Internet Engineering Task Force
Internet Draft

J. Elwell
Siemens
F. Audet
Nortel

draft-elwell-sipping-service-retargeting-00.txt
Expires: April 2006 October 2005

Indicating Service Retargeting in the Session Initiation Protocol (SIP)

Status of this Memo

Copyright Notice

Abstract

This contains motivation, requirements and a proposed solution for indicating service retargeting information in SIP requests and responses. Retargeting of a request can be considered to be service retargeting when it goes beyond "normal" routing and might be of interest to applications at the UAS or UAC.

Table of Contents

1 Introduction

Central to SIP [SIP] is the concept of retargeting a request by a proxy, whereby the Request-URI in the original request is replaced before forwarding the request on the next hop. Retargeting can also occur because of redirection by a redirect server using a SIP 3xx response code and subsequent recursion by the UAC or a proxy. Except where otherwise stated, the term retargeting is used in this document to cover recursion as well as retargeting. A given request from a User Agent Client (UAC) can be retargeted zero or more times before reaching the User Agent Server (UAS).

Retargeting is a normal part of routing a request in SIP. For example, an outbound proxy might convert the initial Request-URI from a telephone URI (perhaps in the form of a dial string) to a SIP URI. As another example, the final proxy typically replaces an Address of Record with the URI of a registered contact.

However, sometimes a service running at a proxy or redirect server (including a UA acting as a redirect server) can initiate retargeting to a specific service URI. Retargeting of this nature can be called service retargeting, because it is based on special services that operate on incoming requests to a target. An example of service retargeting can be found in [SRVCTRL]. [SRVCTRL] specifies a means for communicating context information to an application, with the expectation that the recipient endpoint or application understands the implications of the context information. Typically the original target user will have made arrangements for service retargeting. Service retargeting can be based on simple or complex rules for handling requests to the original target.

For example, a request could be retargeted to a destination that can handle requests that encounter busy or no reply at the original target. As another example, a user could arrange that requests targeted at the user be retargeted to a deputy, perhaps because the original user expects to be absent or does not wish to be disturbed. The fact that a request has been service retargeted is often of interest to the users involved, i.e., the retargeted-to user and the calling user, or to an application. Therefore it would be very useful to provide to the UAS and the UAC details of retargeting in the form of the original target URI, the retargeted-to URI and the reason for retargeting.

Service retargeting information is also useful when interworking with PSTN/ISDN. Service retargeting in SIP is similar to diversion in PSTN/ISDN, and therefore service retargeting information in SIP can be mapped to/from diversion information in PSTN/ISDN. For example,

for a call that is service retargeted in the SIP network because the

original target is busy, if the new target is in PSTN/ISDN the PSTN/ISDN can be told that the call has been diverted on busy.

As a further example, service retargeting information can be of use to a voice mail server. When a request is service retargeted to a voice mail server the voice mail server is likely to need to know the identity of the original target in order to access the correct mailbox and the reason for service retargeting in order to behave appropriately, e.g., play an appropriate announcement.

In all these examples, information about normal SIP retargeting, as opposed to service retargeting, is not generally of interest.

[HIST] specifies a means of providing the UAS and UAC with information about the retargeting of a request. This information includes the initial Request-URI and any retarget-to URIs. This information is placed in the History-Info header, field, which, except where prevented by privacy considerations, is built up as the request progresses and, on reaching the UAS, is returned in certain responses. Within the History-Info header field, each URI, except for the final one, includes as a parameter a Reason Header [REASON] indicating the SIP response code that led to retargeting from that URI to the next URI. This is either the response code received as a result of forwarding the request to that URI or the nearest equivalent if retargeting occurs without having forwarded the request.

[HIST], when deployed at relevant SIP entities and not subject to privacy, is intended to provide a comprehensive trace of retargeting for a SIP request, along with the SIP response codes that led to retargeting. [HIST] is captured independently of any service interactions that might have resulted in retargeting. [HIST] captures the information independently of how an endpoint might make use of the information. Thus, it does not fully meet the needs of reporting service retargeting for the following reasons:

- [HIST] reports all retargets, not just service retargets. This puts the burden on the UAS or UAC to pick out which retargets are for service reasons and which are for normal SIP routing reasons.

- [HIST] reports reasons in the form of SIP response codes, which do not necessarily reflect service reasons for retargeting very well and are not always meaningful to applications.

