Internet Engineering Task Force   G. Gross
INTERNET DRAFT   Intel Corporation
draft-gross-sipaq-00.txt
November, 2000   H. Sinnreich
Expires: May 2001   D. Rawlins
SIP Working Group   MCI WorldCom

                                                       S. Thomas
                                                      TransNexus

QoS and AAA Usage with SIP Based IP Communications

Status of this Memo

Abstract

   This document specifies the architecture, protocols and messages for
   SIP based IP communications between Internet domains in support of
   QoS and AAA. Detailed message flows and message contents are
   discussed and specified. AAA requirements including inter-domain and
   user authorization in mobile and non-mobile environments are
   addressed. A solution is proposed where session setup and teardown
   are linked with QoS and AAA signaling using AAA policy servers and
   clearinghouses.

Table of Contents

[1](#). **Introduction**

   Commercial grade IP communications may require voice and other media
   transport of equal or higher quality than present 3.1 kHz circuit
   switched voice. Conversely, lower media quality may be acceptable in
   cases where other service advantages exist, similar to wireless
   audio/video streaming.

   We focus here on those circumstances where voice and other media
   quality are important and require end-to-end network resources for
   QoS with larger bandwidth and/or lower delay. Dynamic setup of end-
   to-end network resources for QoS requires highly scalable mechanisms
   to authenticate, authorize and account (AAA) for network resources
   across the Internet. This must be able to happen between a very
   large number of independent and various access domains that may have
   no business or trust relationship with each other, or may not even
   know of each other's existence before initiating end-to-end
   communications.

   The term IP communications is used here for a large class of new
   communications enabled by IP and the Internet such as presence,
   instant text, voice or multimedia conferences, the integration of
   messaging and real time communications, the integration of
   communications in productivity software, with transactions, games,
   entertainment and other. Not all IP communication services can be
   extended to other networks, such as PSTN, ISDN, H.323, BICC or the
   so-called "softswitch" networks that use MEGACO or similar master-
   slave signaling protocols.

   AAA services are important because QoS and IP to PLMN and PSTN
   termination through gateways are services that are billable.
   Unauthorized users should be prevented from using these services and
   service providers should be able to appropriately bill authorized
   users.

   This document specifies the architecture, protocols and messages for
   SIP based IP communications between Internet domains in support of
   QoS and AAA [1]. It builds on information presented in [2] and [3].
   This document discusses AAA requirements including inter-domain and
   user authorization in mobile and non-mobile environments. One AAA
   solution is proposed. The developments in this document assume 2
   party call control only. The term originator implies a user who
   initiates and participates in the IP communication session.

[2](#). **Terminology**

   This section defines terms used throughout this document. Some of
   these terms may have other meanings outside the context of this

work. Their outside meanings are not guaranteed to coincide with the
definitions given here.

APS: AAA and Policy Server. The APS acts as a policy decision point,
   PDP, for network usage related policies, including IP telephony

and QoS requests such as bandwidth reservation. The APS acts on
service requests, such as SIP INVITEs for calls requiring QoS
and possibly outsources requests to other PDPs, such as a DIR,
ADB, or CH. The APS renders a decision and may then apply
policy to network elements.

CH: Clearinghouse. The CH authorizes inter-domain calls with QoS
and collects usage reports for settlement between service
providers.

DIR: Directory. The DIR is the source for end user names and their
services. A DIR has the list of all individual users and some
attributes that the APS may use as criteria for policy
decisions on an individual basis.

ADB: Accounts Database. The ADB is part of the "back office" of the
service provider. The ADB contains a list of all corporate
accounts and the respective service level specifications that
apply at the edges of their networks. It may have classes of
policies or customized policies for various corporate accounts.

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 [4].

3. Overview

The components involved in AAA and QoS enabled IP communication
sessions are shown in Figure 1. SP represents a SIP Proxy. The
clearinghouse (CH) exists outside the access domains and is
responsible for providing inter-domain AAA services. In some cases a
customer APS may exist outside the access domain. One such case may
be where the customer has his or her own corporate domain with a
corresponding corporate APS.

Routers internal to the domain are labeled "R" and the edge router
is labeled "ER". The media agent, "MA", is the application that
sends/receives telephony/multimedia session data. The ER may be
responsible for aggregating RSVP flows into appropriate Diffserv
classes.

All developments discussed in this document apply using SIP for
setting up IP communications. Other signaling means such as H.323,
MEGACO or related protocols, may have a different structure in the
dependency between signaling, QoS setup and AAA and are therefore
not the object of this draft.

The SIP User Agent, SIP UA, acts as client and server on behalf of
the user. If an IP phone originated the session, the SIP UA resides

on the IP phone. If the signal entering the access domain came
directly from a gateway, the SIP UA may reside in the access domain,
as shown in the figure. In any case, the specific details of this
configuration are not relevant to the development in this document.

The large box in Figure 1 is labeled as an ISP. In general, it may
be an enterprise domain. Additionally, an enterprise domain may
outsource SIP services to an ISP. In that case, both domains may be
shown in the figure. For simplicity, Figure 1 is shown with a single
domain.

```
         +-------------------------------------------+
         |  ISP                                      |
         |                +-----+   +-----+          |
         |                | DIR |   | ADB |          |
         |                +-----+   +-----+          |
         |                   |         |             |
         |                   |         |             |
+-----+  |                +-------+     |    +----+
|Cstmr|  |                |       |     |----------+---| CH |
| APS |--+----------------|  APS  |          |      +----+
+-----+  |                |       |     |------------+   |
         |                +-------+     |         |  |
         |  +--------+       |     /             |  |
+-----+  |  | SIP UA |       |    /              |  |
| IP  |--+--|        |       |   /               |  |
|Phone|  |  | +----+ |  +----+  /                |  | Signaling
| or  |  |  | |SIP |-+--| SP |--+-------------+---+-------------
|Gtwy |  |  | | |    | |  +----+  /           |  |
+-----+  |  | +----+ |       /              |  |
         |  |        |      /               |  |
         |  | +----+ |     +---+        +----+ | Session data
         |  | | MA |-+--------| R |---------| ER |-+--------------
         |  | +----+ |     +---+        +----+ |
         |  +--------+                        |
         +-------------------------------------------+
```
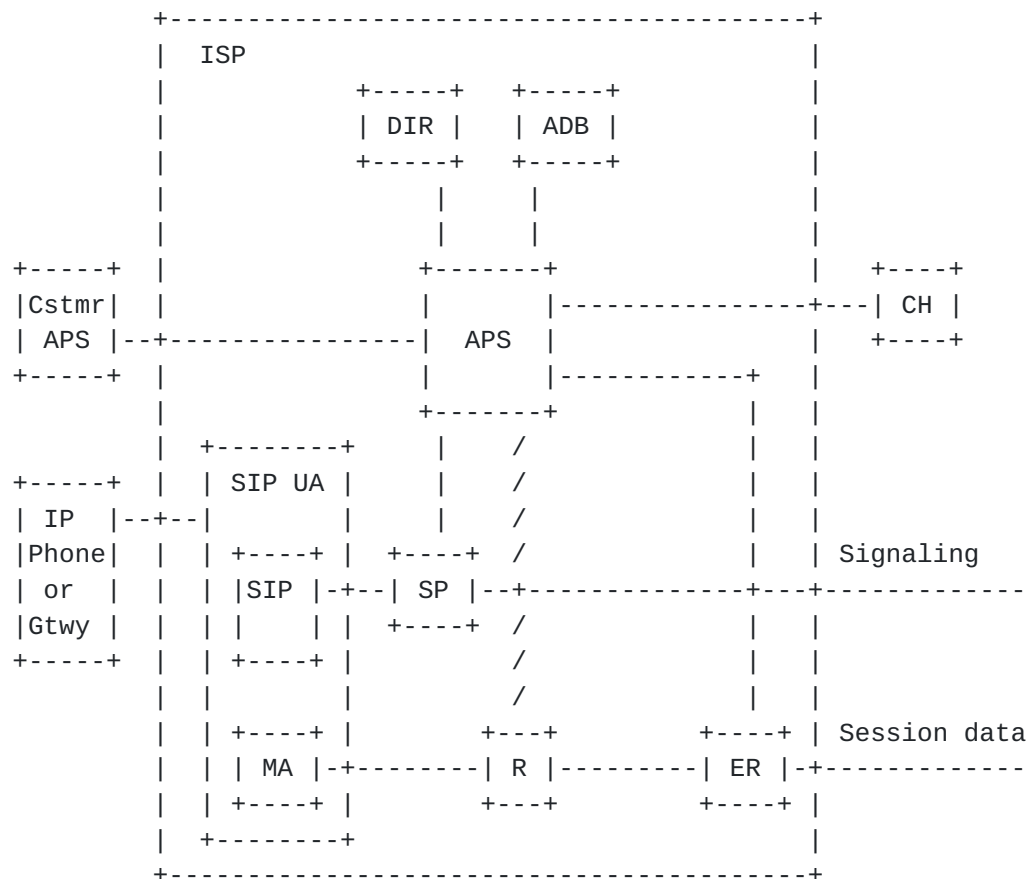
Figure 1: Components to Support Inter-domain AAA QoS Services

