Network Working Group   James Polk
Internet Draft   Cisco Systems
Expires: Mar 4, 2012   Brian Rosen
Intended Status: Standards Track (PS)   Jon Peterson
                                                        NeuStar
                                                   Sept 4, 2011

         Location Conveyance for the Session Initiation Protocol
              draft-ietf-sipcore-location-conveyance-09.txt

Abstract

   This document defines an extension to the Session Initiation
   Protocol (SIP) to convey geographic location information from one
   SIP entity to another SIP entity. The SIP extension covers
   end-to-end conveyance as well as location-based routing, where SIP
   intermediaries make routing decisions based upon the location of the
   Location Target.

Status of this Memo

   This Internet-Draft is submitted to IETF in full conformance with
   the provisions of BCP 78 and BCP 79.

   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.

   This Internet-Draft will expire on Mar 4, 2012.

Copyright Notice

Table of Contents

Polk, et al.   Expires Mar 4, 2012   [Page 2]

[1].   Conventions and Terminology 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 [RFC2119]. This document furthermore uses numerous terms defined
   in RFC 3693 [RFC3693], including Location Object, Location
   Recipient, Location Server, Target, Rulemaker and Using Protocol.

[2].   Introduction

   Session Initiation Protocol (SIP) [RFC3261] creates, modifies and
   terminates multimedia sessions. SIP carries certain information
   related to a session while establishing or maintaining calls. This
   document defines how SIP conveys geographic location information of
   a Target to a Location Recipient (LR). SIP acts as a Using Protocol
   of location information, as defined in RFC 3693.

   In order to convey location information, this document specifies
   three new SIP header fields, Geolocation, Geolocation-Routing and
   Geolocation-Error, which carry a reference to a Location Object
   (LO), grant permission to route a SIP request based on the
   location-value and provide error notifications specific to location
   errors respectively. The Location Object (LO) may appear in a MIME
   body attached to the SIP request, or it may be a remote resource in

the network.

A Target is an entity whose location is being conveyed, per [RFC 3693](). Thus, a Target could be a SIP user agent (UA), some other IP device (a router or a PC) that does not have a SIP stack, a non-IP device (a person or a black phone) or even a non-communications device (a building or store front). In no way does this document assume that the SIP user agent client which sends a request containing a location object is necessarily the Target. The location of a Target conveyed within SIP typically corresponds to that of a device controlled by the Target, for example, a mobile phone, but such devices can be separated from their owners, and moreover, in some cases the user agent may not know its own location.

In the SIP context, a location recipient will most likely be a SIP UA, but due to the mediated nature of SIP architectures, location information conveyed by a single SIP request may have multiple recipients, as any SIP proxy server in the signaling path that inspects the location of the Target must also be considered a Location Recipient. In presence-like architectures, an intermediary

that receives publications of location information and distributes them to watchers acts as a Location Server per [RFC 3693](). This location conveyance mechanism can also be used to deliver URIs pointing to such Location Servers where prospective Location Recipients can request Location Objects.

[3](). Overview of SIP Location Conveyance

An operational overview of SIP location conveyance can be shown in 4 basic diagrams, with most applications falling under one of the following basic use cases. Each is separated into its own subsection here in [section 3]().

Each diagram has Alice and Bob as UAs. Alice is the Target, and Bob is an LR. A SIP intermediary appears in some of the diagrams. Any SIP entity that receives and inspects location information is an LR, therefore in any of the diagrams the SIP intermediary that receives a SIP request is potentially an LR - though that does not mean such an intermediary necessarily has to route the SIP request based on the location information. In some use cases, location information passes through the LS on the right of each diagram.

Location Conveyed by Value

   We start with the simplest diagram of Location Conveyance, Alice to
   Bob, where no other layer 7 entities are involved.

```
      Alice            SIP Intermediary        Bob                 LS
        |                    |                  |                   |
        |          Request w/Location           |                   |
        |-------------------------------------->|                   |
        |                    |                  |                   |
        |               Response                |                   |
        |<--------------------------------------|                   |
        |                    |                  |                   |
```
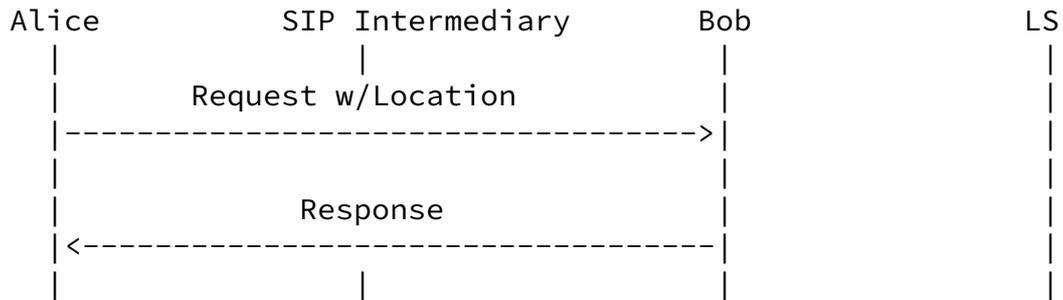
        Figure 1. Location Conveyed by Value

   In Figure 1, Alice is both the Target and the LS that is conveying
   her location directly to Bob, who acts as an LR. This conveyance is
   point-to-point - it does not pass through any SIP-layer
   intermediary. A Location Object appears by-value in the initial SIP
   request as a MIME body, and Bob responds to that SIP request as
   appropriate. There is a 'Bad Location Information' response code
   introduced within this document to specifically inform Alice if she
   conveys bad location to Bob (e.g., Bob "cannot parse the location
   provided", or "there is not enough location information to determine
   where Alice is").

Location Conveyed as a Location URI

   Here we make Figure 1 a little more complicated by showing a
   diagram of indirect Location Conveyance from Alice to Bob, where
   Bob's entity has to retrieve the location object from a 3rd party
   server.

```
      Alice            SIP Intermediary        Bob                 LS
        |                    |                  |                   |
        |        Request w/Location URI         |                   |
        |-------------------------------------->|                   |
        |                                       |      Dereference  |
        |                                       |        Request    |
```

```
        |                                       (To: Location URI) |
        |                                   |---------------->|
        |                                   |                 |
        |                                   |    Dereference  |
        |                                   |      Response   |
        |                                   (includes location) |
        |                                   |<----------------|
        |             Response              |                 |
        |<----------------------------------|                 |
        |              |                     |                 |
```
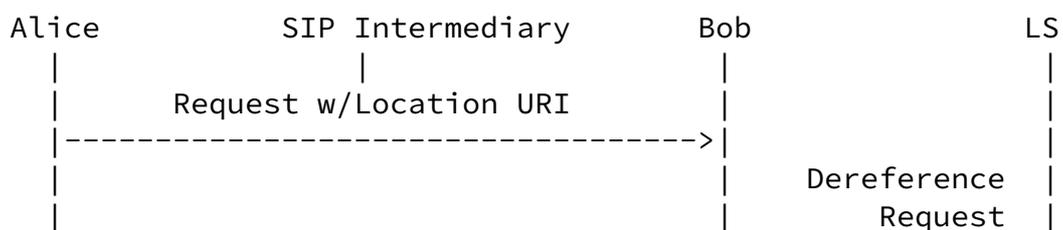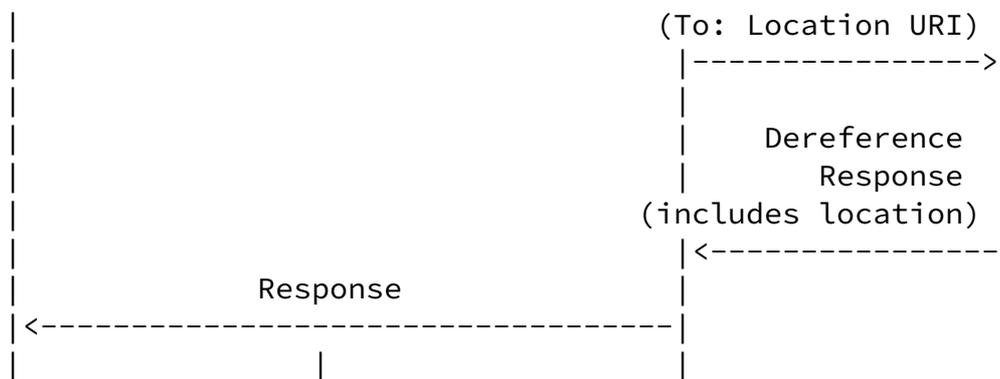
             Figure 2. Location Conveyed as a Location URI