- The SIP response codes captured by [HIST] are dependent upon whether retargeting is as a result of recursion or not. When recursion is used, the SIP response code will always be in the 3xx range, but otherwise, even if the reason for retargeting is

identical, the reason will not be in the 3xx range. For example, if

retargeting is due to the previous target being busy, the SIP response code used without recursion would normally be 486, but with recursion it would have to be a 3xx response code (e.g., 302).

This document defines a mechanism that provides simple but meaningful information to a service retargeted-to user or application to represent the most recent retarget of a request. The mechanism makes use of the solution approach specified in [SRVCTRL], which provides the flexibility to provide service retargeting information in SIP requests. When used in conjunction with [HIST] it provides more comprehensive information to the retargeted-to user or application and also to the calling user or application. Although aimed primarily at INVITE requests, it can in principle apply to other SIP methods.

2 Requirements

REQ-1. When forwarding a service-retargeted request to a UAS, it must be possible to include information that denotes the service reason for service retargeting and the previous target, in order to assist the user or application in determining how to behave, e.g.:

- how to respond to the request;
- in the case of an INVITE request that is answered, how to behave during the established session (e.g., greeting to be given).

REQ-2. It must be possible to include this information in a service-retargeted request to a UAS also in the case where service retargeting has been followed by retargeting that is not service retargeting.

REQ-3. When a request from a UAC has been service-retargeted, it must be possible to include information in a response that denotes the reason for service retargeting and new target, in order to assist the user in determining how to behave, e.g.:

- in the case of a failed request, under what circumstances it might be appropriate to re-attempt the request (e.g., if retargeted because of busy but the new target does not answer, it might be appropriate to retry a few minutes later);
- in the case of an INVITE request that results in an established session, whether to abandon that session and if so under what circumstances it might be appropriate to re-attempt the request;
- in the case of an INVITE request that results in an established session, how to behave during that session (e.g., greeting to be given).

REQ-4. It must be possible to indicate that the reason for retargeting is because there are no registered contacts for the URI.

REQ-5. It must be possible to indicate that the reason for retargeting is because contacts for the URI are busy.

REQ-6. It must be possible to indicate that the reason for retargeting is because the request was not answered during the alerting period.

REQ-7. It must be possible to indicate that the reason for retargeting is because the user has arranged for requests to be retargeted irrespective of the state of registered contacts.

REQ-8. It must be possible to indicate that the reason for retargeting is because the user declined the request during alerting.

REQ-9. It must be possible to indicate that the reason for retargeting is because the user has arranged for requests to be distributed among a number of targets.

REQ-10. It must be possible to indicate that the reason for retargeting is because of network conditions.

REQ-11. It must be possible to indicate (e.g., by default) that there is no service reason for retargeting.

REQ-12. It must be possible to extend the list of service retargeting reasons in the future.

REQ-13. It must be possible to suppress information concerning service retargeting in order to reflect network policy or respect the wishes of the retargeted-from user.

3 Overview of the solution

[SRVCTRL] describes how URI parameters can be used to control a service or application at the UAS by providing appropriate context information. It describes this only in principle, without assigning any new URI parameter names or values. For a given deployment, the principles can be used to achieve control of a service or application by configuring the appropriate URI parameter names and values at the equipment concerned or by using equipment with appropriate capabilities from a single vendor. This requires a lot of coordination for configuring the various pieces of equipment, matching service URIs, mapping service URIs to phone numbers, etc. Further standardisation is required to allow easy deployment of equipment from different vendors and with various level of capabilities.

The solution here adopts the principles of [SRVCTRL] and defines parameter names and values for indicating retargeting details to a service or application. This enhancement to SIP, when used alone, is sufficient to satisfy the needs of some applications and can also provide useful information to a retargeted-to user. When used in conjunction with [HIST] it can provide very comprehensive information not only to retargeted-to applications and users but also to source applications and users.

When a request is service retargeted (for a reason meaningful to a retargeted-to user or application), two parameters are added to the retargeted-to URI: the old-target parameter contains the previous target URI and the retargeting-reason parameter contains the reason for service retargeting. Provided this is the last retarget, these parameters will reach the UAS and can be provided to the user or application.

This provides a simple means of satisfying the needs of certain applications such as voice mail servers that just require information about the most recent retarget in order to trigger appropriate behaviour.

