SIP Working Group
Internet Draft
Document: <draft-dcsgroup-sip-call-auth-02.txt>

W. Marshall
K. Ramakrishnan
AT&T

E. Miller
G. Russell
CableLabs

B. Beser
M. Mannette
K. Steinbrenner
3Com

D. Oran
F. Andreasen
Cisco

J. Pickens
Com21

P. Lalwaney
Nokia

J. Fellows
Motorola

D. Evans
Secure Cable Solutions

K. Kelly
NetSpeak

June, 2000

SIP Extensions for 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. It is filed as <draft-dcsgroup-sip-call-auth-02.txt>, and expires December 31, 2000. Please send comments to the authors.

1. Abstract

This document describes the need for call authorization and offers a mechanism for call authorization that can be used for admission control and against denial of service attacks.

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 [2].

3. Background and Motivation

The current IP Telephony systems consider a perfect world in which there is unlimited amount of bandwidth and network layer QoS comes free. The reality is that bandwidth is neither unlimited nor free. Enhanced quality of service, as required for high-grade voice communication, needs special authorization for better than `best-effort' service. Without such a capability, it is possible that a single berserk IP telephony device can cause denial of service to a significant number of others.

4. Overview

Integration of Media Authorization and Call Signaling architecture consists of User Agents (UAs) which are considered untrusted, and SIP-Proxy which authorizes the call that is initiated by UA.

The SIP-Proxy authorizes the Media data flow to/from the UA and returns to the UA a Media-Authorization-Token, which is to be used for authorization when bandwidth is requested for the data-stream.

When the UA is ready to send the media data-stream to the other end-point, it first requests bandwidth, using the Authorization-Token it received from its SIP-Proxy.

5. Changes to SIP to Support Media Authorization

This document extends SIP in support of an authorization scheme. In this architecture the SIP-Proxy supplies the UA an Authorization-Token which is to be used for bandwidth requests. The extension defined allows network resources to be authorized by the SIP-Proxy.

The following syntax specification uses the augmented Backus-Naur Form (BNF) as described in RFC-2234 [3].

5.1 SIP Header Extension

The Media-Auth-Token general header conveys an identifier of the local Gate to a UA. This information is used for authorizing the Media Stream.

```
Media-Auth       = "Media- Authorization" ":"
                          Media-Authorization-Token

Media-Authorization-Token       = 1*hex
```

5.2 SIP Procedures

This section defines a SIP [4] profile for usage in Media Authorization compatible systems from the point of view of Authorizing Calls.

The initial SIP INVITE message, as well as mid-call resource change messages and mid-call changes in call destination should be authorized. These SIP messages are sent through the proxies to receive this authorization.

5.2.1. User Agent Client (UAC)

The Media-Auth-Token, contained in the Media-Authorization header, is included in the first response message sent by the SIP-Proxy to the UAC.

The UAC SHOULD use the Media-Auth-Token when requesting bandwidth for Media data stream during initiation and retaining of the bandwidth.

5.2.2. User Agent Server (UAS)

The User Agent Server receives the Media-Auth-Token in the INVITE message from SIP-Proxy.

The UAS SHOULD use the Media-Auth-Token when requesting bandwidth for media data stream during initiation and retaining of the bandwidth.

5.2.3. Originating Proxy (OP)

The Originating Proxy (OP) authenticates the caller, and verifies the caller is authorized to receive the requested level of QoS. In cooperation with originating Policy Decision Point (PDP-o), the OP obtains a Media-Auth-Token that contains sufficient information for the

UAC to get the authorized bandwidth for the media streams.

The Originating Proxy MUST insert the Media-Authorization header in the response message that it sends to the UAC.

5.2.4. Destination Proxy (DP)

The Destination Proxy (DP) authenticates the called party, and verifies the called party is authorized to receive the requested level of QoS. In cooperation with termination Policy Decision Point (PDP-t), the DP obtains a Media-Auth-Token that contains sufficient information for the destination UAS to get the authorized bandwidth for the media streams.

The Destination Proxy MUST insert the Media-Authorization header in the INVITE message that it sends to -the UAS.

6. Examples

6.1. Requesting Bandwidth via RSVP messaging

Resource Reservation Protocol (RSVP) is the end-to-end Layer 3 reservation protocol that is widely used [7].

6.1.1. User Agent Client Side

Figure 1 presents a high-level overview of a basic call flow with Media Authorization from the viewpoint of the UAC. It is assumed that the SIP-Proxy has a previously established a authentication relationship with the client.