The SIP proxy acts as a policy enforcement point, PEP, for IP
communication sessions that use SIP. An extension to COPS has been
defined that outlines the syntax and semantics of COPS messages and
COPS objects for use with SIP [5]. The APS is the corresponding
policy decision point, PDP, for SIP sessions. The APS also interacts
with the DIR, ADB, customer APS and CH for information on which to
base a service usage decision. If QoS is requested and granted, the
APS may also interact with applicable network device(s) to aid in
QoS setup.

Clearinghouses are used to provide scalable, inter-domain AAA
services. One or more clearinghouses may be involved in an IP
communications session. Network devices along the session data path

use one or more QoS mechanisms to provide a user specified level of
service. RSVP [6] may be one such QoS mechanism in access networks
and Diffserv [7] may be a QoS mechanism in the transit network.

Internal routers may or may not participate in bandwidth reservation. If it can be assumed that internal routers are not bottlenecks and will always have sufficient resources to handle requests without reservations, message exchanges with the APS may be eliminated. In this case, the slanted line connecting the APS with R in Figure 1 may be ignored.

4. Authorization and Authentication

Proper authorization and authentication may be accomplished in a variety of ways. In pursuit of the most suitable technique, various factors must be considered. These factors include:

1) minimizing call setup time
2) minimizing the time and occurrences that authorization
   tokens/messages are placed on the wire
3) minimizing implementation complexity
4) optimization of business relationship models (use of
   clearinghouses as opposed to many bi-lateral agreements).

With these factors in mind, this document discusses some of the requirements of authorization and authentication and suggests one technique as a solution.

Requirements of authorization and authentication include:

1) user authorization
2) inter-domain authorization

In this document, user authorization is taken for granted when the session originator is in his/her home domain. This scenario is discussed in the first sub-section below. When the session originator roams into a foreign domain, or another party participating in the session roams into a foreign domain (called party), user authorization is necessary. Foreign domains are referred to as local domains in this document because they are local to the roaming user. This scenario is considered in the second sub-section below.

While roaming, user registration is assumed to occur before an IP communication session is initiated [8]. During the user registration process, relevant information is exchanged between the roaming user and the local domain. This information includes the roaming users home domain. The registration process may use the AAA infrastructure described in this document. Further details concerning user registration are out of the scope of this document.

The solution suggested within this document to handle AAA requirements in QoS enabled IP communication sessions is with the

use of one or more authorization tokens and clearinghouses. This
solution makes every attempt to address the factors listed
previously to provide the most suitable solution.

Although accounting is not discussed in this section, it is an implied necessity. IP communication sessions must trigger the submission of usage indications or reports after session completion. This facilitates correct accounting.

4.1. Inter-domain

Assume Domain 1, D1, and Domain 2, D2, register with Clearinghouse x (CHx). The necessary security infrastructure is put in place between CHx and D1 and CHx and D2. The security infrastructure must support authentication and authorization services. In some situations it may also be important to support a non-repudiation service to prevent the false denial of IP communication services.

Such an infrastructure can be supplied in the form of a public key infrastructure, PKI, based system or a symmetric key based system such as Kerberos. This infrastructure must be operational before the services of CHx are available. If a PKI based system is used D1 may register with CHx, and in the process exchange public key certificates with CHx. CHx may then use the certificate from D1 to authenticate that any message received from D1 actually came from D1. Analogously, D1 may use the certificate from CHx to authenticate that any message received from CHx actually came from CHx. This can be facilitated by the built in security functionality of OSP [9].

Authentication of the SIP proxy and all end users within a domain is the responsibility of the domain administrator. Maintenance of intra-domain security is required because CHx only authenticates D1 as a whole through the APS. Intra-domain authentication of users requires another level of authentication not discussed in this section. This level of authentication is an especially important consideration for roaming users.

When an end host caller from D1, EH1, calls an end host callee in D2, EH2, the APS in D1, APS1, requests an authorization token from CHx to verify that an appropriate business relationship exists with D2. This development is illustrated in Figure 2. The figure only illustrates messaging that includes the authorization token.

If authorization is granted, CHx replies with an authorization token to APS1. This token carries sufficient authentication information so that D2 (and possibly CHx) can later verify that it was created by CHx (or possibly another trusted CH) and not by a fraudulent source. This is in addition to the digital signatures contained in the messages exchanged between CHx and APS1 used to authenticate individual messages.

The APS1 may now authorize the call to the SIP proxy of D1, SP1.

APS1 may store the session source, destination, and media
information to aid in QoS setup. SP1 embeds the authorization token
in the SIP INVITE messages and forwards it to the SIP proxy of D2,
SP2.