When retargeting occurs and a History-Info header field element is added to record the retarget-to URI and the SIP reason that led to retargeting, if the retargeting is service retargeting the old-target and retargeting-reason parameters in the retargeted-to URI will also appear in the History-Info header field element. If History-Info header field elements are forwarded to the UAS, the UAS will be able to see which retargets were service retargets and the service retargeting reasons concerned. Likewise, if the History-Info header field elements are sent back to the UAC, the UAC will be able to see which retargets were service retargets. This information can be presented to the user or application at the UAS or UAC.

4 Behaviour

4.1 UAC behaviour

A UAC MAY use service redirection information in a received History-Info header field to present to the user or application.

> Note that when a UAC recurses as a result of receiving a 3xx response, any service redirection information in the retargeted-to URI (received in the Contact header field) will automatically be copied into the Request URI.

4.2 Proxy behaviour

When retargeting a request for service reasons, a proxy MAY add an old-target parameter and a retargeting-reason parameter to the new target URI as placed in the Request-URI of the forwarded request. If a new History-Info header field element is created to contain the new target URI, this too MUST contain the same old-target and retargeting-reason parameters.

4.3 Redirect behaviour

When redirecting a request for service reasons, a redirect MAY add an old-target parameter and a retargeting-reason parameter to any or all URIs placed in the Contact URI header field in the 3xx response.

4.4 UAS behaviour

A UAS MAY use service redirection information in a received Request-URI or History-Info header field to present to the user or application.

5 Syntax

This RFC updates the SIP URI parameters registry as defined in [URIREG]. Two new URI parameters are defined.

URI parameter old-target, when present, means that the URI became the target URI for the request (the new Request URI) as a result of service retargeting and the URI parameter value was the Request URI prior to service retargeting.

URI parameter retargeting-reason, when present, means that the URI became the target URI for the request (the new Request URI) as a result of service retargeting and the URI parameter value indicates the reason for service retargeting.

The following retargeting-reason values are defined in this specification:

no-contacts - service retargeting because there are no registered contacts for the URI;

busy û service retargeting because contacts for the URI are busy;

no-reply û service retargeting because the request was not answered during the alerting period;

unconditional û service retargeting because the user has arranged for requests to be retargeted irrespective of the state of registered contacts;

declined û service retargeting because the user declined the request during alerting;

distribution û service retargeting because the user has arranged for requests to be distributed among a number of targets;

network û service retargeting because of network conditions.

If a received retargeting-reason value is not recognized it SHOULD be treated as "unconditional".

The ABNF definition of these parameters is as follows.

```
uri-parameter      = transport-param / user-param / method-param
                     / ttl-param / maddr-param / lr-param
                     / old-target / retargeting-reason / other-param
old-target         = "old-target=" Request-URI
redirecting-reason = "redirecting-reason=" service-reason
service-reason     = ("no-contacts" / "busy" / "no-reply"
                     / "unconditional" / "declined" / "distribution"
                     / "network" / other-reason)
other-reason       = token
```

6 PSTN Mapping

The mapping to the PSTN/ISDN protocols is important both for gateways that connect the IP network to existing TDM equipment, such as PBXs and voicemail systems, and for gateways that connect the IP network to the PSTN/ISDN network. Both Q.931 and ISUP have signaling for this information that can be treated as roughly equivalent for the purposes here.

For a service-retargeted call from SIP to PSTN/ISDN, the user portion of the URI SHOULD be used as the address of the service retargeted-to entity in the PSTN/ISDN, while the old-target SHOULD be mapped to the PSTN/ISDN original redirecting number.

If the gateway and Proxy are in the same Trust Domain (defined in RFC 3325 [PASSERT]), and the Spec(T) includes compliance with that specification, and the Spec(T) asserts that the Proxy will do screening (whatever that means), then the gateway MAY claim that the original redirecting number is screened; otherwise it SHOULD NOT assert that the original redirecting number is screened.

The following SHOULD be used as the mapping from retargeting-reason parameters to ISUP/Q.931/QSIG redirect reason codes:

Retargeting reason value	ISUP/Q.931/QSIG redirect reason codes
no-contacts - service retargeting because there are no registered contacts for the URI;	Unknown / not available (Unconditional for QSIG)
busy û service retargeting because contacts for the URI are busy;	User busy
no-reply û service retargeting because the request was not answered during the alerting period;	No reply
unconditional û service retargeting because the user has arranged for requests to be retargeted irrespective of the state of registered contacts;	Unconditional
declined û service retargeting because the user declined the request during alerting;	Deflection during alerting (No reply for QSIG)
distribution û service retargeting because the user has arranged for requests to be distributed among a number of targets;	Deflection immediate response (Unconditional for QSIG)
network û service retargeting because of network conditions.	Network congestion (Unconditional for QSIG)

The redirection counters SHOULD be set to one unless additional information is available.