When a user goes off-hook and dials a telephone number, the UAC collects the dialed digits and sends the initial INVITE message to the Originating SIP-Proxy.

The Originating SIP-Proxy (OP) authenticates
UAC
and forwards the INVITE
message to the proper SIP-proxy.

Assuming that the call is not forwarded, the other end-point sends a 183 response to the initial INVITE, forwarded back to OP. Included in this response is the negotiated bandwidth requirement for the connection.

When OP receives the 183, it has sufficient information regarding the end-points, bandwidth and characteristics of the media exchange. It initiates a Policy-Setup message to PDP-o.


```
UAC         ER-o            PDP-o           OP
|  Invite    |               |               | Client Authentication
|-------------------------------------------->| and Call Authorization
|            |               |               | Invite
|            |               |               |-------------->
|            |               |               | 180/3
|            |               | Auth. Profile |<--------------
|            |               |<--------------|
|            |               |  Auth. Token  |
|            |               |-------------->| Auth. Token put into
|            |               |   180/3       | Media-Authorization header
|<--------------------------------------------| extension.
|Copies the RSVP policy object               |
|from the Media-Authorization                |
| RSVP-PATHo |               |               |
|----------->| REQ           |               |
|            |-------------->| Using the Auth-Token and Authorized
|            |       DEC     | Profile that is set by the SIP Proxy
|            |<--------------| the PDP makes the decision
|            |               |               |   RSVP-PATHo
|            |------------------------------------------------>
|            |               |               |   RSVP-PATHt
|<--------------------------------------------------------------
|Copies the RSVP policy object               |
|from the Media-Authorization                |
| RSVP-RESVt |               |               |
|----------->|      REQ      |               |
|            |-------------->| Using the Auth-Token and Authorized
|            |       DEC     | Profile that is set by the SIP Proxy
```

```
|            |<--------------| the PDP makes the decision
|            |               |               |   RSVP-RESVt
|            |---------------------------------------------------->
|            |               |               |   RSVP-RESVo
|<-----------------------------------------------------------------
|            |               |               |   RSVP-RESVCONFo
|----------------------------------------------------------------->
|            |               |               |   RSVP-RESVCONFt
|<-----------------------------------------------------------------
|            |               |               |   200 OK
|<-------------------------------------------|<------------------
|            |               |               |   MEDIA
|<===============================================================>
|            |               |               |   ACK
|----------------------------------------------------------------->
```

Figure 1

The PDP-o stores the authorized Media description in its local store generates an Authorization-Token that points to this description and returns the Authorization-Token to OP.

The OP includes the Authorization-Token in the Media-Auth-Token header extension of the 183 message.

The UAC upon reception, stores the Media-Authorization-Token inside the Media-Auth-Token header extension.

Before sending the Media stream, the UAC requests bandwidth using RSVP-PATH message which includes the Session info that describes the Media data-stream and TSpec that describes the bandwidth requested along with Authorization information that was stored in Media-Authorization-Token.

ER-o, upon reception of the RSVP-PATHo message checks the authorization through a PDP-o COPS message exchange. The PDP-o checks the authorization using the stored authorized Media description that was linked to the Authorization-Token that it returned to OP. If authorization is successful PDP-o returns an "install" Decision.

ER-o checks the admissibility for the call and if admission succeeds, it forwards the RSVP-PATHo message.

Once the UAC receives the RSVP-PATHt message it sends RSVP-RESVt message to reserve the bandwidth.

ER-o, upon reception of the RSVP-RESVt message checks the authorization through PDP-o COPS message exchange. The PDP-o checks the authorization using the stored authorized Media description that was linked to Authorization-Token that it returned to OP. If authorization is successful PDP-o returns "install" Decision.

ER-o checks the admissibility for the call and if admission succeeds, it forwards the RSVP-RESVt message.

Upon reception of RSVP-RESVo message the UAC sends RSVP-RESVCONFo message to indicate that the reservation completed for one direction.

Upon reception of both RSVP-RESVCONFt and 200OK the UAC returns ACK message.