Upon reception of the INVITE message, SP2 contacts APS2, passing it
the authorization token, to request local and inter-domain
authorization to complete session setup. Because the authorization
token contains self-authentication information, APS2 can
authenticate that CHx has actually authorized the incoming call.
This removes the requirement for APS2 to contact CHx.

```
                         (1)     +--------+
                      +-------|  CHx   |
                      |       +--------+
          Domain 1    |                            Domain 2
    +----------------+---+                +--------------------+
    |                |   |                |                    |
    |     (2) +------+   |                |  +------+ (4)       |
    |      +----| APS1 | |                |  | APS2 |----+      |
    |      |    +------+ |    ---------    |  +------+    |      |
    |   +-----+   (3)    |   ( Transit )   |           +-----+  |
    |   | SP1 +----------+---( Network )---+---------->+ SP2 |  |
    |   +-----+          |   (         )   |           +-----+  |
    |          +------+  |    ---------    |  +------+           |
    |          | ER1  |  |                 |  | ER2  |           |
    |          +------+  |                 |  +------+           |
    |   +-----+          |                 |           +-----+   |
    |   | EH1 |          |                 |           | EH2 |   |
    |   +-----+          |                 |           +-----+   |
    |                    |                 |                     |
    +-------------------+                 +--------------------+
```
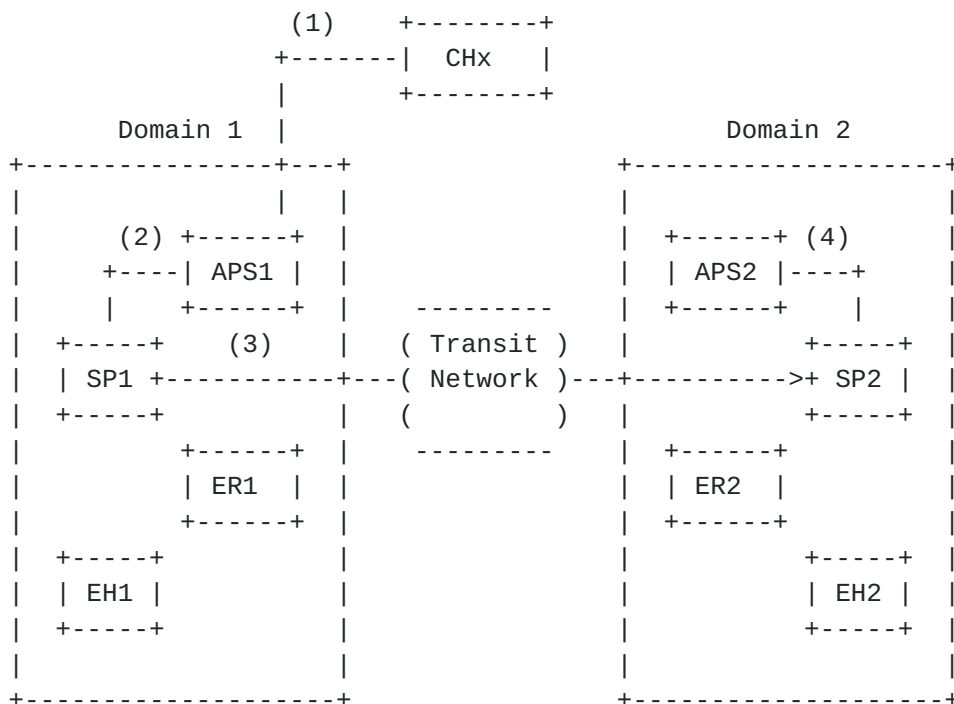
    1) APS1 requests an auth token from CH, triggered by session
       setup request from EH1
    2) APS1 returns auth token to SP1 (SP1 embeds token in
       session signaling message)
    3) SP1 signals SP2 with embedded token
    4) SP2 sends auth token to APS2 for authorization and
       authentication
    5) auth token no longer used, may be destroyed

            Figure 2: Authorization Token Life Cycle

After EH1 and EH2 have been notified that the IP communication
session has been authorized, they may now proceed to reserve
bandwidth using a mechanism such as RSVP. Bandwidth management
services determine if the requested bandwidth is available over the
specified path.

The originating and terminating domains have now completed proper
inter-domain authorization. If authorization was granted call setup
can complete and data may be exchanged over the reserved path. In

some models, pre-session establishment of QoS may be a requirement.
In such cases, completion of session setup may only transpire if QoS
has been established in the required direction(s) [2], [10]. In
other models, establishment of QoS and the IP communication session
may be decoupled, where each proceeds independently [2].

4.2. **Application Level and Pre-call Mobility**

   Mobility of an end user demands additional infrastructure to
   authenticate and authorize the user while roaming. Three or more
   domains may be involved in the AAA and call setup process. The local
   domain may be defined as the domain that the user has roamed into.
   The home domain may be defined as the domain where the user
   maintains a user profile that contains, among other things, a list
   of services for that user. The called domain is the domain in which
   the called party is present. Note that in the general case, this may
   not be the called party's home domain. That is, the called party may
   also be roaming. An additional level of authorization and
   authentication would be necessary in this case. For simplicity, this
   document addresses the case where the called party is reached at his
   or her home domain.

   In general, authorization and authentication between domains is
   necessary because billable QoS services may be requested along a
   path between them. All carriers included in this path who transmit
   the session data and provide the requested QoS services will expect
   accounting and/or payment.

   However, there is a distinction between the end domains where per
   call accounting may be required and the transit networks that need
   not to be burdened with the knowledge or understanding of each
   individual qos flow. For scalability, the transit networks will
   group all qos flows in some Diffserv class of traffic. The
   discussion that follows applies only to the end domains where the
   calls originate and terminate.

   Accounting agreements can be encompassed in a business relationship
   with a clearinghouse. An authorization token can be used to verify
   the business relationship between the local domain and the
   clearinghouse and the called domain and the clearinghouse. These are
   the domains between which the session data will travel.

   A business relationship may also include roaming allowances and
   services. This implies that a user who roams into a foreign domain
   may proceed to use the IP communication services that he/she pays
   for and normally receives from his/her home domain. An authorization
   token can be used between the local and home domains to verify such
   a business relationship with a clearinghouse.

   Under the assumption that the caller pays for services, the local
   domain is obligated to pay for the bandwidth consumed by the session
   data between the local and called domains. The charges received by
   the local domain must propagate back to the home domain of the

caller so that the call is ultimately accounted. The charges would
likely appear on the caller's monthly statement. The use of
authorization tokens to verify business agreements can provide the
infrastructure to allow such transactions to be completed.

In most cases, SIP signaling sessions which involve mobile SIP
terminals will be directed through the home domain of the mobile
user in order to maintain home control. Home control is important
for the execution of signaled services because the user then sees
the same services irrespective of the network capabilities of the
local domain he/she has roamed into. These services are contained in
a user profile at the user's home domain.

The authorization tokens obtained from one or more clearinghouses
may be embedded in the SIP signaling during session establishment.
The order in which tokens are obtained is not clear at this time.
Also, the domain(s) that contact the clearinghouse(s) for
authorization token requests is not clear at this time. Two possible
scenarios are illustrated in Figures 3 and 4. We note that in each,
options exist concerning clearinghouse contacts and messaging order.