For a call from PSTN/ISDN that has been redirected within the PSTN/ISDN, information from the PSTN/ISDN MAY be used to indicate service retargeting in the SIP INVITE request. In this case, the original redirecting number SHOULD be used to derive the old-target URI and the ISUP/Q.931/QSIG redirect reason code should be used to derive the retargeting-reason, in accordance with the table above.

More comprehensive mapping to/from PSTN/ISDN may be achieved if the History-Info header field is also taken into account (e.g., by taking into account multiple service retargets and by mapping information sent towards the calling party). This is outside the scope of this document.

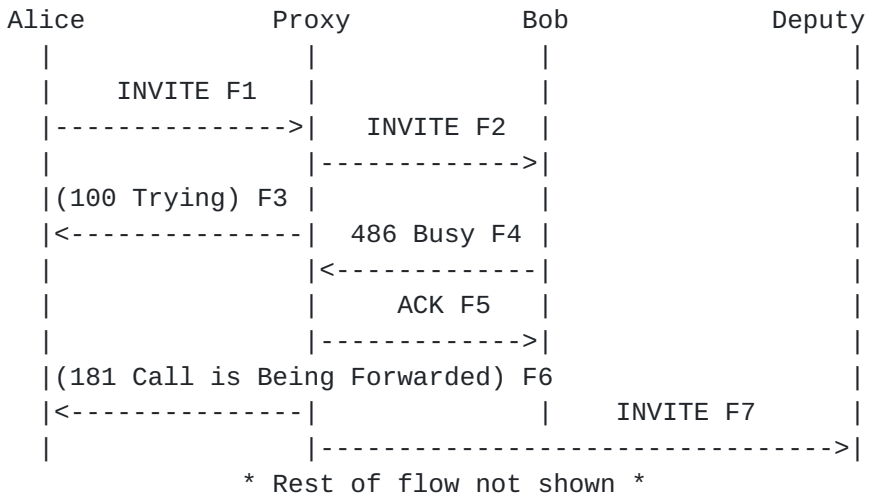
7 Examples

This section provides some example use cases for the solution proposed in this document. The examples are intended to highlight the potential applicability of this solution and are not intended to limit its applicability. The term "deputy" is used to define the role of a recipient UA, after retargeting, in several of the examples. This term is intended to represent a general role of an entity that could be an automata (eg. voicemail server) or another person, such as another member of a work group (e.g. supervisor) or agent in a call center application, etc..

Also the examples show just service retargeting on busy, but can easily be adapted to show other forms of service retargeting.

7.1 Proxy forwards busy to deputy

In this example, Alice calls Bob. BobÆs proxy determines that Bob is busy, and the proxy forwards the call to Bob's deputy (or voice mail). Alice's phone is at 192.168.0.1 while Bob's phone is at 192.168.0.2. The important thing to note is the URI in message F7.