6.1.2. User Agent Server Side

Figure 2 presents a high-level overview of a call flow with Media Authorization from the viewpoint of the UAS. It is assumed that the SIP-Proxy has a previously established authentication relationship with the - UAS.


```
UAS         ER-t            PDP-t          DP
 |           |               |               | Invite
 |           |               |               |<--------------
 |           |               |               | Proxy Authentication
 |           |               | Auth. Profile | and Call Authorization
 |           |               |<--------------|
 |           |               |  Auth. Token  |
 |           |               |-------------->| Auth. Token put into
 |           |               |       Invite  | Media-Authorization header
 |<------------------------------------------| extension
 |   180/3   |               |               |
 |------------------------------------------>| 180/3
 |Copies the RSVP policy object              |-------------->
 |from the Media-Authorization               |
 | RSVP-PATHt|               |               |
 |---------->| REQ           |               |
 |           |-------------->| Using the Auth-Token and Authorized
 |           |          DEC  | Profile that is set by the SIP Proxy
```

```
 |           |<--------------| the PDP makes the decision
 |           |               |               |   RSVP-PATHt
 |           |-------------------------------------------------->
 |           |               |               |   RSVP-PATHo
 |<--------------------------------------------------------------
 |Copies the RSVP policy object              |
 |from the Media-Authorization               |
 | RSVP-RESVo|               |               |
 |---------->|               |               |
 |           | REQ           |               |
 |           |-------------->| Using the Auth-Token and Authorized
 |           |         DEC   | Profile that is set by the SIP Proxy
 |           |<--------------| the PDP makes the decision
 |           |               |               |   RSVP-RESVo
 |           |--------------------------------------------------->
 |           |               |               |   RSVP-RESVt
 |<---------------------------------------------------------------
 |           |               |               |   RSVP-RESVCONFt
 |--------------------------------------------------------------->
 |           |               |               |   RSVP-RESVCONFo
 |<---------------------------------------------------------------
 |           |               |               |   200 OK
 |-----------------------------------------> |------------------->
 |           |               |               |   ACK
 |<----------------------------------------------------------------
```

Figure 2

Since Destination SIP-Proxy (DP)has sufficient information regarding the end-points, bandwidth and characteristics of the media exchange. It initiates a Policy-Setup message to the termination Policy Decision Point (PDP-t).

The PDP-t stores the authorized Media description in its local store generates an Authorization-Token that points to this description and returns the Authorization-Token to DP.

Assuming that the call is not forwarded, the UAS sends a 183 response to the initial INVITE message, which is forwarded back to UAC. At the same time UAS sends RSVP-PATHt message for Media data-stream that includes the Session info that describes the Media data-stream and TSpec that describes the bandwidth requested along with Authorization information that was stored in Media-Authorization-Token.

ER-t upon reception of the RSVP-PATHt message checks the authorization through a PDP-t COPS message exchange. The PDP-t checks the authorization using the stored authorized Media description that was linked to Authorization-Token that it returned to DP. If authorization is successful PDP-t returns "install" Decision.

ER-t checks the admissibility for the call and if admission succeeds, it forwards the RSVP-PATHt message.

Once UAS receives the RSVP-PATHo message it sends RSVP-RESVo message to reserve the bandwidth.

ER-t upon reception of the RSVP-RESVo message checks the authorization through a PDP-t COPS message exchange. The PDP-t checks the authorization using the stored authorized Media description that was linked to Authorization-Token that it returned to DP. If authorization is successful PDP-t returns "install" Decision.

ER-t checks the admissibility for the call and if admission succeeds, it forwards the RSVP- RESVo message.

Upon reception of RSVP-RESVd message the UAS sends RSVP-RESVCONFt message to indicate that the reservation completed for one direction.

Upon reception of both RSVP-RESVCONFo and 200OK the UAS returns ACK message.

6.2. Requesting Bandwidth via DOCSIS MAC messaging

The DOCSIS MAC layer [5] QoS Set-Up the call flows are different in the sense that the Authorization token is a simple 32bit number [6]. And DSA-REQ, DSA-RSP, and DSA-ACK are layer 2 messages that are specific to and optimized for Cable environment which simplifies/reduces delays for the embedded client implementation [6].


```
UAC                 ER/CMTSo                  OP
|  Invite             |                        |
|-------------------------------------------->| Client Authentication
|                     |                        |and Call Authorization
|                     |                        |
|                     |                        | Invite
|                     |                        |----------->
|                     |                        |
|                     |                        | 180/3 OK
```

```
   |                    |                       |<------------
   |                    |                       |
   |                    |  Gate-Setup           |
   |                    |<--------------------- |
   |                    |       Gate-Setup-Ack  |
   |                    |---------------------> |
   |                    |                       | GateID put into
   |                    |                       | Media-Authorization header
   |                    |                       | extension
   |                    |       180/3 OK        |
   |<-------------------------------------------|
   |Copies the GAteID object                    |
   |from the Media-Authorization                |
   |                    |                       |
   | DSA-REQ            |                       |
   |------------------->|                       |
   |                    | Using the GateID and the Profile
   |                    | communicated during Gate-Setup
   |                    | the CMTS honors the request and creates
   | DSA-RSP            | a scheduler with appropriate settings
   |<-------------------|                       |
   |                    |                       |
   | DSA-ACK            |                       |
   |------------------->|                       |
   |                    |                       |
```