In Figure 3, session signaling (SIP INVITE message) arrives at the
SIP proxy of the local domain (1). The SP, acting as a SIP PEP,
makes a request to the APS, acting as a SIP PDP (2). The APS of the
local domain contacts one or more clearinghouses seeking appropriate
business relationships with the home and called domains (3, 4). If
all three domains are registered with the same clearinghouse, only
that clearinghouse need be contacted. The clearinghouses return one
or more authorization tokens to the APS, which passes them back to
the SP. The SP embeds the tokens within the SIP INVITE message and
forwards it to the home domain of the caller (5).

```
              |  Local   | Clearing | Home Dom  |  Called   |
              |  Domain  |  House   |  of UA1   |  Domain   |
             +----------+----------+-----------+----------+
              |          |          |           |          |
              |  +----+  |3 +----+  |           |          |
              |  |APS |--+--|CHx |  |  +-----+  |  +----+  |
              |  |    |  |  +----+  |  | APS |  |  |APS |  |
              |  |    |  |          |  |     |  |  |    |  |
              |  |    |  |4 +----+  |  |     |  |  |    |  |
              |  |    |  |--+--|CHy |  |  +-----+  |  +----+  |
              |  +----+  |  +----+  |     |     |     |     |
              |    |     |          |     |     |     |     |
              |    |     |          |  6  |     |  8  |     |
              |  2 |     |          |     |     |     |     |
     +---+    |    |     |          |     |     |     |     |   +---+
     |SIP| 1| +----+  |     5    |  +-----+  |7 +----+  |9 |SIP|
     |UA1|--+--| SP |--+-----------+--|  SP   |--+--| SP |--+--|UA2|
     +---+    | +----+  |          |  +-----+  |  +----+  |   +---+
              |    |     |          |     |     |     |
```
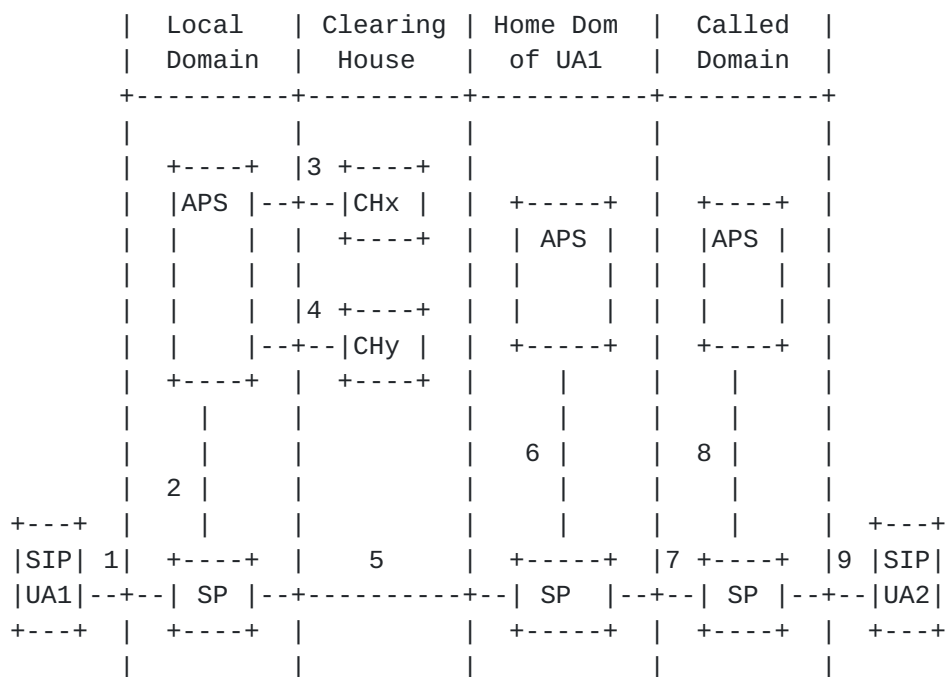
              Figure 3: Scenario 1 - Session Setup with AAA Support

The SP in the home domain contacts the APS using a PEP/PDP
relationship (6). The SP or APS refer to the user profile to verify
that the requested services allowed. The APS verifies the applicable
authorization token and may make additional policy-based admission

decisions. The decision is passed back to the SP. The INVITE message
is then forwarded to the SP of the called domain (7). The SP
contacts the APS using a PEP/PDP relationship (8). The APS verifies
the applicable authorization token and may make additional policy-
based admission decisions. The decision is passed back to the SP.
The SP finally forwards the INVITE message to the called user, SIP
UA2 (9).

In Figure 4, the messaging is different only in one way. The APS of
the local domain contacts the APS of the home domain before any
authorization tokens are obtained (3). The APS of the home domain
checks the user's profile to authorize the use of services. If the
home domain authorizes the session, the APS in the local domain
receives a success reply and proceeds to obtain necessary
authorization tokens as described for Figure 3.

```
             | Local    | Clearing | Home Dom  | Called   |
             | Domain   |  House   |  of UA1   | Domain   |
            +----------+----------+-----------+----------+
            |          |          |           |          |
            |  +----+  |4 +----+  |           |          |
            |  |APS |--+--|CHx |  |  +-----+  |  +----+  |
            |  |    |  |  +----+  |  | APS |  |  |APS |  |
            |  |    |  |    3     |  |     |  |  |    |  |
            |  |    |--+----------+--|     |  |  |    |  |
            |  |    |  |  |       |  |     |  |  |    |  |
            |  |    |  |5 +----+  |  |     |  |  |    |  |
            |  |    |--+--|CHy |  |  +-----+  |  +----+  |
            |  +----+  |  +----+  |           |          |
            |    |     |          |     |     |    |     |
            |    |     |          |  7  |     |  9 |     |
            |  2 |     |          |     |     |    |     |
   +---+    |    |     |          |     |     |    |     |   +---+
   |SIP| 1| +----+     |    6     |  +-----+  |8 +----+   |10|SIP|
   |UA1|--+--| SP |--+----------+--| SP   |--+--| SP |--+--|UA2|
   +---+  |  +----+     |          |  +-----+  |  +----+  |  +---+
          |     |       |          |     |     |    |     |
```
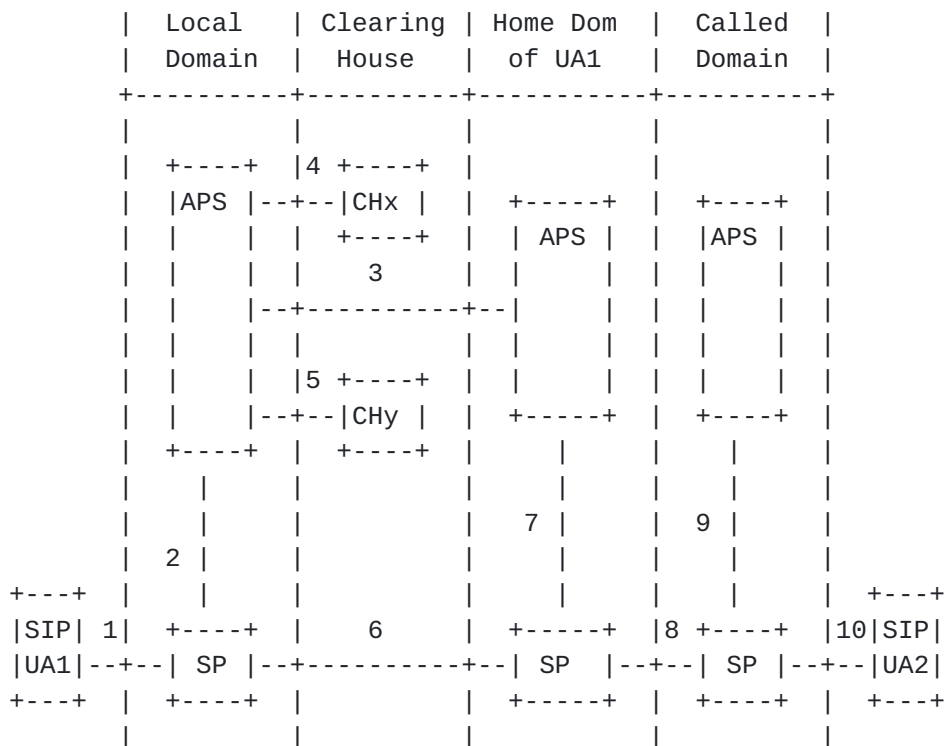
          Figure 4: Scenario 2 - Session Setup with AAA Support

The advantage of the scenario in Figure 4 is that the user's profile
is checked before any authorization tokens are obtained. In this
way, valuable airtime in the wireless case would not be wasted
transporting authorization tokens if the user's profile did not
allow the session to proceed. A disadvantage is that call setup time
may be lengthened somewhat due to an extra inter-domain message
exchange. Another disadvantage may be that a messaging protocol
between APSs would have to be defined. COPS is one protocol that may

be used for this interaction [11].