   In Figure 2, location is conveyed indirectly, via a Location URI
   carried in the SIP request (more of those details later). If Alice
   sends Bob this Location URI, Bob will need to dereference the URI –
   analogous to Content Indirection [RFC4483] – in order to request the
   location information. In general, the LS provides the location value
   to Bob instead of Alice directly for conveyance to Bob. From a user
   interface perspective, Bob the user won't know that this information
   was gathered from an LS indirectly rather than culled from the SIP
   request, and practically this does not impact the operation of
   location-based applications.

   The example given in this section is only illustrative, not
   normative. In particular, applications can choose to dereference a
   location URI at any time, possibly several times, or potentially not
   at all. Applications receiving a Location URI in a SIP transaction
   need to be mindful of timers used by different transactions. In
   particular, if the means of dereferencing the Location URI might
   take longer than the SIP transaction timeout (Timer C for INVITE
   transactions, Timer F for non-INVITE transactions), then it needs to
   rely on mechanisms other than the transaction's response code to
   convey location errors, if returning such errors are necessary.

3.3 Location Conveyed though a SIP Intermediary

   In Figure 3, we introduce the idea of a SIP intermediary into the
   example to illustrate the role of proxying in the location
   architecture. This intermediary can be a SIP proxy or it can be
   a back-to-back-user-agent (B2BUA). In this message flow, the SIP
   intermediary could act as a LR, in addition to Bob. The primary use

case for intermediaries consuming location information is
location-based routing. In this case, the intermediary chooses a
next hop for the SIP request by consulting a specialized location
service which selects forwarding destinations based on geographical
location.

```
    Alice              SIP Intermediary        Bob               LS
     |                     |                     |                 |
     |    Request          |                     |                 |
     |     w/Location      |                     |                 |
     |--------------->|                     |                 |
     |                     |    Request          |                 |
     |                     |     w/Location      |                 |
     |                     |----------------->|                 |
     |                     |                     |                 |
     |                     |    Response         |                 |
     |                     |<-----------------|                 |
     |     Response        |                     |                 |
     |<--------------|                     |                 |
     |                     |                     |                 |
```
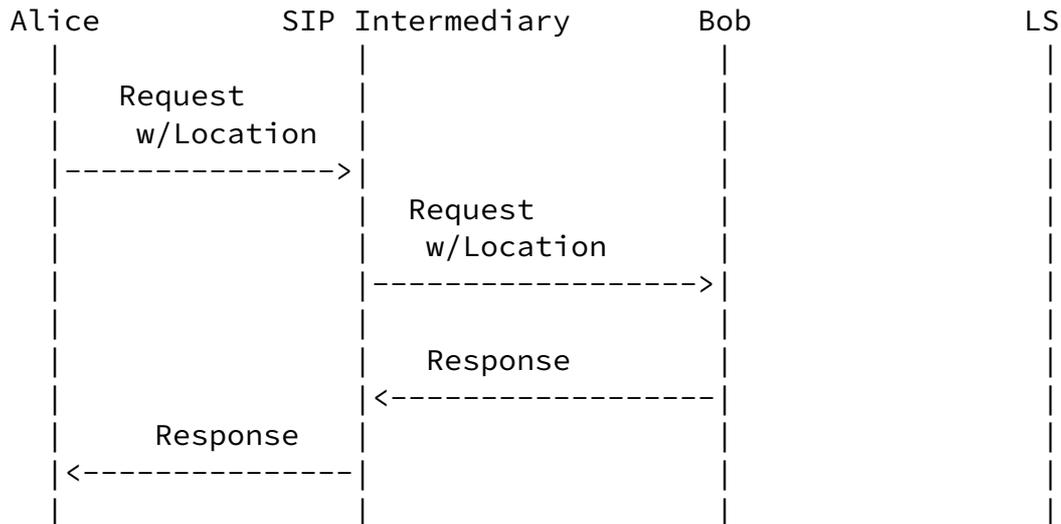
         Figure 3. Location Conveyed though a SIP Intermediary

   However, the most common case will be one in which the SIP
   intermediary receives a request with location information (conveyed
   either by-value or by-reference) and does not know or care about
   Alice's location, or support this extension, and merely passes it on
   to Bob. In this case, the intermediary does not act as a Location
   Recipient. When the intermediary is not an LR, this use case is the
   same as the one described in Section 3.1.

   Note that an intermediary does not have to perform location-based
   routing in order to be a Location Recipient. It could be the case
   that a SIP intermediary which does not perform location-based
   routing does care when Alice includes her location; for example,
   it could care that the location information is complete or that it
   correctly identifies where Alice is. The best example of this is
   intermediaries that verify location information for emergency
   calling, but it could also be for any location based routing - e.g.,
   contacting your favorite local pizza delivery service, making sure
 that organization has Alice's proper location in the initial SIP
 request.

   There is another scenario in which the SIP intermediary cares about
   location and is not an LR, one in which the intermediary inserts
   another location of the Target, Alice in this case, into the
   request, and forwards it. This secondary insertion is generally not

advisable because downstream SIP entities will not be given any
guidance about which location to believe is better, more reliable,
less prone to error, more granular, worse than the other location or
just plain wrong.

This document takes a "you break it, you bought it" approach to
dealing with second locations placed into a SIP request by an
intermediary entity. That entity becomes completely responsible for
all location within that SIP request (more on this in Section 4).

3.4 SIP Intermediary Replacing Bad Location

If the SIP intermediary rejects the message due to unsuitable
location information, the SIP response will indicate there was 'Bad
Location Information' in the SIP request, and provide a location
specific error code indicating what Alice needs to do to send an
acceptable request (see Figure 4 for this scenario).

```
    Alice              SIP Intermediary       Bob              LS
     |                 |                       |                |
     |    Request      |                       |                |
     |     w/Location  |                       |                |
     |--------------->|                        |                |
     |                 |                       |                |
     |    Rejected     |                       |                |
     | w/New Location  |                       |                |
     |<---------------|                        |                |
     |                 |                       |                |
     |    Request      |                       |                |
     | w/New Location  |                       |                |
     |--------------->|                        |                |
     |                 |    Request            |                |
     |                 |   w/New Location      |                |
     |                 |------------------->|                   |
     |                 |                       |                |
```
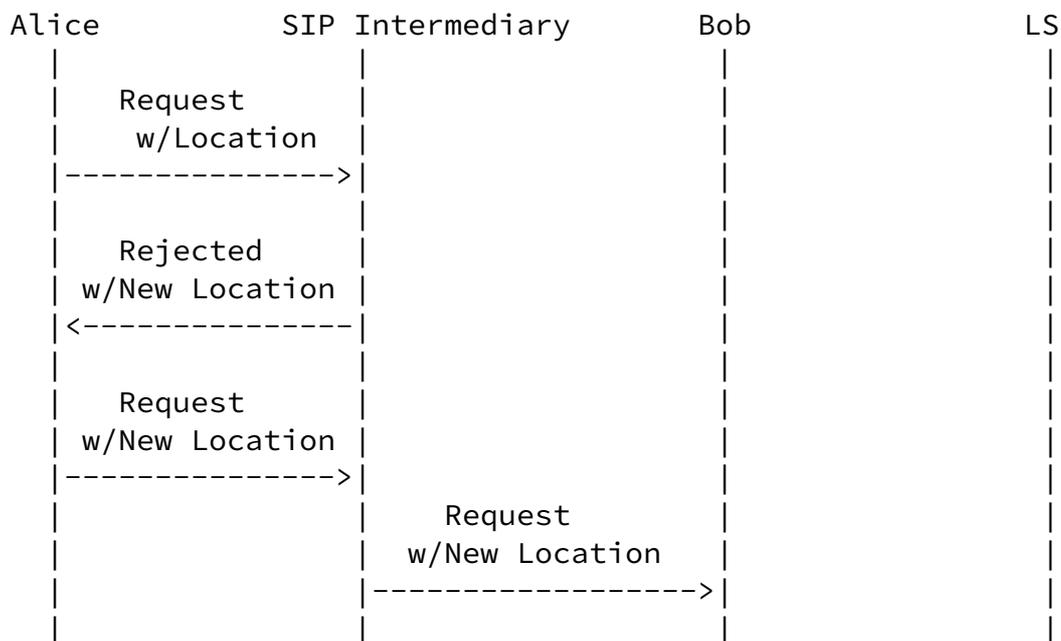
              Figure 4. SIP Intermediary Replacing Bad Location