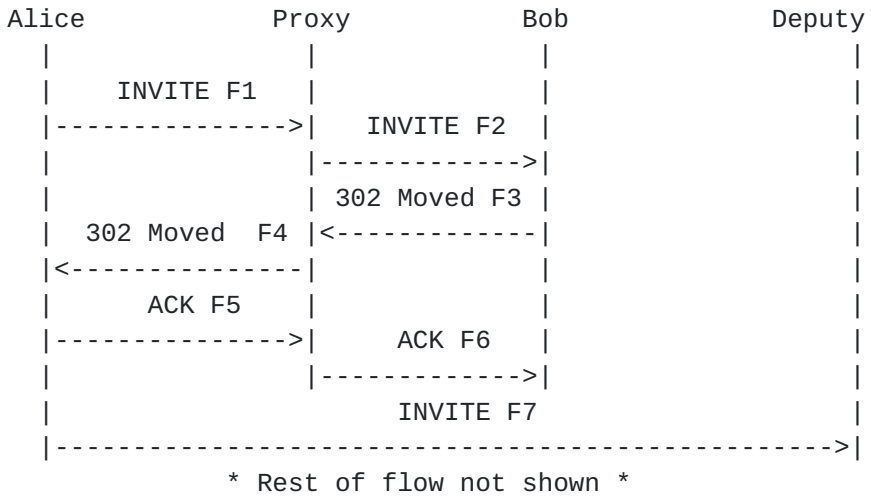

```
F1: INVITE 192.168.0.1 -> proxy.example.com

INVITE sip:+15555551002@example.com;user=phone  SIP/2.0
Via: SIP/2.0/TCP 192.168.0.1:5060;branch=z9hG4bK-74bf9
From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
To: sip:+15555551002@example.com;user=phone
Call-ID: c3x842276298220188511
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:alice@92.168.0.1>
Content-Type: application/sdp
```

```
Content-Length: *Body length goes here*

* SDP goes here*


F2: INVITE proxy.example.com -> 192.168.0.2

INVITE sip:line1@192.168.0.2 SIP/2.0
Via: SIP/2.0/TCP 192.168.1.4:5060;branch=z9hG4bK-ik80k7g-1
Via: SIP/2.0/TCP 192.168.0.1:5060;branch=z9hG4bK-74bf9
From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
To: sip:+15555551002@example.com;user=phone
Call-ID: c3x842276298220188511
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:alice@192.168.0.1>
Content-Type: application/sdp
Content-Length: *Body length goes here*

* SDP goes here*


F4: 486 192.168.0.2 -> proxy.example.com

SIP/2.0 486 Busy Here
Via: SIP/2.0/TCP 192.168.1.4:5060;branch=z9hG4bK-ik80k7g-1
Via: SIP/2.0/TCP 192.168.0.1:5060;branch=z9hG4bK-74bf9
From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
To: sip:+15555551002@example.com;user=phone;tag=09xde23d80
Call-ID: c3x842276298220188511
CSeq: 1 INVITE
Content-Length: 0

F7: INVITE proxy.example.com -> um.example.com

INVITE sip:deputy@example.com; \
       old-target=sip:+15555551002@example.com;user=phone; \
       retargeting-reason=busy  SIP/2.0
Via: SIP/2.0/TCP 192.168.1.4:5060;branch=z9hG4bK-ik80k7g-2
Via: SIP/2.0/TCP 192.168.0.1:5060;branch=z9hG4bK-74bf9
From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
To: sip:+15555551002@example.com;user=phone
Call-ID: c3x842276298220188511
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:alice@192.168.0.1>
Content-Type: application/sdp
Content-Length: *Body length goes here*
```

```
* SDP goes here*
```

7.2 Endpoint forwards busy to deputy

In this example, Alice calls Bob. Bob is busy, but forwards the session directly to his deputy (or voicemail). Alice's phone is at 192.168.0.1 while Bob's phone is at 192.168.0.2. The important thing to note is the URI in the Contact in message F3.




```
F1: INVITE 192.168.0.1 -> proxy.example.com

INVITE sip:+15555551002@example.com;user=phone  SIP/2.0
Via: SIP/2.0/TCP 192.168.0.1:5060;branch=z9hG4bK-74bf9
From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
To: sip:+15555551002@example.com;user=phone
Call-ID: c3x842276298220188511
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:alice@92.168.0.1>
Content-Type: application/sdp
Content-Length: *Body length goes here*

* SDP goes here*


F2: INVITE proxy.example.com -> 192.168.0.2

INVITE sip:line1@192.168.0.2 SIP/2.0
Via: SIP/2.0/TCP 192.168.1.4:5060;branch=z9hG4bK-ik80k7g-1
Via: SIP/2.0/TCP 192.168.0.1:5060;branch=z9hG4bK-74bf9
From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
To: sip:+15555551002@example.com;user=phone
Call-ID: c3x842276298220188511
```

```
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:alice@192.168.0.1>
Content-Type: application/sdp
Content-Length: *Body length goes here*

* SDP goes here*

F3: 302 192.168.0.2 -> proxy.example.com

SIP/2.0 302 Moved Temporarily
Via: SIP/2.0/TCP 192.168.1.4:5060;branch=z9hG4bK-ik80k7g-1
Via: SIP/2.0/TCP 192.168.0.1:5060;branch=z9hG4bK-74bf9
From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
To: sip:+15555551002@example.com;user=phone;tag=09xde23d80
Call-ID: c3x842276298220188511
CSeq: 1 INVITE
Contact: <sip: deputy@example.com; \
       old-target=sip:+15555551002@example.com;user=phone; \
       retargeting-reason=busy;>
Content-Length: 0

F7: INVITE proxy.example.com -> um.example.com

INVITE sip: deputy@example.com; \
       old-target=sip:+15555551002@example.com;user=phone; \
       retargeting-reason=busy  SIP/2.0
Via: SIP/2.0/TCP 192.168.1.4:5060;branch=z9hG4bK-ik80k7g-2
Via: SIP/2.0/TCP 192.168.0.1:5060;branch=z9hG4bK-74bf9
From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
To: sip:+15555551002@example.com;user=phone
Call-ID: c3x842276298220188511
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:alice@192.168.0.1>
Content-Type: application/sdp
Content-Length: *Body length goes here*

* SDP goes here*
```

7.3 Endpoint forwards busy to TDM via a gateway

In this example, the deputy (or mailbox) is reached via a gateway to a TDM network. Bob's number is +1 555 555-1002, while deputy's number on the TDM network is +1-555-555-2000.