The authorization tokens ensure that authentic, billable parties
exist and that account, billing and charge settlement may be
achieved in a previously agreed upon manner. For scalability,

business relationships between domains do not need to exist.
Instead, business relationships with a clearinghouse can be used.

5. Message Contents

This section defines the data content of messages passed between the
SIP proxies, APS, and clearinghouse to provide QoS and AAA linkage
with SIP for inter-domain IP communication sessions. The messaging
discussed does not consider mobility. It considers an originating
domain and a terminating domain, each containing a SIP UA, a SIP
proxy, and an APS, similar to the illustration in Figure 2. If
inter-domain authorization and gateway location services are not
required, interaction with a CH and inclusion of an authorization
token in all exchanges listed in this section can be ignored.

A companion document defines a COPS extension for SIP that details
the messaging and message contents between the SP and APS [5]. The
current document merely discusses this messaging in general terms.
Please refer to the referenced document for full details.

5.1. SIP Proxy to APS (Originating Domain)

When a SIP proxy receives an INVITE, it sends to the APS source,
destination, and possibly media information. The source and
destination information may be used by the APS for intra-domain
policy-based admission authorization. It must be sent to the CH for
inter-domain authorization.

The SIP call identifier (callID) can be used by the APS for intra-
domain accounting. The callID must be sent to the CH in the
authorization request message. The CH may use this identifier when
generating an authorization token.

If the INVITE contains a SDP attribute specifying bandwidth
reservation [10], the APS may need to know the amount of bandwidth
requested. The bandwidth is implied by the media description [12],
[13]. Bandwidth information is necessary if the APS is charged with
the responsibility of managing bandwidth allocation based on user
and application information. For example, the APS may have a policy
that allows user X to reserve 300 Kbps for multimedia sessions with
users A through E and only 50 Kbps multimedia sessions with other
users.

5.2. APS to CH (from Originating Domain)

The information required by the CH for accurate AAA support may be
CH dependent. It is expected that all CHs require knowledge of the
source and destination domains for basic AAA purposes. The call
identifier may be useful for authorization token generation.

Bandwidth reservation amount may be required by a CH dependent on
the specific business agreement with the domains. This quantity may
be used as a basis for granting or denying authorization. If

bandwidth reservation amount is required, it must be put into a form
agreed upon by the parties involved, such as Kbps.

5.3. CH to APS (to Originating Domain)

The clearinghouse has the responsibility of making an authorization
decision concerning IP communication between the specified source
and destination domains. If gateway services are also requested, the
decision may also be based upon available gateways and subsequent
QoS or cost characteristics corresponding with that gateway. For
example, the business relationship of the end domains with the
clearinghouse may exclude IP communication sessions that incur costs
above a specific limit. Costs may result from long distance charges
over the PSTN or from bandwidth reservation over the IP network. The
location of a gateway will likely affect one or both of these costs.

The CH must return to the APS an authorization decision. If the
request is granted, the CH must also return to the APS an
authorization token. The authorization token is expected to contain
authentication information so that both end point domains recognize
it as coming from a trusted CH, as described in a previous section.
A transaction identifier may be returned by the CH and subsequently
used to correlate original authorization requests with usage
indication reports generated after the session has completed.

5.4. APS to SIP Proxy (Originating Domain)

The APS finally responds to the SIP proxy INVITE message with a
status, indicating if the user is allowed to send the INVITE further
along the SIP signaling chain. If the authorization is granted, the
APS passes the authorization token it received from the CH to the
SIP proxy. The SIP proxy includes this token inside the
authorization token header field of the INVITE message [14].

5.5. SIP Proxy to SIP Proxy (Originating to Terminating Domain)

The SIP proxy forwards the INVITE message containing the
authorization token from the originating domain to the terminating
domain in the manner defined by SIP.

5.6. SIP Proxy to APS (Terminating Domain)

The APS in the terminating domain requires the same information as
the APS in the originating domain on which to base an intra-domain
authorization decision. Additionally, if the APS receives an
authorization token, it performs an authentication check on it using
the security infrastructure previously established with the CH. This
action verifies that the authorization token is authentic and that
the requested service has been authorized by a trusted source.

[6](#). Protocol Support

The exchange of information between the APS and the SIP proxy may be
handled using COPS. As mentioned previously, a new COPS extension
for SIP is being developed concurrently with this work [5].
Exchanges between the APS and the CH can be handled using OSP [9].
OSP defines all messaging and message data field specifications that
are outlined in this document. No additional protocol work is
required for this exchange. Also, OSP has been embraced and is in
use by a number of large industry participants.

7. Messaging Overview

This section details the message exchange and message contents to
initiate and terminate a SIP-based IP multimedia session. Mobility
is not considered in this section. The caller and callee are both
present and active at their respective home domains.

It is assumed that the media will be transmitted and received from
both ends and that bandwidth reservation requests are made in both
directions using the SDP attributes discussed in [10]. In the first
subsection the inter-domain authorization occurs at the originating
domain. In the second subsection the inter-domain authorization
occurs at the terminating domain.
Descriptions of SIP messages, including requests and responses, are
not discussed in this document. They are discussed in detail in [1].
Descriptions of RSVP messages are not discussed in this document but
are discussed in detail in [15]. It is assumed that edge routers are
RSVP enabled PEPs. Furthermore, it is assumed that the edge routers
interact with the APS as PDPs of their respective domains for
policy-based management decisions concerning RSVP. Message exchanges
of this nature are assumed implicit in this section and are not
included in the messaging overview. Details concerning this message
exchange are in [16].

As discussed in [2], two QoS models may be defined for IP
communication sessions. The QoS assured model is one in which the
session and QoS signaling are coupled. In this case the session does
not proceed until/unless QoS has been successfully established. The
QoS enabled model decouples session and QoS signaling. In this case,
the session setup may complete and session data may be exchanged
even if QoS has not yet been, or never gets, established. The
messaging discussed in this document only considers the QoS enabled
model. The development in this section may be extended to work with
the QoS enabled model with the inclusion of extra messages defined
in [10] and [17].

Since QoS assured is assumed in the session flow examples, the RSVP
and SIP messaging are decoupled and may occur asynchronously. The
SIP, COPS and OSP messages outlined in the call flow examples may

therefore not necessarily be in chronological order with the RSVP
messages.

All components involved in message passing are illustrated in Figure
1. Those in the originating domain are subscripted with "o" and

   components in the terminating domain are subscribed with "t". The
   subscript "o/t" implies corresponding components in each domain. The
   protocol used for each exchange is indicated at each step. Each step
   also contains notes concerning the contents or special attributes of
   the message.

7.1. Originating Domain Contacts Clearinghouse

   The following discussion refers to Figures 5 and 6. The step numbers
   of Figure 5 are indicated as message labels in Figure 6. In step 1,
   the caller picks up the phone, requests a bandwidth reserved
   connection and dials a number. This causes the UAo to include
   appropriate SDP attributes in the SIP INVITE message indicating that
   QoS is being requested in both directions. The necessary information
   is passed from the SPo to APSo in step 2. APSo checks if local
   policy allows the call. This may include interaction with an
   external policy database, a DIR, an ADB, and/or another APS.

   If local policy authorizes the call, APSo sends the CH an
   authorization request for inter-domain authorization in step 3. The
   CH considers the source and destination information to determine if
   appropriate business relationships exist with the originating and
   terminating domains. Bandwidth and/or media information may also be
   used on which to base a decision. If authorization is granted, the
   CH generates an authorization token using the call identifier as
   well as other data. The CH sends the token to the APSo in step 4
   along with a status value indicating if authorization has been
   granted or not. The APSo passes this information on to the SPo in
   step 5.