In this last use case, the SIP intermediary wishes to include a
Location Object indicating where it understands Alice to be. Thus,
it needs to inform her user agent what location it will include in
any subsequent SIP request that contains her location. In this
case, the intermediary can reject Alice's request and, through the
SIP response, convey to her the best way to repair the request in
order for the intermediary to accept it.

Overriding location information provided by the user requires a

deployment where an intermediary necessarily knows better than an
end user - after all, it could be that Alice has an on-board GPS,
and the SIP intermediary only knows her nearest cell tower. Which is
more accurate location information? Currently, there is no way to

tell which entity is more accurate, or which is wrong - for that
matter. This document will not specify how to indicate which
location is more accurate than another.

As an aside, it is not envisioned that any SIP-based emergency
services request (i.e., IP-911, or 112 type of call attempt) will
receive a corrective 'Bad Location Information' response from an
intermediary. Most likely, the SIP intermediary would in that
scenario act as a B2BUA and insert into the request by-value any
appropriate location information for the benefit of Public Safety
Answering Point (PSAP) call centers to expedite call reception by
the emergency services personnel; thereby, minimizing any delay in
call establishment time. The implementation of these specialized
deployments is, however, outside the scope of this document.

4.   SIP Extensions for Geolocation Conveyance

   The following sections detail the extensions to SIP for location
   conveyance.

4.1 The Geolocation Header Field

   This document defines "Geolocation" as a new SIP header field
   registered by IANA, with the following ABNF [RFC5234]:

   message-header   /= Geolocation-header ; (message-header from 3261)
   Geolocation-header = "Geolocation" HCOLON locationValue
                        *(COMMA locationValue)
   locationValue   = LAQUOT locationURI RAQUOT
                         *(SEMI geoloc-param)
   locationURI   = sip-URI / sips-URI / pres-URI
                         / http-URI / https-URI
                         / cid-url ; (from RFC 2392)
                         / absoluteURI ; (from RFC 3261)
   geoloc-param   = generic-param; (from RFC 3261)

   HCOLON, COMMA, LAQUOT, RAQUOT, and SEMI are defined in RFC3261
   [RFC3261].

sip-URI, sips-URI and absoluteURI are defined according to [RFC3261].

The pres-URI is defined in [RFC3859].

http-URI and https-URI are defined according to [RFC2616] and [RFC2818], respectively.

The cid-url is defined in [RFC2392] to locate message body parts. This URI type is present in a SIP request when location is conveyed as a MIME body in the SIP message.

GEO-URIs [RFC5870] are not appropriate for usage in the SIP

Geolocation header, because it does not include retention and re-transmission flags as part of the location information. Other URI schemes used in the location URI MUST be reviewed against the RFC 3693 [RFC3693] criteria for a Using Protocol. Section 4.6 discusses how URI schemes are communicated using this SIP extension, and what to do if a URI scheme is received that cannot be supported.

The generic-param in the definition of locationValue is included as a mechanism for future extensions that might require parameters. This document defines no parameters for use with locationValue. If a Geolocation header field is received that contains generic-params, each parameter SHOULD be ignored, and SHOULD NOT be removed when forwarding the locationValue. If a need arises to define parameters for use with locationValue, a revision/extension to this document is required.

The Geolocation header field MUST have at least one locationValue. A SIP intermediary SHOULD NOT add location to a SIP request that already contains location. This will quite often lead to confusion within LRs. However, if a SIP intermediary adds location, even if location was not previously present in a SIP request, that SIP intermediary is fully responsible for addressing the concerns of any 424 (Bad Location Information) SIP response it receives about this location addition, and MUST NOT pass on (upstream) the 424 response. A SIP intermediary that adds a locationValue MUST position the new locationValue as the last locationValue within the Geolocation header field of the SIP request.

This document defines the Geolocation header field as valid in the following SIP requests:

```
    INVITE [RFC3261],              REGISTER [RFC3261],
    OPTIONS [RFC3261],             BYE [RFC3261],
    UPDATE [RFC3311],              INFO [RFC6086],
    MESSAGE [RFC3428],             REFER [RFC3515],
    SUBSCRIBE [RFC3265],           NOTIFY [RFC3265],
    PUBLISH [RFC3903]
```

The Geolocation header field MAY be included in any one of the
above listed requests by a UA, and a 424 response to any one of the
requests sent above. Fully appreciating the caveats/warnings
mentioned above, a SIP intermediary MAY add the Geolocation header
field.

A SIP intermediary MAY add a Geolocation header field if one is not
present - for example, when a user agent does not support the
Geolocation mechanism but their outbound proxy does and knows the
Target's location, or any of a number of other use cases (see
Section 3).

The Geolocation header field MAY be present in a SIP request or
response without the presence of a Geolocation-Routing header

(defined in Section 4.2). As stated in Section 4.2, the default
value of Geolocation-Routing header-value is "no", meaning SIP
intermediaries MUST NOT view (i.e., process, inspect or actively
dereference) any direct or indirect location within this SIP
message. This is for at least two fundamental reasons,

    1) to make the possibility of retention of the Target's location
       moot (because it was not viewed in the first place); and

    2) to prevent a different treatment of this SIP request based on
       the contents of the Location Information in the SIP request.

Any locationValue MUST be related to the original Target. This is
equally true for the location information in a SIP response, i.e.,
from a SIP intermediary back to the Target as explained in Section
3.4. SIP intermediaries SHOULD NOT modify or delete any existing
locationValue(s). A use-case in which this would not apply would be
where the SIP intermediary is an anonymizer. The problem with this
scenario is that the geolocation included by the Target then becomes
useless for the purpose or service they wanted to use (include) it
for. For example, 911/emergency calling or finding the nearest

(towing company/pizza delivery/dry cleaning) service(s) will not
yield intended results if the Location Information were to be
modified or deleted from the SIP request.

4.2 The Geolocation-Routing Header Field

   This document defines "Geolocation-Routing" as a new SIP header
   field registered by IANA, with the following ABNF [RFC5234]:

   message-header   /= Georouting-header ; (message-header from 3261)
   Georouting-header = "Geolocation-Routing" HCOLON
                         ("yes" / "no" / generic-value)
   generic-value   = generic-param; (from RFC 3261)

   HCOLON is defined in RFC3261 [RFC3261].

   The only defined values for the Geolocation-Routing header field are
   "yes" or "no". When the value is "yes", the locationValue can be
   used for routing decisions along the downstream signaling path by
   intermediaries. Values other than "yes" or "no" are permitted for
   future extensions. Implementations not aware of an extension MUST
   treat any other received value the same as "no".

   If no Geolocation-Routing header field is present in a SIP request,
   a SIP intermediary MAY insert this header. Without knowledge from a
   Rulemaker, the SIP intermediary inserting this header-value SHOULD
   NOT set the value to "yes", as this may be more permissive than the
   originating party intends. An easy way around this is to have the
   Target always insert this header-value as "no".

   When this Geolocation-Routing header-value is set to "no", this
   means no locationValue (inserted by the originating UAC or any
   intermediary along the signaling path) can be used by any SIP
   intermediary to make routing decisions. Intermediaries that attempt
   to use the location information for routing purposes in spite of
   this counter indication could end up routing the request improperly
   as a result. Section 4.4 describes the details on what a routing
   intermediary does if it determines it needs to use the location in
   the SIP request in order to process the message further. The
   practical implication is that when the Geolocation-Routing
   header-value is set to "no", if a cid:url is present in the SIP
   request, intermediaries MUST NOT view the location (because it is

not for intermediaries to consider when processing the request), and
if a location URI is present, intermediaries MUST NOT dereference
it. UAs are allowed to view location in the SIP request even when
the Geolocation-Routing header-value is set to "no". An LR MUST by
default consider the Geolocation-Routing header-value as set to
"no", with no exceptions, unless the header field value is set to
"yes".

A Geolocation-Routing header-value that is set to "no" has no
special security properties. It is at most a request for behavior
within SIP intermediaries. That said, if the Geolocation-Routing
header-value is set to "no", SIP intermediaries are still to process
the SIP request and send it further downstream within the signaling
path if there are no errors present in this SIP request.

The Geolocation-Routing header field satisfies the recommendations
made in [section 3.5 of RFC 5606](#) [[RFC5606](#)] regarding indication of
permission to use location-based routing in SIP.

SIP implementations are advised to pay special attention to the
policy elements for location retransmission and retention described
in [RFC 4119](#).

The Geolocation-Routing header field cannot appear without a
header-value in a SIP request or response (i.e., a null value is not
allowed). The absence of a Geolocation-Routing header-value in a SIP
request is always the same as the following header field:

    Geolocation-Routing: no

The Geolocation-Routing header field MAY be present without a
Geolocation header field in the same SIP request. This concept is
further explored in [Section 4.2.1](#).

4.2.1 Explaining Geolocation-Routing header-value States

   The Geolocation header field contains a Target's location, and MUST
   NOT be present if there is no location information in this SIP
   request. The location information is contained in one or more

   locationValues. These locationValues MAY be contained in a single
   Geolocation header field, or distributed among multiple Geolocation
   header fields. (See [section 7.3.1 of RFC3261](#).)

The Geolocation-Routing header field indicates whether or not SIP
intermediaries can view and then route this SIP request based on the
included (directly or indirectly) location information. The
Geolocation-Routing header field MUST NOT appear more than once in
any SIP request, and MUST NOT lack a header-value. The default or
implied policy of a SIP request that does not have a
Geolocation-Routing header field is the same as if one were present
and the header-value were set to "no".

There are only 3 possible states regarding the Geolocation-Routing
header field

- "no"
- "yes"
- no header-field present in this SIP request

The expected results in each state are:

If the Geolocation-Routing	Only possible interpretations:
"no"	SIP intermediaries MUST NOT process included geolocation information within this SIP request.
	SIP intermediaries inserting a locationValue into a Geolocation header field (whether adding to an existing header-value or inserting the Geolocation header field for the first time) MUST NOT modify or delete the received "no" header-value.
"yes"	SIP intermediaries can process included geolocation information within this SIP request, and can change the policy to "no" for intermediaries further downstream.
Geolocation-Routing absent	If a Geolocation header field exists (meaning a locationValue is already present), a SIP intermediary MUST interpret the lack of a Geolocation-Routing header field as if there were one present and the header-value is set to "no".

If there is no Geolocation header
field in this SIP request, the default
Geolocation-Routing is open and can be
set by a SIP intermediary or not at
all.

4.3 424 (Bad Location Information) Response Code

   This SIP extension creates a new location-specific response code,
   defined as follows,

      424 (Bad Location Information)

   The 424 (Bad Location Information) response code is a rejection of
   the request due to its location contents, indicating location
   information that was malformed or not satisfactory for the
   recipient's purpose, or could not be dereferenced.

   A SIP intermediary can also reject a location it receives from a
   Target when it understands the Target to be in a different location.
   The proper handling of this scenario, described in Section 3.4, is
   for the SIP intermediary to include the proper location in the 424
   Response. This SHOULD be included in the response as a MIME message
   body (i.e., a location value), rather than as a URI; however, in
   cases where the intermediary is willing to share location with
   recipients but not with a user agent, a reference might be
   necessary.

   As mentioned in Section 3.4, it might be the case that the
   intermediary does not want to chance providing less accurate
   location information than the user agent; thus it will compose its
   understanding of where the user agent is in a separate <geopriv>
   element of the same PIDF-LO [RFC4119] message body in the SIP
   response (which also contains the Target's version of where it is).
   Therefore, both locations are included - each with different
   <method> elements. The proper reaction of the user agent is to
   generate a new SIP request that includes this composed location
   object, and send it towards the original LR. SIP intermediaries can
   verify that subsequent requests properly insert the suggested
   location information before forwarding said requests.

   SIP intermediaries that are forwarding (as opposed to generating) a
   424 response MUST NOT add, modify, or delete any location appearing

in that response. This specifically applies to intermediaries that
are between the 424 response generator and the original UAC.
Geolocation and Geolocation-Error header fields and PIDF-LO body
parts MUST remain unchanged, never added to or deleted.

Section 4.4 describes a Geolocation-Error header field to provide
more detail about what was wrong with the location information in
the request. This header field MUST be included in the 424 response.

It is only appropriate to generate a 424 response when the
responding entity needs a locationValue and there are no values in
the request that are usable by the responder, or when the responder
has additional location information to provide. The latter case is
shown in Figure 4 of section 3.4. There, a SIP intermediary is
informing the upstream UA which location to include in the next SIP
request.

A 424 MUST NOT be sent in response to a request that lacks a
Geolocation header entirely, as the user agent in that case may not
support this extension at all. If a SIP intermediary inserted a
locationValue into a SIP request where one was not previously
present, it MUST take any and all responsibility for the corrective
action if it receives a 424 to a SIP request it sent.

A 424 (Bad Location Information) response is a final response within
a transaction, and MUST NOT terminate an existing dialog.

4.4 The Geolocation-Error Header Field

As discussed in Section 4.3, more granular error notifications
specific to location errors within a received request are required
if the location inserting entity is to know what was wrong within
the original request. The Geolocation-Error header field is used for
this purpose.

The Geolocation-Error header field is used to convey
location-specific errors within a response. The Geolocation-Error
header field has the following ABNF [RFC5234]:

    message-header   /= Geolocation-Error
                               ; (message-header from 3261)

```
Geolocation-Error         = "Geolocation-Error" HCOLON
                              locationErrorValue
locationErrorValue        = location-error-code
                             *(SEMI location-error-params)
location-error-code       = 1*3DIGIT
location-error-params     = location-error-code-text
                            / generic-param ; from RFC3261
location-error-code-text = "code" EQUAL quoted-string ; from RFC3261
```

HCOLON, SEMI, and EQUAL are defined in RFC3261 [RFC3261]. DIGIT is defined in RFC5234 [RFC5234].

The Geolocation-Error header field MUST contain only one locationErrorValue to indicate what was wrong with the locationValue the Location Recipient determined was bad. The locationErrorValue contains a 3-digit error code indicating what was wrong with the

location in the request. This error code has a corresponding quoted error text string that is human understandable. The text string is OPTIONAL, but RECOMMENDED for human readability, similar to the string phrase used for SIP response codes. That said, the strings are complete enough for rendering to the user, if so desired. The strings in this document are recommendations, and are not standardized - meaning an operator can change the strings - but MUST NOT change the meaning of the error code. Similar to how RFC 3261 specifies, there MUST NOT be more than one string per error code.

The Geolocation-Error header field MAY be included in any response to one of the SIP Methods mentioned in Section 4.1, so long as a locationValue was in the request part of the same transaction. For example, Alice includes her location in an INVITE to Bob. Bob can accept this INVITE, thus creating a dialog, even though his UA determined the location contained in the INVITE was bad. Bob merely includes a Geolocation-Error header value in the 200 OK to the INVITE informing Alice the INVITE was accepted but the location provided was bad.

If, on the other hand, Bob cannot accept Alice's INVITE without a suitable location, a 424 (Bad Location Information) is sent. This message flow is shown in Figures 1, 2 or 3 in Sections 3.1, 3.2 and 3.3 respectively.

If Alice is deliberately leaving location information out of the LO

because she does not want Bob to have this additional information,
implementations should be aware that Bob could error repeatedly in
order to receive more location information about Alice in a
subsequent SIP request. Implementations MUST be on guard for this,
by not allowing continually more information to be revealed unless
it is clear that any LR is permitted by Alice to know all that Alice
knows about her location. A limit on the number of such rejections
to learn more location information SHOULD be configurable, with a
RECOMMENDED maximum of 3 times for each related transaction.

A SIP intermediary that requires Alice's location in order to
properly process Alice's INVITE also sends a 424 with a
Geolocation-Error code. This message flow is shown in Figure 4 of
[Section 3.4](#).

If more than one locationValue is present in a SIP request and at
least one locationValue is determined to be valid by the LR, the
location in that SIP request MUST be considered good as far as
location is concerned, and no Geolocation-Error is to be sent.

Here is an initial list of location based error code ranges for any
SIP response, including provisional responses (other than 100
Trying) and the new 424 (Bad Location Information) response. These
error codes are divided into 3 categories, based on how the response
receiver should react to these errors. There MUST be no more than
one Geolocation-Error code in a SIP response, regardless of how many

locationValues there are in the correlating SIP request. There is no
guidance given in this document as to which locationValue, when more
than one was present in the SIP request, is related to the
Geolocation-Error code; meaning that, somehow not defined here, the
LR just picks one to error.

o 1XX errors mean the LR cannot process the location within the
   request

   A non-exclusive list of reasons for returning a 1XX is

   - the location was not present or could not be found,
   - there was not enough location information to determine
     where the Target was,
   - the location information was corrupted or known to be
     inaccurate,

o 2XX errors mean some specific permission is necessary to process
      the included location information.

   o 3XX errors mean there was trouble dereferencing the Location URI
      sent.

   Dereference attempts to the same request SHOULD be limited to 10
   attempts within a few minutes. This number SHOULD be configurable,
   but result in a Geolocation-Error: 300 error once reached.

   It should be noted that for non-INVITE transactions, the SIP
   response will likely be sent before the dereference response has
   been received. This document does not alter that SIP protocol
   reality. This means the receiver of any non-INVITE response to a
   request containing location SHOULD NOT consider a 200 OK to mean the
   act of dereferencing has concluded and the dereferencer (i.e., the
   LR) has successfully received and parsed the PIDF-LO for errors and
   found none. The end of [section 3.2](#) discusses how transaction timing
   considerations lead to this requirement.

   Additionally, if an LR cannot or chooses not to process location
   from a SIP request, a 500 (Server Internal Error) SHOULD be used
   with or without a configurable Retry-After header field. There is no
   special location error code for what already exists within SIP
   today.

   Within each of these ranges, there is a top level error as follows:

   Geolocation-Error: 100 ; code="Cannot Process Location"

   Geolocation-Error: 200 ; code="Permission To Use Location
                                  Information"

   Geolocation-Error: 300 ; code="Dereference Failure"

   If an error recipient cannot process a specific error code (such as
   the 201 or 202 below), perhaps because it does not understand that
   specific error code, the error recipient SHOULD process the error
   code as if it originally were a top level error code where the X in
   X00 matches the specific error code. If the error recipient cannot
   process a non-100 error code, for whatever reason, then the error
   code 100 MUST be processed.

There are two specific Geolocation-Error codes necessary to include
in this document, both have to do with permissions necessary to
process the SIP request; they are

     Geolocation-Error: 201 ; code="Permission To Retransmit Location
                                   Information to a Third Party"

This location error is specific to having the Presence Information
Data Format (PIDF-LO) [RFC4119] <retransmission-allowed> element set
to "no". This location error is stating it requires permission
(i.e., PIDF-LO <retransmission-allowed> element set to "yes") to
process this SIP request further. If the LS sending the location
information does not want to give this permission, it will not
change this permission in a new request. If the LS wants this
message processed with the <retransmission-allowed> element set to
"yes" it MUST choose another logical path (if one exists) for this
SIP request.

     Geolocation-Error: 202 ; code="Permission to Route based on Location
                                   Information"

This location error is specific to having the Geolocation-Routing
header value set to "no". This location error is stating it requires
permission (i.e., the Geolocation-Routing header value set to "yes")
to process this SIP request further. If the LS sending the location
information does not want to give this permission, it will not
change this permission in a new request. If the LS wants this
message processed with the <retransmission-allowed> element set to
"yes" it MUST choose another logical path (if one exists) for this
SIP request.

4.5 Location URIs in Message Bodies

In the case where an LR sends a 424 response and wishes to
communicate suitable location by reference rather than by value, the
424 MUST include a content-indirection body per RFC 4483.

4.6 Location Profile Negotiation

The following is part of the discussion started in Section 3, Figure
2, which introduced the concept of sending location indirectly.

If a location URI is included in a SIP request, the sending user
agent MUST also include a Supported header field indicating which
location profiles it supports. Two option tags for location profiles
are defined by this document: "geolocation-sip" and
"geolocation-http". Future specifications MAY define further
location profiles per the IANA policy described in [Section 8.3](#).

The "geolocation-sip" option tag signals support for acquiring
location information via the presence event package of SIP
([RFC3856]). A location recipient who supports this option can send
a SUBSCRIBE request and parse a resulting NOTIFY containing a
PIDF-LO object. The URI schemes supported by this option include
"sip", "sips" and "pres".

The "geolocation-http" option tag signals support for acquiring
location information via an HTTP ([RFC2616]). A location recipient
who supports this option can request location with an HTTP GET and
parse a resulting 200 response containing a PIDF-LO object. The URI
schemes supported by this option include "http" and "https". A
failure to parse the 200 response, for whatever reason, will return
a "Dereference Failure" indication to the original location sending
user agent to inform it that location was not delivered as intended.

If the location URI receiver does not understand the URI scheme sent
to it, it will return an Unsupported header value of the option-tag
from the SIP request, and include the option-tag of the preferred
URI scheme in the response's Supported header field.

See [ID-GEO-FILTERS] or [ID-HELD-DEREF] for more details on
dereferencing location information.

5. Geolocation Examples

5.1 Location-by-value (in Coordinate Format)

   This example shows an INVITE message with a coordinate location. In
   this example, the SIP request uses a sips-URI [RFC3261], meaning
   this message is protected using TLS on a hop-by-hop basis.