The call flow is the same as in section 7.2 except for the Contact URI in F3 and the Request URI in F7.

```
   F3: 302 192.168.0.2 -> proxy.example.com

   SIP/2.0 302 Moved Temporarily
   Via: SIP/2.0/TCP 192.168.1.4:5060;branch=z9hG4bK-ik80k7g-1
   Via: SIP/2.0/TCP 192.168.0.1:5060;branch=z9hG4bK-74bf9
   From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
   To: sip:+15555551002@example.com;user=phone;tag=09xde23d80
   Call-ID: c3x842276298220188511
   CSeq: 1 INVITE
   Contact: <sip:+15555552000@example.com;user=phone;\
             old-target=tel:+15555551002;retargeting-reason=busy>
   Content-Length: 0

F7: INVITE proxy.example.com -> gw.example.com (for both 7.1 and 7.2)

   INVITE sip:+15555552000@example.com;user=phone;\
          old-target=tel:+15555551002;retargeting-reason=busy  \
          SIP/2.0
   Via: SIP/2.0/TCP 192.168.1.4:5060;branch=z9hG4bK-ik80k7g-2
   Via: SIP/2.0/TCP 192.168.0.1:5060;branch=z9hG4bK-74bf9
   From: Alice <sip:5551001@example.com;user=phone>;tag=9fxced76sl
   To: sip:+15555551002@example.com;user=phone
   Call-ID: c3x842276298220188511
   CSeq: 1 INVITE
   Max-Forwards: 70
   Contact: <sip:alice@192.168.0.1;transport=tcp>
   Content-Type: application/sdp
   Content-Length: *Body length goes here*

   * SDP goes here*
```

7.4 Endpoint forwards busy to deputy with History Info

This example illustrates how History Info [HIST] works in conjunction with service retargeting. The scenario is the same as 7.1.

```
   F1: INVITE 192.168.0.1 -> proxy.example.com

   INVITE sip:+15555551002@example.com;user=phone  SIP/2.0
   Via: SIP/2.0/TCP 192.168.0.1:5060;branch=z9hG4bK-74bf9
   From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
   To: sip:+15555551002@example.com;user=phone
   Call-ID: c3x842276298220188511
   CSeq: 1 INVITE
   Max-Forwards: 70
   Contact: <sip:alice@92.168.0.1>
   History-Info: <sip:+15555551002@example.com;user=phone >;index=1
   Content-Type: application/sdp
   Content-Length: *Body length goes here*
```

```
* SDP goes here*


F2: INVITE proxy.example.com -> 192.168.0.2

INVITE sip:line1@192.168.0.2 SIP/2.0
Via: SIP/2.0/TCP 192.168.1.4:5060;branch=z9hG4bK-ik80k7g-1
Via: SIP/2.0/TCP 192.168.0.1:5060;branch=z9hG4bK-74bf9
From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
To: sip:+15555551002@example.com;user=phone
Call-ID: c3x842276298220188511
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:alice@192.168.0.1>
History-Info: <sip:+15555551002@example.com;user=phone >;index=1,
              <sip:line1@192.168>;index=1.1

Content-Type: application/sdp
Content-Length: *Body length goes here*

* SDP goes here*

F7: INVITE proxy.example.com -> um.example.com

INVITE sip: deputy@example.com; \
       old-target=sip:+15555551002@example.com;user=phone; \
       retargeting-reason=busy  SIP/2.0
Via: SIP/2.0/TCP 192.168.1.4:5060;branch=z9hG4bK-ik80k7g-2
Via: SIP/2.0/TCP 192.168.0.1:5060;branch=z9hG4bK-74bf9
From: Alice <sip:+15551001@example.com;user=phone>;tag=9fxced76sl
To: sip:+15555551002@example.com;user=phone
Call-ID: c3x842276298220188511
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:alice@192.168.0.1>
History-Info: <sip:+15555551002@example.com;user=phone >;index=1,
              <sip:line1@192.168?Reason=SIP%3Bcause%3D302;
               text=öMoved Temporarilyö>;index=1.1
              <sip: deputy@example.com; \
              old-target=sip:+15555551002@example.com;user=phone;\
              retargeting-reason=busy>;index=2
Contact: <sip:alice@192.168.0.1>
Content-Type: application/sdp
Content-Length: *Body length goes here*

* SDP goes here*
```

8 IANA considerations

This specification adds a new value to the IANA registration in the "SIP/SIPS URI Parameters" sub-registry at http://www.iana.org/assignments/sip-parameters as defined in [URIREG].

Parameter Name	Predefined Values	Reference
old-target	No	[RFCAAAA]
retargeting-reason	Yes	[RFCAAAA]

[Note to IANA: Please replace AAAA with the RFC number of this specification.

This document requests that IANA create a new registry for retargeting-reason values. Each registry entry must contain the value and the specification in which the value is defined. New values for this registry may be defined only in Standards Track RFCs. This registry is to be populated initially with the following entries defined in section 5: no-contacts; busy; no-reply; unconditional; declined; distribution; network.

9 Security Considerations

This draft discusses transactions involving at least three parties, which increases the complexity of the privacy issues. In addition, the security considerations of [HIST] apply when the History-Info header field is used.

The new URI parameters defined in this draft are generally sent from a Proxy or call control system to a retargeted-to UA (or to a gateway to the PSTN and then to a retargeted-to device). These new parameters tell the retargeted-to UA what service the proxy wishes to have performed. Just as any message sent from the proxy to the retargeted-to UA needs to be integrity protected, these messages need to be integrity protected to stop attackers from, for example, causing speech (e.g., voicemail) meant for a company's CEO to go to an attacker. RFC 3261 provides a TLS mechanism suitable for performing this integrity protection.

The signaling from the Proxy to the retargeted-to UA will reveal who is calling whom and possibly some information about a user's presence based on whether the call was answered or retargeted. This information can be protected by encrypting the SIP traffic between the Proxy and the retargeted-to UA. Again, RFC 3261 contains mechanisms for accomplishing this using TLS.

The S/MIME based mechanisms in RFC 3261 will generally not be applicable for protecting this information because they are meant for end to end issues and this is primarily a middle to end scenario. Without end-to-end or middle-to-end security, reliance is placed on on hop-by-hop security using TLS and the SIPS URI scheme. This requires that all hops between the Proxy and the retareget-to UR be trusted, which is the case in many deployment scenarios.

9.1 Integrity Protection of Forwarding in SIP

The forwarding of a call in SIP brings up a very strange trust issue. Consider the normal case when A calls B and the call gets forwarded to C by a network element in B's domain, and then C answers the call. A has called B but ended up talking to C. This scenario may be hard to separate from a man in the middle attack.

There are two possible solutions. One is that B sends back information to A saying don't call me, call C and signs it as B. The problem is that this solution involves revealing that B has forwarded to C, which B often may not want to do. For example, B may be a work phone that has been forwarded to a mobile or home phone. The user does not want to reveal their mobile or home phone number but, even more importantly, does not want to reveal that they are not in the office.

The other possible solution is that A needs to trust B only to forward to a trusted identity. This requires a hop by hop transitive trust such that each hop will only send to a trusted next hop and each hop will only do things that the user at that hop desired. This solution is enforced in SIP using the SIPS URI and TLS based hop by hop security. It protects from an off axis attack, but if one of the hops is not trustworthy, the call may be diverted to an attacker.

Any redirection of a call to an attacker's mailbox is serious. It is trivial for an attacker to make its mailbox seem very much like the real mailbox and forward the messages to the real mailbox so that the fact that the messages have been intercepted or even tampered with escapes detection.

9.2 Privacy Related Issues on the Second Call Leg

When A calls B and gets redirected to C, occasionally people say there is a requirement for the call leg from B to C to be anonymous. This is not the PSTN and there is no call leg from B to C; instead there is a VoIP session between A and C. If A had put a To header containing B in the initial invite message, unless something special is done about it, C will see that To header. If the person who answers phone C says "I think you dialed the wrong number, who were

you trying to reach?" A will probably specify B.

If A does not want C to see that the call was to B, A needs a special relationship with the forwarding Proxy to induce it not to reveal that information. The call should go through an anonymizer service that provides session or user level privacy (as described in [PRIV] [4]) service before going to C. It is not hard to figure out how to meet this requirement, but it is unclear why anyone would want this service.

The scenario in which B wants to make sure that C does not see that the call was to B is easier to deal with but a bit weird. The usual argument is B wants to forward his phone to C but does not want C to find out his phone number. It is hard to imagine that C would want to accept all BÆs calls without knowing how to call B to complain. Several popular web portals will send SMS alert message about things like stock prices and weather to mobile phone users today. Some of these contain no information about the account on the web portal that initiated them, making it nearly impossible for the mobile phone owner to stop them. This anonymous message forwarding has turned out to be a really bad idea even where no malice is present. Clearly some people are fairly dubious about the need for this, but never mind: let's look at how it is solved.

In the general case, the proxy needs to route the call through an Anonymization Service and everything will be cleaned up. Any Anonymization service that performs the "Privacy: Header" Service in [PRIV] MUST remove the reason and target URI parameters from the URI. [PRIV] already makes it clear you would need to clean up this sort of information.

There is a specialized case of some interest in which the mechanisms in this specification are being used in conjunction with [PRIV], and the retargeted-to UA and the Proxy are both in the trust domain. In this limited case, the problem that B does not want to reveal their address to C can be solved by ensuring that the target parameter URI should never be in a message that is forwarded outside the trust domain. If it is passed to a PSTN device in the trust domain, the appropriate privacy flag needs to be set in the ISUP or ISDN signaling.

In several scenarios it is possible that a service retargeted-to user will receive unwanted calls. Arranging for automatic rejection of such calls can alleviate the problem, although it would be preferable to take steps to prevent the service retargeting, e.g., by contacting the retargeting user. Of course, if for privacy reasons service retargeting information is not provided, this will not be possible.

10 Acknowledgements

Some of the text was taken from Cullen Jennings' draft on voicemail-uri. The following individuals provided valuable comments during the initial formulation of this document: Denis Alexeitsev, Mary Barnes, Martin Dolly, Roland Jesske, Joanne McMillen.

11 Author's Addresses

John Elwell
Siemens Communications
Technology Drive
Beeston
Nottingham, UK, NG9 1LA
email: john.elwell@siemens.com

Fran ois Audet
Nortel Networks
4655 Great America Parkway
Santa Clara, CA 95054
USA
mailto:audet@nortel.com

12 Normative References

[SIP] J. Rosenberg, H. Schulzrinne, et al., "SIP: Session initiation protocol", RFC 3261.

[HIST] M. Barnes, "An Extension to the Session Initiation Protocol for Request History Information", draft-ietf-sipping-history-info-06 (work in progress).

[REASON] H. Schulzrinne, D. Oran, G. Camarillo, "The Reason Header for the Session Initiation Protocol (SIP)", RFC 3326.

[SRVCTRL] B. Campbell, R. Sparks, "Control of Service Context using SIP Request-URI", RFC 3087.

[URIREG] G. Camarillo, "The Internet Assigned Number Authority (IANA) Uniform Resource Identifier (URI) Parameter Registry for the Session Initiation Protocol (SIP)", RFC 3969.

[PASSERT] Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, November 2002.

[PRIV] Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)", RFC 3323, November 2002.

Intellectual Property Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

13 Appendix - Rejected Alternatives (temporary û to be removed)

The following alternative solutions were considered and rejected.

13.1 Extending the SIP Reason header

This alternative involves defining a new "protocol" (namespace) in the SIP Reason header for service retargeting reasons. A service-retargeted request could then convey, as a URI header in the History-Info header field, a Reason header field indicating the service retargeting reason, in addition to the SIP reason for retargeting. In addition, the Reason header field could be used in a 3xx response to indicate a service reason for redirection. This was considered to have the following disadvantages:

- It is not backwards compatible with existing UACs or proxies, which would not copy a Reason header from a 3xx response into a History-Info header field when recursing.

- The need for escape characters in URI headers makes this less readable.

- It does not provide a basic level of support to applications at the UAS without requiring use of the History-Info header field.

13.2 New 3xx response codes

There are many unused response codes in the 3xx range, and a few of these could have been used for service retargeting reasons. This was considered to have the following disadvantages:

- Service reasons for retargeting are in some ways orthogonal to SIP reasons, and it would be unwise to mix the two in the same namespace.

- There may be advantages in having both a SIP retargeting reason and a service retargeting reason available.

- It does not provide a basic level of support to applications at the UAS without requiring use of the History-Info header field.