   The SPo forwards the INVITE with the embedded authorization token
   down the SIP signaling chain in step 6 to SPt in the terminating
   domain. The SPt sends the necessary information to APSt in step 7.
   The APSt requests local authorization in a similar fashion as that
   described for the originating domain. The APSt then uses the
   authorization token and other message data to authenticate the token
   and determine if inter-domain authorization has been granted. In
   step 8 the APSt passes a status to the SPt indicating if the session
   has been authorized. If the call and all requested services are
   granted, the SPt forwards the INVITE on to the UAt in step 9.

   The UAt may then send the RSVP Path message to UAo in step 10 since
   it knows the source and destination addresses and ports and the
   traffic specifications. Note that in some cases, the SDP sent from
   UAt to UAo may contain multiple media formats, each having different
   bandwidth requirements. In this case, the UAo must make a final
   decision considering the choice of media formats. If the traffic
   specifications change, additional RSVP messages may be sent to

update the network devices along the session data path.

In steps 11 and 12 the UAt sends back a 180 (ringing) SIP response
to SPo via SPt. In some cases, the UAt may send a 183 (session
progress) SIP response followed by a 180 response. The 183 response

would follow the same path as the 180 response. For simplicity, only
the 180 response is shown in the figures.

```
1)   UAo   -->   SPo    (SIP)  INVITE; (SDP "a=qos:")
2)   SPo   -->   APSo   (COPS) src, dest, media, callID
3)   APSo  -->   CH     (OSP)  src, dest, callID
4)   CH    -->   APSo   (OSP)  status, auth token
5)   APSo  -->   SPo    (COPS) status, auth token
6)   SPo   -->   SPt    (SIP)  INVITE, (SDP "a=qos:"), auth token
7)   SPt   -->   APSt   (COPS) src, dest, media, callID, auth
                                   token
8)   APSt  -->   SPt    (COPS) status
9)   SPt   -->   UAt    (SIP)  INVITE
10)  UAt   -->   R/ERt  (RSVP) Path
11)  UAt   -->   SPt    (SIP)  180
12)  SPt   -->   SPo    (SIP)  180
13)  SPo   -->   APSo   (COPS) src, dest, media
14)  APSo  -->   SPo    (COPS) status
15)  SPo   -->   UAo    (SIP)  180
16)  UAo   -->   R/ERo  (RSVP) Path
17)  UAt   -->   R/ERt  (RSVP) Resv
18)  UAo   -->   R/ERo  (RSVP) Resv
19)  UAt   -->   SPo    (SIP)  200 OK via SPt (SDP (a=qos:))
20)  SPo   -->   APSo   (COPS) src, dest, media
21)  APSo  -->   SPo    (COPS) status
22)  SPo   -->   UAo    (SIP)  200 OK (SDP (a=qos:))
23)  UAo   -->   SPo    (SIP)  ACK
24)  SPo   -->   APSo   (COPS) src, dest, media
25)  APSo  -->   SPo    (COPS) status
26)  SPo   -->   SPt    (SIP)  ACK
27)  SPt   -->   APSt   (COPS) src, dest, media
28)  APSt  -->   SPt    (COPS) status
29)  SPt   -->   UAt    (SIP)  ACK

30)  UAo   <->   UAt    (RTP)  session data exchanged

31)  UAo   -->   SPo    (SIP)  BYE
32)  SPo   -->   APSo   (COPS) RPT, DRQ
33)  SPo   -->   SPt    (SIP)  BYE
34)  SPt   -->   APSt   (COPS) RPT, DRQ
35)  SPt   -->   UAt    (SIP)  BYE
36)  UAo   -->   ERo    (RSVP) PathTear and ResvTear
37)  UAt   -->   ERt    (RSVP) PathTear and ResvTear
38)  APSo  -->   CH     (OSP)  usage report - session duration,
                                   bandwidth consumed, etc.
39)  APSt  -->   CH     (OSP)  usage report - session duration,
                                   bandwidth consumed, etc.
```

Figure 5: Message Flow Details

     The SPo checks if the source, destination or media information are
     different from what was specified in the INVITE message. If so, SPo
     sends the information to APSo in step 13. APSo checks local policy

and returns a status to SPo in step 14 indicating if the session is
still allowed. If so, SPo sends the 180 response to UAo in step 15.

```
+---+    +---+   +----+ +---+   +---+   +---+ +----+   +---+   +---+
|SIP|    |SPo|   |APSo| |ERo|   |CH |   |ERt| |APSt|   |SPt|   |SIP|
|UAo|    |   |   |    | |   |   |   |   |   | |    |   |   |   |UAt|
+---+    +---+   +----+ +---+   +---+   +---+ +----+   +---+   +---+
  |        |       |      |       |       |      |       |       |
  |   1    |       |      |       |       |      |       |       |
  |------>|   2    |      |       |       |      |       |       |
  |        |----->|   3   |       |       |      |       |       |
  |        |       |------------>|       |      |       |       |
  |        |       |      |   4   |       |      |       |       |
  |        |   5   |<------------|       |      |       |       |
  |        |<-----|      |       |       |      |       |       |
  |        |       |      |   6   |       |      |       |       |
  |        |-------------------------------------------------->|       |
  |        |       |      |       |       |      |   7   |       |
  |        |       |      |       |       |      |<-----|       |
  |        |       |      |       |       |      |   8   |       |
  |        |       |      |       |       |      |----->|   9   |
  |        |       |      |       |       |      |       |----->|
  |        |       |      |       |       |      |  10   |       |
  |        |       |      |       |       |<-------------------|
  |        |       |      |       |       |      |       |  11   |
  |        |       |      |       |  12   |      |       |<-----|
  |        |<------------------------------------------|       |
  |        |  13   |      |       |       |      |       |       |
  |        |----->|      |       |       |      |       |       |
  |        |  14   |      |       |       |      |       |       |
  |   15   |<-----|      |       |       |      |       |       |
  |<------|       |  16   |       |       |      |       |       |
  |-------------------->|       |       |      |  17   |       |
  |        |  18   |      |       |       |<-------------------|
  |-------------------->|       |  19   |      |       |  19   |
  |        |<------------------------------------------|<-----|
  |        |  20   |      |       |       |      |       |       |
  |        |----->|      |       |       |      |       |       |
  |        |  21   |      |       |       |      |       |       |
  |   22   |<-----|      |       |       |      |       |       |
  |<------|       |      |       |       |      |       |       |
  |   23   |       |      |       |       |      |       |       |
  |------>|  24   |      |       |       |      |       |       |
  |        |----->|      |       |       |      |       |       |
  |        |  25   |      |       |       |      |       |       |
  |        |<-----|      |   26   |       |      |       |       |
  |        |-------------------------------------------->|       |
```
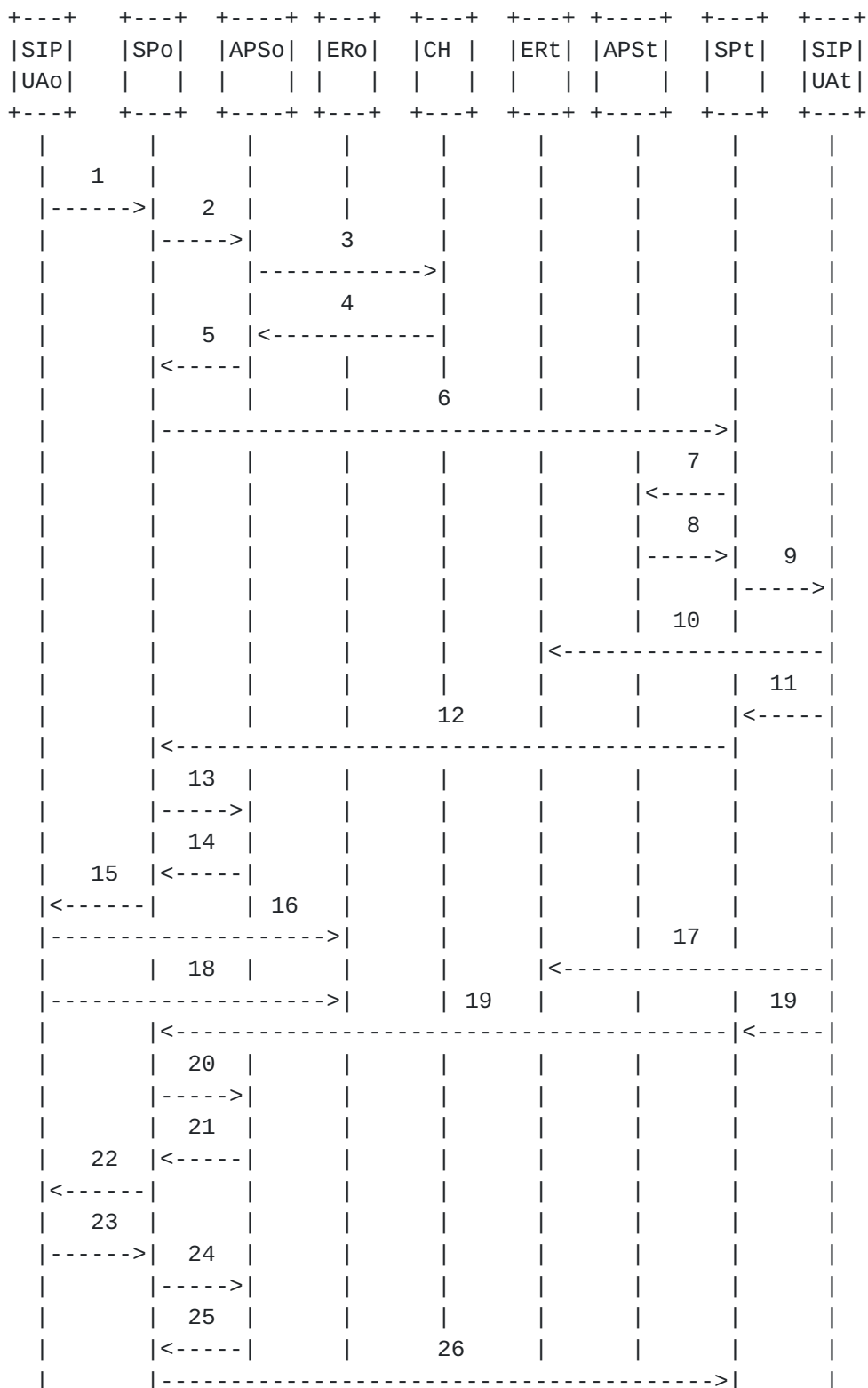
Figure 6: Message Flow