   INVITE sips:bob@biloxi.example.com SIP/2.0
   Via: SIPS/2.0/TLS pc33.atlanta.example.com;branch=z9hG4bK74bf9
   Max-Forwards: 70
   To: Bob <sips:bob@biloxi.example.com>
   From: Alice <sips:alice@atlanta.example.com>;tag=9fxced76sl
   Call-ID: 3848276298220188511@atlanta.example.com
   Geolocation: <cid:target123@atlanta.example.com>
   Geolocation-Routing: no
   Accept: application/sdp, application/pidf+xml
   CSeq: 31862 INVITE

```
   Contact: <sips:alice@atlanta.example.com>
   Content-Type: multipart/mixed; boundary=boundary1
```

```
   Content-Length: ...

   --boundary1

   Content-Type: application/sdp

   ...SDP goes here

   --boundary1

   Content-Type: application/pidf+xml
   Content-ID: <target123@atlanta.example.com>
   <?xml version="1.0" encoding="UTF-8"?>
       <presence
          xmlns="urn:ietf:params:xml:ns:pidf"
          xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
          xmlns:gbp="urn:ietf:params:xml:ns:pidf:geopriv10:basicPolicy"
          xmlns:cl="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
          xmlns:gml="http://www.opengis.net/gml"
          xmlns:dm="urn:ietf:params:xml:ns:pidf:data-model"
          entity="pres:alice@atlanta.example.com">
       <dm:device id="target123-1">
         <gp:geopriv>
           <gp:location-info>
             <gml:location>
               <gml:Point srsName="urn:ogc:def:crs:EPSG::4326">
                 <gml:pos>32.86726 -97.16054</gml:pos>
               </gml:Point>
             </gml:location>
           </gp:location-info>
           <gp:usage-rules>
             <gbp:retransmission-allowed>false
             </gbp:retransmission-allowed>
             <gbp:retention-expiry>2010-11-14T20:00:00Z
             </gbp:retention-expiry>
           </gp:usage-rules>
           <gp:method>802.11</gp:method>
         </gp:geopriv>
         <dm:deviceID>mac:1234567890ab</dm:deviceID>
         <dm:timestamp>2010-11-04T20:57:29Z</dm:timestamp>
       </dm:device>
```

```
        </presence>
--boundary1--
```

The Geolocation header field from the above INVITE:

```
   Geolocation: <cid:target123@atlanta.example.com>
```

... indicates the content-ID location [RFC2392] within the multipart message body of where location information is. The other message body part is SDP. The "cid:" eases message body parsing and disambiguates multiple parts of the same type.

If the Geolocation header field did not contain a "cid:" scheme, for example, it could look like this location URI:

```
   Geolocation: <sips:target123@server5.atlanta.example.com>
```

... the existence of a non-"cid:" scheme indicates this is a location URI, to be dereferenced to learn the Target's location. Any node wanting to know where the target is located would subscribe to the SIP presence event package [RFC3856] at

```
   sips:target123@server5.atlanta.example.com
```

(see Figure 2 in Section 3.2 for this message flow).

5.2 Two Locations Composed in Same Location Object Example

This example shows the INVITE message after a SIP intermediary rejected the original INVITE (say, the one in section 5.1). This INVITE contains the composed LO sent by the SIP intermediary which includes where the intermediary understands Alice to be. The rules of RFC 5491 [RFC5491] are followed in this construction.

This example is here, but ought not be taken as occurring very often. In fact, this example is believed to be a corner case of location conveyance applicability.

```
INVITE sips:bob@biloxi.example.com SIP/2.0
Via: SIPS/2.0/TLS pc33.atlanta.example.com;branch=z9hG4bK74bf0
Max-Forwards: 70
To: Bob <sips:bob@biloxi.example.com>
```

```
   From: Alice <sips:alice@atlanta.example.com>;tag=9fxced76sl
   Call-ID: 3848276298220188512@atlanta.example.com
   Geolocation: <cid:target123@atlanta.example.com>
   Geolocation-Routing: no
   Accept: application/sdp, application/pidf+xml
   CSeq: 31863 INVITE
   Contact: <sips:alice@atlanta.example.com>
   Content-Type: multipart/mixed; boundary=boundary1
   Content-Length: ...

   --boundary1

   Content-Type: application/sdp

   ...SDP goes here

   --boundary1

   Content-Type: application/pidf+xml
   Content-ID: <target123@atlanta.example.com>
```

```xml
   <?xml version="1.0" encoding="UTF-8"?>
     <presence
        xmlns="urn:ietf:params:xml:ns:pidf"
        xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
        xmlns:gbp="urn:ietf:params:xml:ns:pidf:geopriv10:basicPolicy"
        xmlns:dm="urn:ietf:params:xml:ns:pidf:data-model"
        xmlns:cl="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
        xmlns:gml="http://www.opengis.net/gml"
        entity="pres:alice@atlanta.example.com">
      <dm:device id="target123-1">
       <gp:geopriv>
         <gp:location-info>
           <gml:location>
             <gml:Point srsName="urn:ogc:def:crs:EPSG::4326">
               <gml:pos>32.86726 -97.16054</gml:pos>
             </gml:Point>
           </gml:location>
         </gp:location-info>
         <gp:usage-rules>
           <gbp:retransmission-allowed>false
           </gbp:retransmission-allowed>
          <gbp:retention-expiry>2010-11-14T20:00:00Z
           </gbp:retention-expiry>
```

```
            </gp:usage-rules>
            <gp:method>802.11</gp:method>
          </gp:geopriv>
          <dm:deviceID>mac:1234567890ab</dm:deviceID>
          <dm:timestamp>2010-11-04T20:57:29Z</dm:timestamp>
        </dm:device>
        <dm:person id="target123">
          <gp:geopriv>
            <gp:location-info>
              <cl:civicAddress>
                <cl:country>US</cl:country>
                <cl:A1>Texas</cl:A1>
                <cl:A3>Colleyville</cl:A3>
                <cl:RD>Treemont</cl:RD>
                <cl:STS>Circle</cl:STS>
                <cl:HNO>3913</cl:HNO>
                <cl:FLR>1</cl:FLR>
                <cl:NAM>Haley's Place</cl:NAM>
                <cl:PC>76034</cl:PC>
              </cl:civicAddress>
            </gp:location-info>
            <gp:usage-rules>
              <gbp:retransmission-allowed>false
              </gbp:retransmission-allowed>
              <gbp:retention-expiry>2010-11-14T20:00:00Z
              </gbp:retention-expiry>
            </gp:usage-rules>
            <gp:method>triangulation</gp:method>
          </gp:geopriv>
```

```
          <dm:timestamp>2010-11-04T12:28:04Z</dm:timestamp>
        </dm:person>
      </presence>
    --boundary1--
```

6. Geopriv Privacy Considerations

   Location information is considered by most to be highly sensitive
   information, requiring protection from eavesdropping and altering in
   transit. [RFC3693] originally articulated rules to be followed by
   any protocol wishing to be considered a "Using Protocol", specifying
   how a transport protocol meets those rules. [RFC6280] updates
   the guidance in RFC3693 to include subsequently introduced

entities and concepts in the geolocation architecture.

RFC5606 explores the difficulties inherent in mapping the GEOPRIV
architecture onto SIP elements. In particular, the difficulties of
defining and identifying recipients of location information are
given in that document, along with guidance in Section 3.3.2 on the
use of location by-reference mechanisms to preserve confidentiality
of location information from unauthorized recipients.

In a SIP deployment, location information may be added by any of
several elements, including the originating user agent or a proxy
server. In all cases, the Rule Maker associated with that location
information decides which entity adds location information and what
access control rules apply. For example, a SIP user agent that does
not support the Geolocation header may rely on a proxy server under
the direction of the Rule Maker adding a Geolocation header with a
reference to location information. The manner in which the Rule
Maker operates on these devices is outside the scope of this
document.

The manner in which SIP implementations honor the Rule Maker's
stipulations for access control rules (including retention and
retransmission) is application-specific and not within the scope of
SIP protocol operations. Entities in SIP networks that fulfill the
architectural roles of the Location Server or Location Recipient
treat the privacy rules associated with location information per
the guidance in [RFC6280] section 4.2.1. In particular, RFC4119
(especially 2.2.2) gives guidance for handling access control rules;
SIP implementations should furthermore consult the emendations in
RFC5606.