Figure 3

6.2.1. User Agent Client Side

Figure 3 presents a high-level overview of a call flow with Media Authorization from the viewpoint of UAC . It is assumed that the SIP-Proxy has a previously established authentication relationship with the client.

When a user goes off-hook and dials a telephone number, the originating SIP Client (UAC) collects the dialed digits and sends the initial INVITE message to Originating SIP-Proxy.

The Originating SIP-Proxy (OP) authenticates UAC and forwards the INVITE message to the proper destination SIP-proxy.

Assuming that the call is not forwarded, the other end-point sends a 183 response to the initial INVITE, forwarded back to OP. Included in this response is the negotiated bandwidth requirement for the connection.

UAS sends DSA-REQ message asking for bandwidth, which includes the 32 bit index value.

ER/CMTSo, upon reception of the RSA-REQ message uses the index value to find the authorized media description. Checks the requested media link against authorized if the both authorization and admission succeeds it starts a layer 2 link for Media data-stream on the Cable Access link and returns DSA-RSP, which is acknowledged by UAC via DSA-ACK message.

Upon reception of 200OK the UAS returns ACK message.

6.2.2. User Agent Server Side

Figure 4 presents a high-level overview of a basic call flow with Media Authorization from the viewpoint of UAS (UAS). It is assumed that the Destination SIP-Proxy (DP) has a previously established authentication relationship with the UAS.

When DP receives the INVITE message, it has sufficient information regarding the end-points, bandwidth and characteristics of the media exchange. It sends a Gate-Setup message to ER/CMTSt containing Media data-stream description and bandwidth characteristics. The ER/CMTSt returns a 32 bit index value that inside ER/CMTSt points to Media definition that DP send out.

The DP includes the 32 bit index value in the Media-Auth-Token header extension that its including into the INVITE message.

The UAS sends a 183 response to the initial INVITE, which is forwarded back to UAC. At the same time UAS sends DSA-REQ message asking for bandwidth which includes the 32 bit index value.

ER/CMTSt, upon reception of the RSA-REQ message uses the index value to find the authorized media description. Checks the requested media link against authorized if the both authorization and admission succeeds it starts a layer 2 link for Media data-stream on the Cable Access link and returns DSA-RSP, which is acknowledged by UAC via DSA-ACK message. Upon reception of DSA-RSP the UAS returns ACK message.

```
   UAS              ER/CMTSt                   DP
   |                    |                       |
   |                    |                       | Invite
   |                    |                       |<-----------
   |                    |                       | Proxy Authentication
   |                    |                       | and Call Authorization
   |                    |  Gate-Setup           |
   |                    |<----------------------|
   |                    |       Gate-Setup-Ack  |
   |                    |---------------------->|
   |                    |                       | GateID put into
   |                    |                       | Media-Authorization header
   |                    |                       | extension
   |  Invite            |                       |
   |<-------------------------------------------|
   |                    |                       |
   |                    |       180/3           |
   |------------------------------------------->|
   |                    |                       | 180/3
   |                    |                       |------------>
   |Copies the GateID object                    |
   |from the Media-Authorization                |
   |                    |                       |
   | DSA-REQ            |
   |------------------->|
   |                    | Using the GateID and the Profile
   |                    | communicated during Gate-Setup
   |                    | the CMTS honors the request and creates
   | DSA-RSP            | a scheduler with appropriate settings
   |<-------------------|
   |                    |
   | DSA-ACK            |                       |
   |------------------->|                       |
   |                    |                       |
   |                    |       200 OK          |
   |------------------------------------------->|
   |                    |                       | 200 OK
   |                    |                       |------------>
```

Figure 4

7. Advantages of the Proposed Approach

The use of call authorization makes it possible to control the utilization of network resources. This in turn makes IP Telephony more robust against denial of service attacks and various kinds of service frauds.

Using the authorization capability, the service provider can control the number of flows, the amount of bandwidth, and the end-point reached making the IP Telephony system dependable in the presence of scarce resources.

8. Security Considerations

Media Authorization Tokens sent from a SIP-Proxy to a UAC/UAS MUST be protected from eavesdropping, through a mechanism such as IPSec.

9. Notice Regarding Intellectual Property Rights

AT&T may seek patent or other intellectual property protection for some or all of the technologies disclosed in the document. If any standards arising from this disclosure are or become protected by one or more patents assigned to AT&T, AT&T intends to disclose those patents and license them on reasonable and non-discriminatory terms. Future revisions of this draft may contain additional information regarding specific intellectual property protection sought or received.

3COM may seek patent or other intellectual property protection for some or all of the technologies disclosed in the document. If any standards arising from this disclosure are or become protected by one or more patents assigned to 3COM, 3COM intends to disclose those patents and license them on reasonable and non-discriminatory terms. Future revisions of this draft may contain additional information regarding specific intellectual property protection sought or received.

10. Reference

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

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

3 Crocker, D. and Overell, P.(Editors), "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, Internet Mail Consortium and Demon Internet Ltd., November 1997

4 M. Handley, H. Schulzrinne, E. Schooler, and J. Rosenberg, "SIP: session initiation protocol,"Request for Comments (Proposed Standard) 2543, Internet Engineering Task Force, Mar. 1999.

5 CableLabs, "Data-Over-Cable Service Interface Specifications, Radio Frequency Interface Specification, SP-RFIv1.1-I04-000407", April 2000.

6 PacketCable, Dynamic Quality of Service Specification, pkt-sp-dqos-

i01-991201, December 1, 1999.

7 RFC 2210, The Use of RSVP with IETF Integrated Services by J. Wroclawski, September 1997.

11. Acknowledgments

The Distributed Call Signaling work in the PacketCable project is the work of a large number of people, representing many different companies. The authors would like to recognize and thank the following for their assistance: John Wheeler, Motorola; David Boardman, Daniel Paul, Arris Interactive; Bill Blum, Jon Fellows, Jay Strater, Jeff Ollis, Clive Holborow, Motorola; Doug Newlin, Guido Schuster, Ikhlaq Sidhu, 3Com; Jiri Matousek, Bay Networks; Farzi Khazai, Nortel; John Chapman, Bill Guckel, Michael Ramalho, Cisco; Chuck Kalmanek, Doug Nortz, John Lawser, James Cheng, Tung-Hai Hsiao, Partho Mishra, AT&T; Telcordia Technologies; and Lucent Cable Communications.

13. Author's Addresses

Bill Marshall
AT&T
Florham Park, NJ 07932
Email: wtm@research.att.com

K. K. Ramakrishnan
AT&T
Florham Park, NJ 07932
Email: kkrama@research.att.com

Ed Miller
CableLabs
Louisville, CO 80027
Email: E.Miller@Cablelabs.com

Glenn Russell
CableLabs
Louisville, CO 80027
Email: G.Russell@Cablelabs.com

Burcak Beser
3Com
Mount Prospect, IL 60004
Email: Burcak_Beser@3com.com

Mike Mannette
3Com
Rolling Meadows, IL 60008
Email: Michael_Mannette@3com.com

Kurt Steinbrenner
3Com
Rolling Meadows, IL 60008
Email: Kurt_Steinbrenner@3com.com

Dave Oran
Cisco
Acton, MA 01720
Email: oran@cisco.com

Flemming Andreasen
Cisco
Edison, NJ
Email: fandreas@cisco.com

John Pickens
Com21
San Jose, CA
Email: jpickens@com21.com

Poornima Lalwaney
Nokia
San Diego, CA 92121
Email: poornima.lalwaney@nokia.com

Jon Fellows
Motorola
San Diego, CA 92121
Email: jfellows@gi.com

Doc Evans
Secure Cable Solutions
Westminster, CO 30120
Email: drevans@securecable.com

Keith Kelly
NetSpeak
Boca Raton, FL 33587
Email: keith@netspeak.com

Full Copyright Statement

Expiration Date This memo is filed as <draft-dcsgroup-sip-call-auth-02.txt>, and expires December 31, 2000.