     UAo may now send a RSVP Path message to UAt in step 16 since it
     knows the source and destination addresses and ports and the traffic

specifications. When RSVP Path messages arrive at UAo and UAt, they
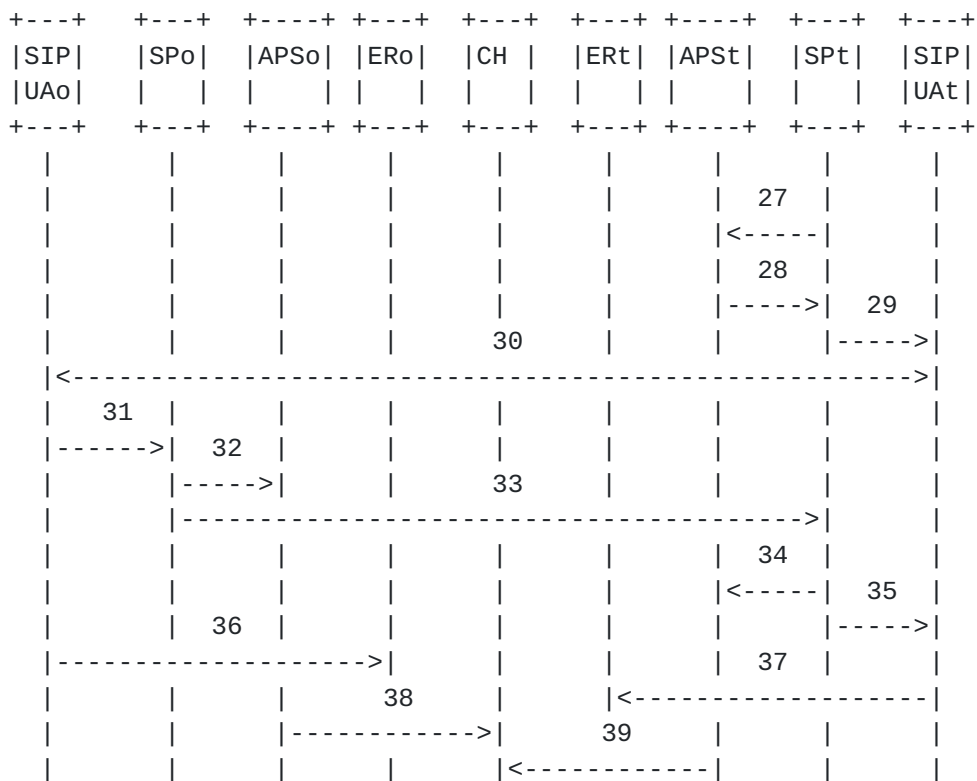may send a RSVP Resv message as shown in steps 17 and 18.

```
  +---+    +---+   +----+ +---+   +---+   +---+ +----+   +---+   +---+
  |SIP|    |SPo|   |APSo| |ERo|   |CH |   |ERt| |APSt|   |SPt|   |SIP|
  |UAo|    |   |   |    | |  | |   |   | |   | | |    |   |   |   |UAt|
  +---+    +---+   +----+ +---+   +---+   +---+ +----+   +---+   +---+
    |        |       |       |       |       |       |       |       |
    |        |       |       |       |       |       |   27  |       |
    |        |       |       |       |       |       |<-----|       |
    |        |       |       |       |       |       |   28  |       |
    |        |       |       |       |       |       |----->|   29  |
    |        |       |       |       |   30  |       |       |----->|
    |<------------------------------------------------------------->|
    |   31   |       |       |       |       |       |       |       |
    |------->|   32  |       |       |       |       |       |       |
    |        |------>|       |   33  |       |       |       |       |
    |        |       |-------------------------------------->|       |
    |        |       |       |       |       |       |   34  |       |
    |        |       |       |       |       |       |<-----|   35  |
    |        |   36  |       |       |       |       |       |----->|
    |-------------------->|       |       |       |   37  |       |
    |        |       |   38  |       |       |<--------------------|
    |        |       |------------>|   39  |       |       |       |
    |        |       |       |       |<------------|       |       |
```

Figure 6 (cont'): Message Flow

In step 19, UAt sends a final 200 (OK) response to SPo via SPt. If
the source, destination or media information are different from what
was specified previously, SPo sends a message to APSo in step 20.
APSo checks local policy and returns a status to SPo in step 21
indicating if the session is still allowed. If so, SPo sends the 200
response to UAo in step 22.