7. Security Considerations

Conveyance of physical location of a UA raises privacy concerns,
and depending on use, there probably will be authentication and
integrity concerns. This document calls for conveyance to
be accomplished through secure mechanisms, like S/MIME encrypting

message bodies (although this is not widely deployed), TLS
protecting the overall signaling or conveyance location by-reference
and requiring all entities that dereference location to authenticate
themselves. In location-based routing cases, encrypting the
location payload with an end-to-end mechanism such as S/MIME is

problematic, because one or more proxies on the path need the
ability to read the location information to retarget the message to
the appropriate new destination UAS. Data can only be encrypted to a
particular, anticipated target, and thus if multiple recipients need
to inspect a piece of data, and those recipients cannot be predicted
by the sender of data, encryption is not a very feasible choice.
Securing the location hop-by-hop, using TLS, protects the message
from eavesdropping and modification in transit, but exposes the
information to all proxies on the path as well as the endpoint. In
most cases, the UA has no trust relationship with the proxy or
proxies providing location-based routing services, so such
end-to-middle solutions might not be appropriate either.

When location information is conveyed by reference, however, one can
properly authenticate and authorize each entity that wishes to
inspect location information. This does not require that the sender
of data anticipate who will receive data, and it does permit
multiple entities to receive it securely, but it does not however
obviate the need for pre-association between the sender of data and
any prospective recipients. Obviously, in some contexts this
pre-association cannot be presumed; when it is not, effectively
unauthenticated access to location information must be permitted. In
this case, choosing pseudo-random URIs for location by-reference,
coupled with path encryption like SIPS, can help to ensure that only
entities on the SIP signaling path learn the URI, and thus restores
rough parity with sending location by-value.

Location information is especially sensitive when the identity of
its Target is obvious. Note that there is the ability, according to
[RFC3693] to have an anonymous identity for the Target's location.
This is accomplished by use of an unlinkable pseudonym in the
"entity=" attribute of the <presence> element [RFC4479]. Though,
this can be problematic for routing messages based on location
(covered in the document above). Moreover, anyone fishing for
information would correlate the identity at the SIP layer with that
of the location information referenced by SIP signaling.

When a UA inserts location, the UA sets the policy on whether to
reveal its location along the signaling path - as discussed in
Section 4, as well as flags in the PIDF-LO [RFC4119]. UAC
implementations MUST make such capabilities conditional on explicit
user permission, and MUST alert the user that location is being
conveyed.

This SIP extension offers the default ability to require permission
to process location while the SIP request is in transit. The
default for this is set to "no". There is an error explicitly

describing how an intermediary asks for permission to view the
Target's location, plus a rule stating the user has to be made aware
of this permission request.

There is no end-to-end integrity on any locationValue or
locationErrorValue header field parameter (or middle-to-end if the
value was inserted by a intermediary), so recipients of either
header field need to implicitly trust the header field contents, and
take whatever precautions each entity deems appropriate given this
situation.

8.   IANA Considerations

The following are the IANA considerations made by this SIP
extension. Modifications and additions to all these registrations
require a standards track RFC (Standards Action).

[Editor's Note: RFC-Editor - within the IANA section, please
             replace "this doc" with the assigned RFC number,
             if this document reaches publication.]

8.1 IANA Registration for the SIP Geolocation Header Field

The SIP Geolocation Header Field is created by this document, with
its definition and rules in Section 4.1 of this document, and should
be added to the IANA sip-parameters registry with the following
actions

1. Update the Header Fields registry with

Registry:
  Header Name   compact   Reference
  -----------------   -------   ---------
  Geolocation   [this doc]

8.2 IANA Registration for the SIP Geolocation-Routing Header Field

The SIP Geolocation-Routing Header Field is created by this document,
with its definition and rules in Section 4.2 of this document, and
should be added to the IANA sip-parameters registry with the
following action

1. Update the Header Fields registry with

Registry:
  Header Name   compact   Reference

```
        -----------------    -------    ---------
        Geolocation-Routing              [this doc]
```

8.3 IANA Registration for Location Profiles

   This document defines two new SIP option tags: "geolocation-sip" and
   "geolocation-http" to be added to the IANA sip-parameters Options
   Tags registry.

```
Name              Description                                Reference
-----------       ------------------------------------------ ---------
geolocation-sip   The "geolocation-sip" option tag signals   [this doc]
                  support for acquiring location information
                  via the presence event package of SIP
                  (RFC 3856). A location recipient who
                  supports this option can send a SUBSCRIBE
                  request and parse a resulting NOTIFY
                  containing a PIDF-LO object. The URI
                  schemes supported by this option include
                  "sip", "sips" and "pres".

geolocation-http  The "geolocation-http" option tag signals  [this doc]
                  support for acquiring location information
                  via an HTTP ([RFC2616]). A location
                  recipient who supports this option can
                  request location with an HTTP GET and
                  parse a resulting 200 response containing
                  a PIDF-LO object. The URI schemes
                  supported by this option include "http"
                  and "https".
```

   The names of profiles are SIP option-tags, and the guidance in this
   document does not supersede the option-tag assignment guidance in
   [RFC3261] (which requires a Standards Action for the assignment of a
   new option tag). This document does however stipulate that
   option-tags included to convey the name of a location profile per
   this definition MUST begin with the string "geolocation" followed by
   a dash. All such option tags should describe protocols used to
   acquire location by reference: these tags have no relevance to
   location carried in SIP requests by value, which use standard MIME
   typing and negotiation.

IANA Registration for 424 Response Code

   In the SIP Response Codes registry, the following is added

   Reference: RFC-XXXX (i.e., this document)
   Response code: 424 (recommended number to assign)
   Default reason phrase: Bad Location Information

   Registry:
     Response Code   Reference
     -- ---------
     Request Failure 4xx

---

        424 Bad Location Information   [this doc]

   This SIP Response code is defined in section 4.3 of this document.

8.5 IANA Registration of New Geolocation-Error Header Field

   The SIP Geolocation-error header field is created by this document,
   with its definition and rules in Section 4.4 of this document, to be
   added to the IANA sip-parameters registry with two actions

   1. Update the Header Fields registry with

   Registry:
     Header Name   compact   Reference
     ----------------   -------   ---------
     Geolocation-Error   [this doc]

   2. In the portion titled "Header Field Parameters and Parameter
      Values", add

                                        Predefined
     Header Field   Parameter Name   Values   Reference
     ----------------   ------------------ ---------- ---------
     Geolocation-Error   code   yes   [this doc]

8.6 IANA Registration for the SIP Geolocation-Error Codes

This document creates a new registry for SIP, called
"Geolocation-Error Codes." Geolocation-Error codes provide reason
for the error discovered by Location Recipients, categorized by
action to be taken by error recipient. The initial values for this
registry are shown below.

Registry Name: Geolocation-Error Codes
Reference: [this doc]
Registration Procedures: Specification Required

Code	Default Reason Phrase	Reference
100	"Cannot Process Location"	[this doc]
200	"Permission To Use Location Information"	[this doc]
201	"Permission To Retransmit Location Information to a Third Party"	[this doc]
202	"Permission to Route based on Location Information"	[this doc]
300	"Dereference Failure"	[this doc]

Details of these error codes are in Section 4.4 of this
document.

9. Acknowledgements

To Dave Oran for helping to shape this idea.

To Dean Willis for guidance of the effort.

To Allison Mankin, Dick Knight, Hannes Tschofenig, Henning
Schulzrinne, James Winterbottom, Jeroen van Bemmel, Jean-Francois
Mule, Jonathan Rosenberg, Keith Drage, Marc Linsner, Martin Thomson,
Mike Hammer, Ted Hardie, Shida Shubert, Umesh Sharma, Richard
Barnes, Dan Wing, Matt Lepinski, John Elwell, Thomas Stach,
Jacqueline Lee and Adam Roach for constructive feedback and nits
checking.

Special thanks to Paul Kyzivat for his help with the ABNF in this
document and to Robert Sparks for many helpful comments and the

proper construction of the Geolocation-Error header field.

And finally, to Spencer Dawkins for giving this doc a good scrubbing to make it more readable.

10. References

10.1 Normative References

[RFC3261] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J.
           Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP:
           Session Initiation Protocol", RFC 3261, May 2002.

[RFC4119] J. Peterson, "A Presence-based GEOPRIV Location Object
           Format", RFC 4119, December 2005

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

[RFC2392] E. Levinson, "Content-ID and Message-ID Uniform Resource
           Locators", RFC 2392, August 1998

[RFC3856] J. Rosenberg, "A Presence Event Package for the Session
           Initiation Protocol (SIP)", RFC 3856, August 2004

[RFC3859] J. Peterson, "Common Profile for Presence (CPP)", RFC 3859,
           August 2004

[RFC3428] B. Campbell, Ed., J. Rosenberg, H. Schulzrinne, C. Huitema,
           D. Gurle, "Session Initiation Protocol (SIP) Extension for

           Instant Messaging" , RFC 3428, December 2002

[RFC3311] J. Rosenberg, "The Session Initiation Protocol (SIP) UPDATE
           Method", RFC 3311, October 2002

[RFC3265] Roach, A, "Session Initiation Protocol (SIP)-Specific
           Event Notification", RFC 3265, June 2002.

[RFC6086] C. Holmberg, E. Burger, H. Kaplan, "Session Initiation
           Protocol (SIP) INFO Method and Package Framework", RFC 6086,
           January 2011

   [RFC3515] R. Sparks, "The Session Initiation Protocol (SIP) Refer
            Method", RFC 3515, April 2003

   [RFC3903] Niemi, A, "Session Initiation Protocol (SIP) Extension
            for Event State Publication", RFC 3903, October 2004.

   [RFC5234] Crocker, D., Ed., and P. Overell, "Augmented BNF for Syntax
            Specifications: ABNF", STD 68, RFC 5234, January 2008.

   [RFC4479] J. Rosenberg, "A Data Model for Presence", RFC 4479, July
            2006

   [RFC4483] E. Berger, "A Mechanism for Content Indirection in SIP", RFC
            4483, May 2006

   [RFC5491] J. Winterbottom, M. Thomson, H. Tschofenig, "GEOPRIV PIDF-LO
            Usage Clarification, Considerations, and Recommendations ",
            RFC 5491, March 2009

   [RFC5870] A. Mayrhofer, C. Spanring, "A Uniform Resource Identifier
            for Geographic Locations ('geo' URI)", RFC 5870, June 2010

   [RFC2616] R. Fielding, J. Gettys, J., Mogul, H. Frystyk, L.,
            Masinter, P. Leach, T. Berners-Lee, "Hypertext Transfer
            Protocol - HTTP/1.1", RFC 2616, June 1999

10.2 Informative References

   [RFC3693] J. Cuellar, J. Morris, D. Mulligan, J. Peterson. J. Polk,
            "Geopriv Requirements", RFC 3693, February 2004

   [RFC2818] E. Rescorla, "HTTP Over TLS", RFC 2818, May 2000

   [RFC5606] J. Peterson, T. Hardie, J. Morris, "Implications of
            'retransmission-allowed' for SIP Location Conveyance",
            RFC5606, Oct 2008

   [ID-GEO-FILTERS] R. Mahy, B. Rosen, H. Tschofenig, "Filtering Location
            Notifications in SIP", draft-ietf-geopriv-loc-filters, "work

            in progress", March 2010

   [ID-HELD-DEREF] J. Winterbottom, H. Tschofenig, H. Schulzrinne, M.

Thomson, M. Dawson, "A Location Dereferencing Protocol Using HELD", "work in progress", June 2011

[RFC6280] R. Barnes, M. Lepinski, A. Cooper, J, Morris, H. Tschofenig, H. Schulzrinne, "An Architecture for Location and Location Privacy in Internet Applications", draft-ietf-geopriv-arch, "work in progress", October 2010

Authors' Addresses

   James Polk
   Cisco Systems
   3913 Treemont Circle
   Colleyville, Texas 76034

   33.00111N
   96.68142W

   Phone: +1-817-271-3552

   Email: jmpolk@cisco.com

   Brian Rosen
   NeuStar, Inc.
   470 Conrad Dr.
   Mars, PA 16046

   40.70497N
   80.01252W

   Phone: +1 724 382 1051
   Email: br@brianrosen.net

   Jon Peterson
   NeuStar, Inc.

   Email: jon.peterson@neustar.biz

Appendix A. Requirements for SIP Location Conveyance

   The following subsections address the requirements placed on the UAC, the UAS, as well as SIP proxies when conveying location. This is from the original requirements draft that has since evolved into the solution document (that is above). This has been kept for historical reasons.

    If a requirement is not obvious in intent, a motivational statement
    is included below it.

A.1 Requirements for a UAC Conveying Location

    UAC-1   The SIP INVITE Method [RFC3261] must support location
            conveyance.

    UAC-2   The SIP MESSAGE method [RFC3428] must support location
            conveyance.

    UAC-3   SIP Requests within a dialog should support location
            conveyance.

    UAC-4   Other SIP Requests may support location conveyance.

    UAC-5   There must be one, mandatory to implement means of
            transmitting location confidentially.

    Motivation: to guarantee interoperability.

    UAC-6   It must be possible for a UAC to update location conveyed
            at any time in a dialog, including during dialog
            establishment.

    Motivation: if a UAC has moved prior to the establishment of a
            dialog between UAs, the UAC must be able to send location
            information. If location has been conveyed, and the UA
            moves, the UAC must be able to update the location previously
            conveyed to other parties.

    UAC-7   The privacy and security rules established within [RFC3693]
            that would categorize SIP as a 'Using Protocol' MUST be met.

    UAC-8   The PIDF-LO [RFC4119] is a mandatory to implement format for
            location conveyance within SIP.

    Motivation: interoperability with other IETF location protocols and
            Mechanisms.

    UAC-9   There must be a mechanism for the UAC to request the UAS send
            its location.

            UAC-9 has been DEPRECATED by the SIP WG, due to the many

problems this requirement would have caused if implemented.
                 The solution is for the above UAS to send a new request to
                 the original UAC with the UAS's location.

        UAC-10 There must be a mechanism to differentiate the ability of the
                 UAC to convey location from the UACs lack of knowledge of its
                 location

        Motivation: Failure to receive location when it is expected can
                 happen because the UAC does not implement this extension, or
                 because the UAC implements the extension, but does not know
                 where the Target is. This may be, for example, due to the
                 failure of the access network to provide a location
                 acquisition mechanism the UAC supports. These cases must be
                 differentiated.

        UAC-11 It must be possible to convey location to proxy servers
                  along the path.

        Motivation: Location-based routing.

A.2 Requirements for a UAS Receiving Location

     The following are the requirements for location conveyance by a UAS:

     UAS-1 SIP Responses must support location conveyance.

             The SIPCORE WG reached consensus that this be allowed, but
             not to communicate the UAS's location; rather for a SIP
             intermediary to inform the UAC which location to include in
             its next SIP request (as a matter of correcting what was
             originally sent by the UAC).

     UAS-2 There must be a unique 4XX response informing the UAC it did
             not provide applicable location information.

     In addition, requirements UAC-5, 6, 7 and 8 also apply to the UAS.

A.3 Requirements for SIP Proxies and Intermediaries

     The following are the requirements for location conveyance by a SIP

proxies and intermediaries:

Proxy-1   Proxy servers must be capable of adding a Location header
          field during processing of SIP requests.

Motivation: Provide network assertion of location
          when UACs are unable to do so, or when network assertion is
          more reliable than UAC assertion of location

Note: Because UACs connected to SIP signaling networks can have
          widely varying access network arrangements, including VPN
          tunnels and roaming mechanisms, it can be difficult for a
          network to reliably know the location of the endpoint.
          Proxies SHOULD NOT assert location of an endpoint unless the
          SIP signaling network has reliable knowledge of the actual
          location of the Targets.

Proxy-2   There must be a unique 4XX response informing the UAC it
          did not provide applicable location information.