to-end
      negotiation for resources to be completed, sends a response to
      the End Host (e.g. RSVP RESV) indicating that resource
      reservation is complete or is progressing

6.2   **Associated Model Authorization Token <<using Two Policy Servers>>**

   Since the RCD Policy Server does not know which SMS and SCD PS are
   involved in session establishment, the token must include:

   - A correlation identifier. This is information that the SCD Policy
      Server can use to correlate the resource reservation request with
      the media authorized during session set up. The SCD Policy Server
      is the only network entity that needs to interpret the contents
      of the correlation identifier therefore, in this model, the
      contents of the correlation identifier are implementation
      dependent. Since the End Host is assumed to be untrusted, the SCD
      Policy Server should take measures to ensure that the integrity
      of the correlation identifier is preserved in transit; the exact
      mechanisms to be used are also implementation dependent.

   - The identity of the authorizing entity. This information is used
      by the RCD Policy Server to determine which SCD Policy Server
      should be used to verify the contents of the resource reservation
      request.

   In some environments, an RCD Policy Server may have no means for
   determining if the identity refers to a legitimate SCD Policy
   Server. In order to protect against redirection of authorization
   requests to a bogus authorizing entity, the token should include:

   - An authentication signature. This signature is calculated over
      all other fields of the token using an agreed mechanism. The RCD
      Policy Server must be able to verify the signature using
      credentials of the signer to confirm a trust relationship. The
      mechanism used by the RCD Policy Server is beyond the scope of

this document.

Note that the information in this token is the same as that in
Section 5.2 for the "One Policy Server" scenario.

6.3   Associated Model Protocol Impacts <<using Two Policy Servers>>

The use of a media authorization token in this version of the
Associated Model requires the addition of new fields to several
protocols:

- Resource reservation protocol. A new protocol field or object
   must be added to the resource reservation protocol to
   transparently transport the token from the End Host to the Edge
   Router. The content and internal structure of this object should
   be opaque to the resource reservation protocol.

- Policy management protocol. A new protocol field or object must
   be added to the policy management protocol to transport the token
   from the SCD Policy Server to the Session Management Server and
   from the Edge Router to the RCD Policy Server. The content and
   internal structure of this object must be specified so that the
   Policy Servers can distinguish between the elements of the token
   described in Section 6.2.

- Session management protocol. A new protocol field or object must
   be added to the session management protocol to transparently
   transport the media authorization token from the Session
   Management Server to the End Host. The content and internal
   structure of this object should be opaque to the session
   management protocol.

Note that these impacts are the same as those discussed in Section
5.3 for the "One Policy Server" scenario. However the use of two
Policy Servers has one additional impact:

- Authorization protocol. A new protocol field or object must be
   added to the authorization protocol to transport the token from
   the RCD Policy Server to the SCD Policy Server. The content and
   internal structure of this object must be specified so that the
   Policy Servers can distinguish between the elements of the token
   described in Section 6.2.

[7](#). The Non-Associated Model

   In this scenario, the Session Management Servers and Edge Routers
   are associated with different Policy Servers, the network entities
   do not have a priori knowledge of the topology of the network and
   there are no pre-established trust relationships between entities in
   the Resource Control District and entities in the Service Control
   District. The keys aspects of this scenario are the following:

   - Policy decisions, including media authorization, are made by
      Policy Servers.

   - The PS in the Resource Control District is separate from the PS
      in the Session Control District.

   - There is a pre-defined trust relationship between the SMS and the
      SCD PS.

   - There is a pre-defined trust relationship between the ER and the
      RCD PS.

   - There are no pre-defined trust relationships between the ER and
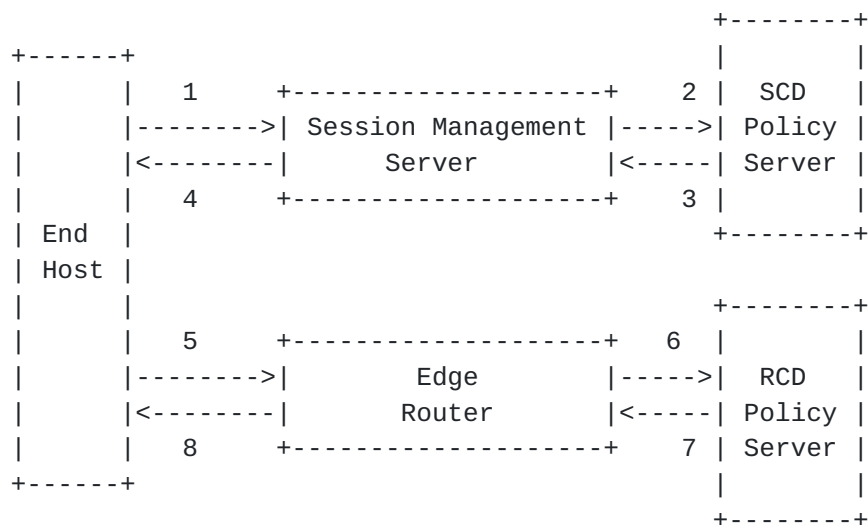   SMS or between the RCD and SCD Policy Servers.

```
                                                 +--------+
                                                 |        |
      +------+                                   |        |
      |      |   1     +--------------------+  2 |  SCD   |
      |      |-------->| Session Management |----->| Policy |
      |      |<--------|      Server        |<-----| Server |
      |      |   4     +--------------------+  3 |        |
      | End  |                                   +--------+
      | Host |
      |      |                                   +--------+
      |      |   5     +--------------------+  6 |        |
      |      |-------->|        Edge        |----->|  RCD   |
      |      |<--------|       Router       |<-----| Policy |
      |      |   8     +--------------------+  7 | Server |
      +------+                                   |        |
                                                 +--------+
```

   Figure 5: The Non-Associated Model

[7.1](#)   Non-Associated Model Call Flow

   In this model it is assumed that the policy servers make independent

decisions for their respective districts, obviating the need for

information exchange between policy servers. Communications between
network entities in this model is described below:

1. The End Host issues a session set-up request (e.g. SIP INVITE) to
   the Session Manager indicating, among other things, the media
   streams to be used in the session. As part of this step, the End
   Host may authenticate itself to the Session Manager.

2. The Session Manager, possibly after waiting for negotiation of
   the media streams to be completed, sends a policy decision
   request (e.g. COPS-SIP REQ) to the SCD Policy Server in order to
   determine if the session set-up request should be allowed to
   proceed.

3. The SCD Policy Server sends a decision (e.g. COPS-SIP DEC) to the
   Session Manager, possibly after modifying the parameters of the
   media to be used. Included in this response is a "token" that can
   subsequently be used by the RCD Policy Server to determine what
   media has been authorized.

4. The Session Manager sends a response to the End Host (e.g. SIP
   200 or 183) indicating that session set-up is complete or is
   progressing. Included in this response is a description of the
   negotiated media along with the token from the SCD Policy Server.

5. The End Host issues a request (e.g. RSVP PATH) to reserve the
   resources necessary to provide the required QoS for the media
   stream. Included in this request is the token from the SCD Policy
   Server provided via the Session Manager.

6. The Edge Router intercepts the reservation request and sends a
   policy decision request (e.g. COPS-RSVP REQ) to the RCD Policy
   Server in order to determine if the resource reservation request
   should be allowed to proceed. Included in this request is the
   token from the SCD Policy Server provided by the End Host.

7. The RCD Policy Server uses this token to extract information
   about the media that was authorized by the SCD Policy Server. The
   RCD Policy Server uses this information in making its decision on
   whether the resource reservation should be allowed to proceed.

   The Policy Server sends a decision (e.g. COPS-RSVP DEC) to the
   Edge Router, possibly after modifying the parameters of the
   resources to be reserved.

8. The Edge Router, possibly after waiting for end-to-end
   negotiation for resources to be completed, sends a response to
   the End Host (e.g. RSVP RESV) indicating that resource
   reservation is complete or is progressing

7.2   Non-Associated Model Authorization Token

In this model, the token must contain sufficient information to
allow the RCD Policy Server to make resource policy decisions
autonomously from the SCD Policy Server. The token is created using
information about the session received by the SMS. The information
in the token must include:

- Calling party IP address and port number (e.g. from SDP "c="
  parameter).

- Called party IP address and port number (e.g. from SDP "c="
  parameter).

- The characteristics of (each of) the media stream(s) authorized
  for this session (e.g. codecs, maximum bandwidth from SDP "m="
  and/or "b=" parameters).

- The lifetime of (each of) the media stream(s) (e.g. from SDP "t="
  parameter).

- The authorization lifetime (e.g. the token should be valid for
  only a few seconds after the start time of the session).

- The identity of the authorizing entity to allow for validation of
  the token.

- An authentication signature used to prevent tampering with the
  token and to provide the credentials of the authorizing entity.
  This signature is calculated over all other fields of the token
  using an agreed mechanism. The RCD Policy Server must be able to
  verify the signature using credentials of the signer to confirm a
  trust relationship. The mechanism used by the RCD Policy Server
  is beyond the scope of this document.

7.3   Non-Associated Model Protocol Impacts

The use of a media authorization token in the Non-Associated Model
requires the addition of new fields to several protocols:

- Resource reservation protocol. A new protocol field or object
  must be added to the resource reservation protocol to
  transparently transport the token from the End Host to the Edge
  Router. The content and internal structure of this object should
  be opaque to the resource reservation protocol.

- Policy management protocol. A new protocol field or object must
       be added to the policy management protocol to transport the token

          from the SCD Policy Server to the Session Management Server and
          from the Edge Router to the RCD Policy Server. The content and
          internal structure of this object must be specified so that the
          Policy Servers can distinguish between the elements of the token
          described in Section 7.2.

     - Session management protocol. A new protocol field or object must
        be added to the session management protocol to transparently
        transport the media authorization token from the Session
        Management Server to the End Host. The content and internal
        structure of this object should be opaque to the session
        management protocol.

8. Conclusions

     In this document we have defined three models for authorizing media
     during session establishment:

     - The Coupled Model which assumes a priori knowledge of network
        topology and where pre-established trust relationships exist
        between network entities.

     - The Associated Model where there are common or trusted policy
        servers but knowledge of the network topology is not known a
        priori.

     - The Non-Associated Model where knowledge of the network topology
        is not known a priori, where there are different policy servers
        involved and where a trust relationship does not exist between
        the policy servers.

     The Associated Model is applicable to environments where the network
     elements involved in establishing a session have a pre-determined
     trust relationship but where their identities must be determined
     dynamically during session set up. The Non-Associated Model is
     applicable to environments where there is a complex network topology
     and/or where trust relationships between domains do not exist.

     In any given network, one or more of these models may be applicable.
     Indeed, the model to be used may be chosen dynamically during
     session establishment based on knowledge of the end points involved
     in the call. In all cases, however, there is no need for the End
     Host, the Edge Router or the Session Management Server to understand
     or interpret the authorization token - to them it is an opaque
     protocol element that is simply copied from one container protocol
     to another.

   Finally, the framework defined in this document is extensible to any
   kind of session management protocol coupled to any one of a number
   of resource reservation and/or policy management protocols.

9. Security Considerations

   The purpose of this draft is to describe a mechanism for media
   authorization to prevent theft of service. It does not cover other
   possible security breaches such as IP spoofing.

   This draft assumes that trust relationships exist between various
   network entities, as described in each of the models. The means for
   establishing these relationships are beyond the scope of this
   document.

   For the authorization token to be effective, its integrity must be
   guaranteed as it passes through untrusted network entities such as
   the End Host. This can be achieved by using digital signatures.

References

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

   [2] J. Vollbrecht et al., "AAA Authorization Framework", RFC 2904,
        August 2000

   [3] P. Calhoun et al., "DIAMETER Base Protocol", Internet Draft
        draft-calhoun-diameter-17.txt, September 2000.

   [4] S. Herzog et al., "COPS usage for RSVP", RFC 2749, January
        2000.

   [5] W.Marshall et al. "Integration of Resource Management and SIP",
        Internet-Draft, draft-ietf-sip-manyfolks-resource-00, November
        2000.

   [6] W. Marshall et al., "SIP Extensions for Media Authorization",
        Internet-Draft, draft-ietf-sip-call-auth-01.txt, February 2001.

   [7] L. Hamer et al. "Session Authorization for RSVP", Internet-
        Draft, draft-hkg-rap-rsvp-authsession-00.txt, February 2001.

   [8] "PacketCable Dynamic Quality of Service Specification",
        CableLabs, December 1999.
        http://www.packetcable.com/specs/pkt-sp-dqos-I01-991201.pdf

        Framework for session set-up with media authorization

Acknowledgments

   The authors would like to thank to following people for their useful
   comments and suggestions related to this draft: Doug Reeves, Sam
   Christie, Matt Broda, Yajun Liu, Brett Kosinski, Francois Audet,
   Jerry Chow, Joe Mierwa, Bill Marshall and many others.

Authors' Addresses

   Louis-Nicolas Hamer
   Nortel Networks
   Ottawa, ON
   CANADA
   Email: nhamer@nortelnetworks.com

   Bill Gage
   Nortel Networks
   Ottawa, ON
   CANADA
   Email: gageb@nortelnetworks.com

Expiration Date

   This memo is filed as <draft-ietf-rap-session-auth-00.txt>, and
   expires September 31, 2001.