The UAo confirms reception of the 200 response and establishment of
the session by sending a SIP ACK message to SPo in step 23. If the
source, destination or media information are different from what was
specified previously, SPo sends a message to APSo in step 24. APSo
checks local policy and returns a status to SPo in step 25
indicating if the session is still allowed. If so, SPo sends the ACK
to SPt in step 26.

If the source, destination or media information known by SPt are
different from what was specified previously, SPt sends a message to
APSo in step 27. APSt checks local policy and returns a status to
SPt in step 28 indicating if the session is still allowed. If so,
SPt sends the ACK to UAt in step 29.

The session data is now exchanged via RTP, or some similar protocol,
in step 30. The session ends for UAo when the SIP BYE message is
sent to SPo in step 31. SPo sends a COPS report and deletes the COPS
request state in APSo in step 32. The BYE message is simultaneously

forwarded to SPt in step 33. SPt sends a COPS report and deletes the
COPS request state in APSt in step 34. The BYE message is sent to
UAt in step 35.

PathTear and ResvTear messages are sent from UAo and UAt upon call
completion (from UAt when it receives the BYE message) in steps 36
and 37. This triggers a COPS DRQ from ERo and ERt to APSo and APSt,
respectively. These messages are not shown but implicitly implied.
APSo and APSt may then perform necessary accounting/bookkeeping
chores. Alternately, ResvErr messages may be sent by an APS under
cancellation circumstances by APSo or APSt.

The APSo and APSt send usage reports to the CH in steps 38 and 39 to
indicate session duration, QoS services consumed such as bandwidth,
and possibly other session details necessary for inter-domain
accounting and settlement.

Usage indication reports are sent to the CH in steps 30 and 31.
Depending on the business agreement and the services used, this
interaction may require contact between the SPo/t and the APSo/t.

Other circumstances may cause the reservation in one or both
directions to fail. In this case, ResvErr messages may be injected
into the session data path. Upon reception of a PathErr or ResvErr
message, an ERo/t would remove the corresponding state and notify
APSo/t.

7.2. Terminating Domain Contacts Clearinghouse

The caller may have a reason to allow the terminating domain to
contact the CH for inter-domain authorization. For example, the
caller may require that the callee make an unusually large bandwidth
reservation for a critical IP communication exchange. The caller
does not know the limits of services the callee is entitled to. In
this case the caller may forego inter-domain authorization during
call setup. Instead, the APSt, on behalf of the callee, receives the
INVITE without a token, negotiates for an allowable level of
service, then contacts the CH for an authorization request. The
resulting authorization token is then placed inside the 200 response
sent back to the caller. Such a scenario may only make sense if the
CH requires bandwidth information (or other QOS service information
such as latency or jitter) to make an authorization decision.

The benefits of this are debatable. One advantage is that if
successful negotiation is not possible, the call may be cancelled
without contacting the CH, saving a message exchange. The message
exchange scenario is similar to that of Figure 5 with minor changes.

8. Accounting, Charging and Billing

We make a clear distinction between accounting, charging and billing
and provide a summary, possibly incomplete description.

Accounting: The process of logging the usage of network resources, such as QoS or PSTN gateway service. The accounting data may or may not be used for usage charging, depending on the service model. This draft addresses accounting only and does not address charging and billing.

Charging: Allocating the cost to various parties according to some business policies. Cost allocation may depend on such parameters as class of service, geographic locations, time of day, promotions, incentives for resellers and other. Examples of different business policies and classes of service are usage based charging and flat rate subscription rates.

Billing: Informing various users of the charges and expected payments.

9. Security Considerations

This document addresses some security issues concerning authentication of inter-domain business relationships. The protocols discussed in this work, SIP, COPS and OSP contain their own security mechanisms. Any security issues not addressed by SIP, COPS or OSP have not been considered in this work and are left as open issues.

10. Acknowledgments

The authors would like to thank Russ Fenger, Arun Raghunath, Changwen Liu, Mark Grosen, Jeff Mark, Kalon Kelley and Dave Durham for insightful discussions and valuable contributions.

11. References

[1] Handley, M., Schulzrinne, H., Schooler, E., and Rosenberg, J., "SIP: Session Initiation Protocol", RFC 2543, March 1999.

[2] Sinnreich, H., Donovan, S., Rawlins, D., Thomas, S., "Interdomain IP Communications with QoS, Authorization and Usage Reporting", Internet Draft, Internet Engineering Task Force, February 2000, Work in progress.

[3] Sinnreich, H., Rawlins, D., Johnston, A., Donovan, S., Thomas, S., "AAA Usage for IP Telephony with QoS", Internet Draft, Internet Engineering Task Force, July 2000, Work in progress.

[4] Bradner, S., "Key words for use in RFCs to indicate requirement levels", RFC 2119, March 1997.

[5] Gross, G., Sinnreich, H., Rawlins, D., Thomas, S., "COPS Usage for SIP", Internet Draft, Internet Engineering Task Force, November

2000, Work in progress.

[6] Braden, R., Zhang, L., Berson, S., Herzog, S. and S. Jamin, "Resource ReSerVation Protocol (RSVP) û Functional Specification", RFC 2205, September 1997.

[7] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., Weiss, W., "An Architecture for Differentiated Services", RFC 2475, December 1998.

[8] Schulzrinne, H., "SIP Registration", Internet Draft, Internet Engineering Task Force, October 2000, Work in progress.

[9] European Telecommunications Standards Institute. "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Inter-domain pricing, authorization, and usage exchange". Technical Specification 101 321 version 1.4.2, December 1998.

[10] Marshall, W., et al. "Integration of Resource Management and SIP", Internet Draft, Internet Engineering Task Force, June 2000, Work in progress.

[11] Boyle, J., Cohen, R., Durham, D., Herzog, S., Raja, R. and A. Sastry, "The COPS (Common Open Policy Service) Protocol", RFC 2748, January 2000.

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

[13] Schulzrinne, H., "RTP Profile for Audio and Video Conferences with Minimal Control", RFC 1890, January 1996.

[14] Johnston, A., Rawlins, D., Sinnreich, H., Thomas, S., "OSP Authorization Token Header for SIP", Internet Draft, Internet Engineering Task Force, November 2000, Work in progress.

[15] Braden, R., Zhang, L., Berson, S., Herzog, S. and S. Jamin, "Resource ReSerVation Protocol (RSVP) û Functional Specification", RFC 2205, September 1997.

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

[17] Rosenberg, J. and Schulzrinne, H., "Reliability of Provisional Responses in SIP", Internet Draft, Internet Engineering Task Force, June 2000, Work in progress.

12. Author's Address

Gerhard Gross

Intel Corporation
MS JF3-206
2111 NE 25th Ave.
Hillsboro, OR 97124

      Phone: +1-503-264-6389
      Fax: +1-503-264-3483
      gerhard.gross@intel.com

      Diana Rawlins
      WorldCom
      901 International Parkway
      Richardson, Texas 75081
      USA
      diana.rawlins@wcom.com

      Henry Sinnreich
      WorldCom
      400 International Parkway
      Richardson, Texas 75081
      USA
      henry.sinnreich@wcom.com

      Stephen Thomas
      TransNexus, LLC
      430 Tenth Street NW
      Suite N-204
      Atlanta, GA 30318
      USA
      stephen.thomas@transnexus.com

[13]. **Full Copyright Statement**

"AS IS" basis and THE INTERNET SOCIETY AND THEINTERNET ENGINEERING
TASK FORCE DISCLIAMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING
BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMAITON