Network Working Group
Internet-Draft
Obsoletes: 4244 (if approved)
Intended status: Standards Track
Expires: September 16, 2011

M. Barnes
Polycom
F. Audet
Skype
S. Schubert
NTT
J. van Elburg
Detecon International Gmbh
C. Holmberg
Ericsson

March 15, 2011

An Extension to the Session Initiation Protocol (SIP) for Request History Information

draft-ietf-sipcore-rfc4244bis-04.txt

Abstract

This document defines a standard mechanism for capturing the history information associated with a Session Initiation Protocol (SIP) request. This capability enables many enhanced services by providing the information as to how and why a SIP request arrives at a specific application or user. This document defines an optional SIP header field, History-Info, for capturing the history information in requests. The document also defines SIP header field parameters for the History-Info and Contact header fields to tag the method by which the target of a request is determined. In addition, this document defines a value for the Privacy header field specific to the History-Info header field.

Table of Contents

1. Introduction

Many services that SIP is anticipated to support require the ability to determine why and how a SIP requests arrived at a specific application. Examples of such services include (but are not limited to) sessions initiated to call centers via "click to talk" SIP Uniform Resource Locators (URLs) on a web page, "call history/ logging" style services within intelligent "call management" software for SIP User Agents (UAs), and calls to voicemail servers. Although SIP implicitly provides the retarget capabilities that enable SIP requests to be routed to chosen applications, there is a need for a standard mechanism within SIP for communicating the retargeting history of the requests. This "request history" information allows the receiving application to determine hints about how and why the SIP request arrived at the application/user.

This document defines a SIP header field, History-Info, to provide a standard mechanism for capturing the request history information to enable a wide variety of services for networks and end-users. SIP header field parameters are defined for the History-Info and Contact header fields to tag the method by which the target of a request is determined. In addition, this document defines a value for the Privacy header field specific to the History-Info header.

The History-info header field provides a building block for development of SIP based applications and services. The requirements for the solution described in this document are included in Appendix A. Example scenarios using the History-info header field are included in Appendix B.

2. Conventions and Terminology

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].

The term "retarget" is used in this document to refer to the process of a SIP entity changing a Uniform Resource Identifier (URI) in a request based on the rules for determining request targets as described in Section 16.5 of [RFC3261] and of the subsequent forwarding of that request as described in step 2 in section 16.6 of [RFC3261]. This includes changing the Request-URI due to a location service lookup and redirect processing. This also includes internal (to a proxy/SIP intermediary) changes of the URI prior to forwarding of the request.

The terms "location service", "forward", "redirect" and "AOR" are

used consistent with the terminology in [RFC3261].

The references to "domain for which the SIP entity/Proxy/Intermediary is responsible" are consistent with and intended to convey the same context as the usage of that terminology in [RFC3261]. The applicability of History-Info to architectures or models outside the context of [RFC3261] is outside the scope of this specification.

3. Background

SIP implicitly provides retargeting capabilities that enable SIP requests to be routed to specific applications as defined in [RFC3261]. The motivation for capturing the request history is that in the process of retargeting a request, old routing information can be forever lost. This lost information may be important history that allows elements to which the request is retargeted to process the request in a locally defined, application-specific manner. This document defines a mechanism for transporting the request history. Application-specific behavior is outside the scope of this specification.

Current network applications provide the ability for elements involved with the request to obtain additional information relating to how and why the request was routed to a particular destination. The following are examples of such applications:

1. Web "referral" applications, whereby an application residing within a web server determines that a visitor to a website has arrived at the site via an "associate" site that will receive some "referral" commission for generating this traffic

2. Email forwarding whereby the forwarded-to user obtains a "history" of who sent the email to whom and at what time

3. Traditional telephony services such as voicemail, call-center "automatic call distribution", and "follow-me" style services

Several of the aforementioned applications currently define application-specific mechanisms through which it is possible to obtain the necessary history information.

In addition, request history information could be used to enhance basic SIP functionality by providing the following:

- Some diagnostic information for debugging SIP requests.

- o Capturing aliases and Globally Routable User Agent URIs (GRUUs) [RFC5627], which can be overwritten by a home proxy upon receipt of the initial request.

- o Facilitating the use of limited use addresses (minted on demand) and sub-addressing.

- o Preserving service specific URIs that can be overwritten by a downstream proxy, such as those defined in [RFC3087], and control of network announcements and IVR with SIP URI [RFC4240].

4. Overview

The fundamental functionality provided by the request history information is the ability to inform proxies and UAs involved in processing a request about the history or progress of that request. The solution is to capture the Request-URIs as a request is retargeted, in a SIP header field: History-Info. This allows for the capturing of the history of a request that would be lost with the normal SIP processing involved in the subsequent retargeting of the request.

The History-info header field is added to a Request when a new request is created by a UAC or forwarded by a Proxy, or when the target of a request is changed. It is possible for the target of a request to be changed by the same proxy/SIP Intermediary multiple times (referred to as 'internal retargeting'). A SIP entity changing the target of a request in response to a redirect also propagates any History-info header field from the initial request in the new request. The ABNF and detailed description of the History-Info header field parameters, along with examples is provided in Section 5. Section 6, Section 7 and Section 8 provide the detailed handling of the History-Info header field by SIP User Agents, Proxies and Redirect Servers respectively.

This specification also defines two new SIP header field parameters, "rc" and "mp", for the History-Info and Contact header fields, to tag the method by which the target of a request is determined. Further detail on the use of these header field parameters is provided in Section 10.4.

In addition, this specification defines a priv-value for the Privacy header, "history", that applies to all the History-info header field entries in a Request or to a specific History-info header field hi-entry as described above. Further detail is provided in Section 10.1.

5. History-Info Header Field Protocol Structure

The History-info header field can appear in any request not associated with an early or established dialog (e.g., INVITE, REGISTER, MESSAGE, REFER and OPTIONS, PUBLISH and SUBSCRIBE, etc.) and any non-100 provisional or final responses to these requests (ISSUER-req, see Appendix A).

The following provides details for the information that is captured in the History-Info header field entries for each target used for forwarding a request:

- hi-targeted-to-uri: A mandatory parameter for capturing the Request-URI for the specific request as it is forwarded.

- hi-index: A mandatory parameter for History-Info reflecting the chronological order of the information, indexed to also reflect the forking and nesting of requests. The format for this parameter is a string of digits, separated by dots to indicate the number of forward hops and retargets. This results in a tree representation of the history of the request, with the lowest-level index reflecting a branch of the tree. By adding the new entries in order (i.e., following existing entries per the details in Section 10.3), including the index and securing the header, the ordering of the History-info header fields in the request is assured. In addition, applications may extract a variety of metrics (total number of retargets, total number of retargets from a specific branch, etc.) based upon the index values.

- hi-target-param: An optional parameter reflecting the mechanism by which the Request URI captured in the hi-targeted-to-uri in the hi-entry was determined. This parameter contains either an "rc" or "mp" header field parameter, which is interpreted as follows:

  "rc": The hi-targeted-to-URI is a contact for the Request-URI, in the incoming request, that is bound to an AOR in an abstract location service. The AOR-to-contact binding has been placed into the location service by a SIP Registrar that received a SIP REGISTER request. The "rc" header field parameter contains the value of the hi-index in the hi-entry with an hi-targeted-to- uri that reflects the Request-URI that was retargeted

  "mp": The hi-targeted-to-URI represents a user other than the user associated with the Request-URI in the incoming request that was retargeted. This occurs when a request is to statically or dynamically retargeted to another user. The value of the index in the "mp" header field parameter

represents the value of the hi-index in the hi-entry with an hi-targeted-to- uri that reflects the Request-URI that was retargeted, thus identifying the "mapped from" target.

- Extension (hi-extension): A parameter to allow for future optional extensions. As per [RFC3261], any implementation not understanding an extension MUST ignore it.

The ABNF syntax for the History-info header field and header field parameters is as follows:

```
History-Info = "History-Info" HCOLON hi-entry *(COMMA hi-entry)

hi-entry = hi-targeted-to-uri *(SEMI hi-param)

hi-targeted-to-uri = name-addr

hi-param = hi-index / hi-target / hi-extension

index-val =  1*DIGIT *("." 1*DIGIT)

hi-index = "index" EQUAL index-val

hi-target-param = rc-param / mp-param

rc-param = "rc" EQUAL index-val

mp-param = "mp" EQUAL index-val

hi-extension = generic-param
```

The ABNF definitions for "generic-param" and "name-addr" are from [RFC3261].

This document also extends the "contact-params" for the Contact header field as defined in [RFC3261] with the "rc" and "mp" header field parameters defined above.

In addition to the parameters defined by the ABNF, an hi-entry may also include a Reason header field and a Privacy header field, which are both included in the hi-targeted-to-uri as described below:

- Reason: An optional parameter for History-Info, reflected in the History-info header field by including the Reason header field [RFC3326] included in the hi-targeted-to-uri. A reason is included for the hi-targeted-to-uri that was retargeted as opposed to the hi-targeted-to-uri to which it was retargeted.

- o Privacy: An optional parameter for History-Info, reflected in the History-Info header field values by including the Privacy Header [RFC3323] included in the hi- targeted-to-uri or by adding the Privacy header field to the request. The latter case indicates that the History-Info entries for the domain MUST be anonymized prior to forwarding, whereas the use of the Privacy header field included in the hi-targeted-to-uri means that a specific hi-entry MUST be anonymized.

Note that since both the Reason and Privacy parameters are included in the hi-targeted-to-uri, these fields will not be available in the case that the hi-targeted-to-uri is a Tel-URI [RFC3966]. In such cases, the Tel-URI SHOULD be transformed into a SIP URI per section 19.1.6 of [RFC3261].

The following provides examples of the format for the History-info header field. Note that the backslash and CRLF between the fields in the examples below are for readability purposes only.

```
History-Info: <sip:UserA@ims.example.com>;index=1;foo=bar

History-Info: <sip:UserA@ims.example.com?Reason=SIP%3B\
              cause%3D302>;index=1.1,\
              <sip:UserB@example.com?Privacy=history&Reason=SIP%3B\
              cause%3D486>;index=1.2;mp=1.1,\
              <sip:45432@192.168.0.3>;index=1.3;rc=1.2
```

5.1. History-Info Header Field Example Scenario

The following is an illustrative example of usage of History-Info.

In this example, Alice (sip:alice@atlanta.example.com) calls Bob (sip:bob@biloxi.example.com). Alice's proxy in her home domain (sip: atlanta.example.com) forwards the request to Bob's proxy (sip: biloxi.example.com). When the request arrives at sip: biloxi.example.com, it does a location service lookup for bob@biloxi.example.com and changes the target of the request to Bob's Contact URIs provided as part of normal SIP registration. In this example, Bob is simultaneously contacted on a PC client and on a phone, and Bob answers on the PC client.

One important thing illustrated by this call flow is that without History-Info, Bob would "lose" the target information, including any parameters in the request URI. Bob can recover that information by locating the last hi-entry with an "rc" header field parameter. This "rc" parameter contains the index of the hi-entry containing the lost target information - i.e., the sip:bob@biloxi.example.com hi-entry

with index=1.1. Note that an hi-entry is not included for the fork to sip:bob@192.0.2.7 since there was no response at the time the 200 OK is sent to Alice.

The formatting in this scenario is for visual purposes; thus, backslash and CRLF are used between the fields for readability and the headers in the URI are not shown properly formatted for escaping. Refer to Section 5.1 for the proper formatting. Additional detailed scenarios are available in Appendix B.

Note: This example uses loose routing procedures.

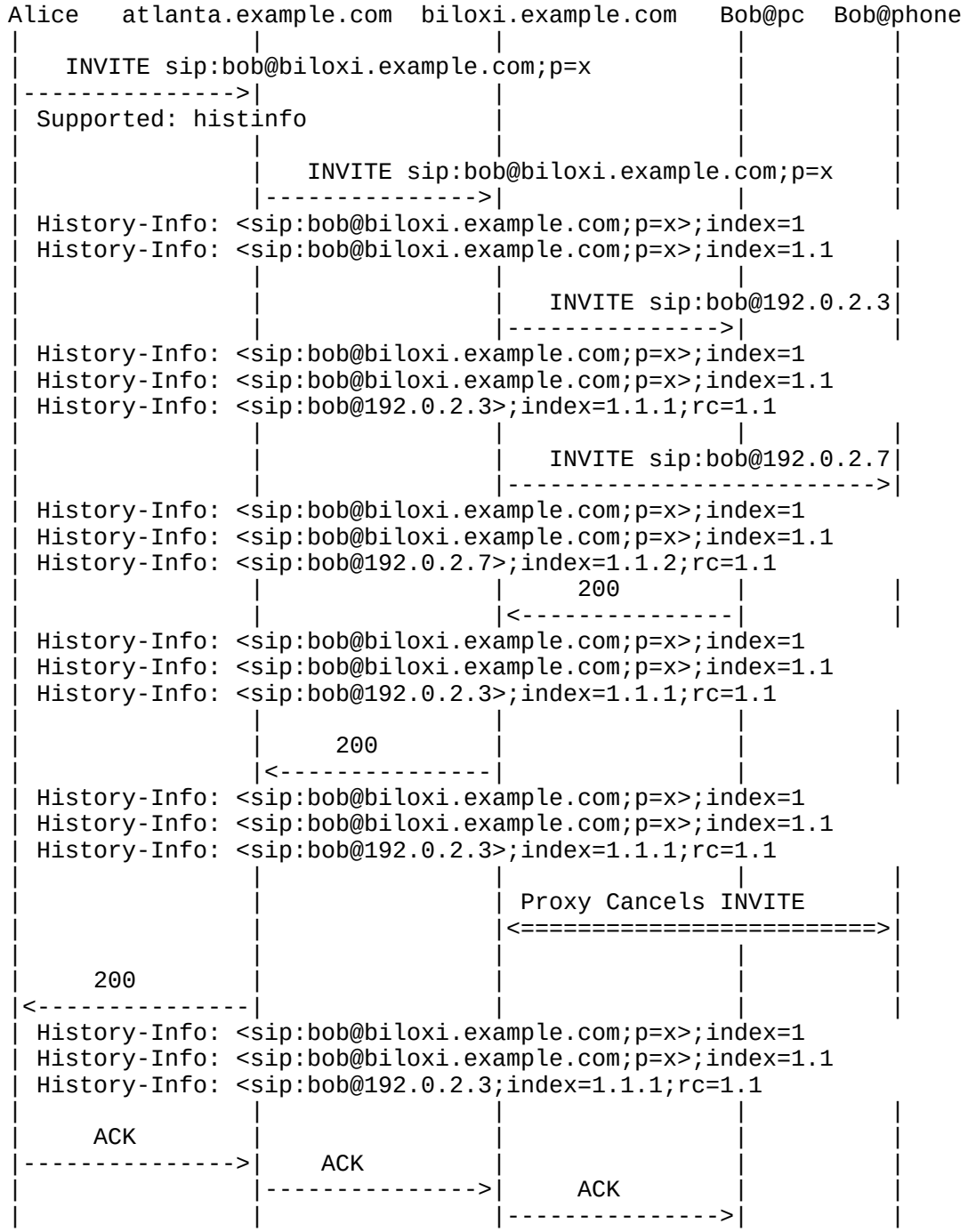

Alice
atlanta.example.com
biloxi.example.com
Bob@pc
Bob@phone
INVITE sip:bob@biloxi.example.com;p=x
Supported: histinfo
INVITE sip:bob@biloxi.example.com;p=x
History-Info: <sip:bob@biloxi.example.com;p=x>;index=1
History-Info: <sip:bob@biloxi.example.com;p=x>;index=1.1
INVITE sip:bob@192.0.2.3
History-Info: <sip:bob@biloxi.example.com;p=x>;index=1
History-Info: <sip:bob@biloxi.example.com;p=x>;index=1.1
History-Info: <sip:bob@192.0.2.3>;index=1.1.1;rc=1.1
INVITE sip:bob@192.0.2.7
History-Info: <sip:bob@biloxi.example.com;p=x>;index=1
History-Info: <sip:bob@biloxi.example.com;p=x>;index=1.1
History-Info: <sip:bob@192.0.2.7>;index=1.1.2;rc=1.1
200
History-Info: <sip:bob@biloxi.example.com;p=x>;index=1
History-Info: <sip:bob@biloxi.example.com;p=x>;index=1.1
History-Info: <sip:bob@192.0.2.3>;index=1.1.1;rc=1.1
200
History-Info: <sip:bob@biloxi.example.com;p=x>;index=1
History-Info: <sip:bob@biloxi.example.com;p=x>;index=1.1
History-Info: <sip:bob@192.0.2.3>;index=1.1.1;rc=1.1
Proxy Cancels INVITE
200
History-Info: <sip:bob@biloxi.example.com;p=x>;index=1
History-Info: <sip:bob@biloxi.example.com;p=x>;index=1.1
History-Info: <sip:bob@192.0.2.3;index=1.1.1;rc=1.1
ACK
ACK
ACK

Figure 1: Basic Call

6. User Agent Handling of the History-Info Header Field

A B2BUA MAY follow the behavior of a SIP intermediary as an alternative to following the behavior of a UAS per Section 6.2 and a UAC per Section 6.1. In behaving as an intermediary, a B2BUA carries forward hi-entries received in requests at the UAS to the request being forwarded by the UAC, as well as carrying forward responses received at the UAC to the responses forwarded by the UAS, subject to privacy considerations per Section 10.1.

6.1. User Agent Client (UAC) Behavior

The UAC MUST include the "histinfo" option tag in the Supported header in any new or out-of-dialog request for which the UAC would like the History-info header field in the response. When issuing a request, the UAC MUST follow the procedures in Section 9.2. Note that in the case of an initial request, there is no cache of hi-entries with which to populate the History-info header field as described in and the hi-index is set to 1 per Section 10.3. When receiving a response the UAC MUST follow the procedures in Section 9.3.

6.2. User Agent Server (UAS) Behavior

When receiving a request, a UAS MUST follow the procedures defined in Section 9.2. When sending a response other than a 3xx response, a UAS MUST follows the procedures as defined in Section 9.4. When sending a 3xx response, the UAS MUST follow the procedures defined for a redirect server per Section 8. An application at the UAS can make use of the cached hi-entries as described in Section 11.

7. Proxy/Intermediary Handling of History-Info Header Fields

This section describes the procedures for proxies and other SIP intermediaries for the handling of the History-Info header fields for each of the following scenarios:

For each outgoing request relating to a target in the target set, the intermediary MUST add an hi-entry for the specific target, per the procedures in Section 9.2.

An intermediary MUST follow the procedures in Section 9.1 for the handling of hi-entries in incoming SIP requests.

An intermediary MUST follow the procedures of Section 9.4 for for the handling of the hi-entries when sending a SIP response.

An intermediary MUST follow the procedures of Section 9.3 when a SIP response containing hi-entries is received.

In some cases, an intermediary may retarget a request more than once before forwarding - i.e., a request is retargeted to a SIP entity that is "internal" to the intermediary before the same intermediary retargets the request to an external target . A typical example would be a proxy that retargets a request first to a different user (i.e., it maps to a different AOR) and then forwards to a registered contact bound to the same AOR. In this case, the intermediary MUST add an hi-entry for (each of) the internal target(s) per the procedures in Section 9.2. The intermediary MAY include a Reason header field in the hi-entry with the hi-targeted-to-uri that has been retargeted as shown in the INVITE (F6) in the example in Appendix B.1. Figure 1 provides an example of internal retargeting.

8. Redirect Server Handling of History-Info Header Fields

A redirect server MUST follow the procedures in Section 9.1 when it receives a SIP Request. A redirect server MUST follow the procedures in Section 9.4 when it sends a SIP Response. When generating the Contact header field in a 3xx response, the redirect server MUST add the appropriate target header field parameter to each Contact header field as described in Section 10.4, if applicable.

9. Handling of History-Info Header Fields in Requests and Responses

This section describes the procedures for SIP entities for the handling of SIP requests and responses containing the History-Info header fields.

9.1. Receiving a Request with History-Info

When receiving a request, a SIP entity MUST create a cache containing the hi-entries associated with the request. The hi-entries MUST be added to the cache in the order in which they were received in the request.

If the Request-URI of the incoming request does not match the hi-targeted-to-uri in the last hi-entry (i.e., the previous SIP entity that sent the request did not include a History-Info header field), the SIP entity MUST add an hi-entry to end of the cache, on behalf of the previous SIP entity, as follows:

The SIP entity MUST set the hi-targeted-to-uri to the value of the Request-URI in the incoming request.

If privacy is required, the SIP entity MUST follow the procedures of Section 10.1.

The SIP entity MUST set the hi-index parameter to a value of "1", as described in Section 10.3.

The SIP entity MUST NOT include an "rc" or "mp" header field parameter.

9.2. Sending a Request with History-Info

When sending a request, a SIP entity MUST include all cached hi-entries in the request. In addition, the SIP entity MUST add a new hi-entry to the outgoing request populating the header field as follows:

The hi-targeted-to-uri MUST be set to the value of the Request-URI of the current (outgoing) request.

If privacy is required, the procedures of Section 10.1 MUST be followed.

The SIP entity MUST include an hi-index for the hi-entry as described in Section 10.3.

The SIP entity MUST include an "rc" or "mp" header field parameter in the hi-entry, if applicable, per the procedures in Section 10.4.

9.3. Receiving a Response with History-Info

When a SIP entity receives a response other than a 100, the SIP entity performs the following steps:

Step 1: Add hi-entry to cache

The SIP entity MUST add the hi-entry that was added to the request that received the non-100 response to the cache, if it was not already cached. The hi-entry MUST be added to the cache in ascending order as indicated by the values in the hi-index parameters of the hi-entries (e.g., 1.2.1 comes after 1.2 but before 1.3).

Step 2: Add Reason header field

The SIP entity then MUST add a Reason header field to the (newly) cached hi-entry reflecting the SIP response code in the non-100 response, per the procedures of Section 10.2.

Step 3: Add additional hi-entries

The SIP entity MUST also add to the cache any hi-entries received in the response that are not already in the cache. This situation can occur when the entity that generated the non-100 response retargeted the request before generating the response. As per Step 1, the hi-entries MUST be added to the cache in ascending order as indicated by the values in the hi-index parameters of the hi-entries

It is important to note that the cache does not contain hi-entries for requests that have not yet received a non-100 response, so there can be gaps in indices (e.g., 1.2 and 1.4 could but present but not 1.3).

9.4. Sending History-Info in Responses

When sending a response other than a 100, a SIP entity MUST include all the cached hi-entries in the response with the following exception: If the received request contained no hi-entries and there is no "histinfo" option tag in the Supported header field, the SIP entity MUST NOT include hi-entries in the response. In the former case, the privacy procedures as described in Section 10.1.2 MUST be followed.

10. Processing the History-Info Header Field

The following sections describe the procedures for processing the History-Info header field. These procedures are applicable to SIP entities such as Proxies/Intermediaries, Redirect Servers or User Agents.

10.1. Privacy in the History-Info Header Field

The privacy requirements for this document are described in Appendix A.2. Section 10.1.1 describes the use of the Privacy header field defined in [RFC3323] to indicate the privacy to be applied to the History-Info header field entries. Section 10.1.2 describes the processing of the priv-values in the Privacy header field to privacy protect the History-Info header field entries in the request or response that is being forwarded.

10.1.1. Indicating Privacy

As with other SIP headers described in [RFC3323], the hi-targeted-to-uris in the History-info header field can inadvertently reveal information about the initiator of the request. Thus, the UAC needs a mechanism to indicate that the hi-targeted-to-uris in the hi-entries need to be privacy protected. The Privacy header field is used by the UAC to indicate the privacy to be applied to all the hi-entries in the request as follows:

- If the UAC is including a Privacy header field with a priv-value of "header" in the request, then the UAC SHOULD NOT include a priv-value of "history" in the the Privacy header field in the Request.

- If the UAC is including any priv-values other than "header" in the Privacy header field, then the UAC MUST also include a priv-value of "history" in the Privacy header field in the Request.

- If the UAC is not including any priv-values in the Privacy header field in the request, then the UAC MUST add a Privacy header field, with a priv-value of "history", to the request. The UAC MUST NOT include a priv-value of "critical" in the Privacy header field in the Request in this case.

In addition, the History-info header field can reveal general routing and diverting information within an intermediary, which the intermediary wants to privacy protect. In this case, the intermediary MUST set a Privacy header field to a priv-value of "history" and include the Privacy header field in the hi-targeted-to-uri, for each hi-entry added by intermediary, as the request is retargeted within the domain for which the SIP entity is responsible. The intermediary MUST NOT include any other priv-values in this Privacy header field. Note that the priv-value in the Privacy header for the incoming request does not necessarily influence whether the intermediary includes a Privacy header field in the hi-entries. For example, even if the Privacy header for the incoming request contained a priv-value of "none", the Proxy can still set a priv-value of "history" in the Privacy header field included in the hi-targeted-to-uri.

Finally, the terminator of the request may not want to reveal the final reached target to the originator. In this case, the terminator MUST include a Privacy header field with a priv-value of "history" in the hi-targeted-to-uri in the last hi-entry, in the response. As noted above, the terminator of the request MUST NOT use any other priv-values in the Privacy header field included in the hi-entry.

10.1.2. Applying Privacy

When a request is retargeted to a URI associated with a domain for which the SIP intermediary is not responsible or a response is forwarded, a Privacy Service at the boundary of the domain applies the appropriate privacy based on the value of the Privacy header field in the request and in the individual hi-entries.

If there is a Privacy header field in the request with a priv-value of "header" or "history", then the hi-targeted-to-uris in the hi-entries, associated with the domain for which a SIP intermediary is responsible, are anonymized. The Privacy Service MUST change any hi-targeted-to-uris in the hi-entries that have not been anonymized to anonymous URIs containing a domain of anonymous.invalid (e.g., anonymous@anonymous.invalid). If the hi-targeted-to-uri in the hi-entry contains an Privacy header field, then the Privacy header field value MUST be removed from the hi-entry. Once all the appropriate hi-entries have been anonymized, the priv-value of "history" MUST be removed from the Privacy header field. If there are no remaining priv-values in the Privacy header field, the Privacy header field MUST be removed from the request per [RFC3323].

If there is not a Privacy header field in the request or response that is being forwarded, the Privacy Service MUST anonymize any hi-entries, associated with the domain for which a SIP intermediary is responsible, that contain a Privacy header field with a priv-value of "history". The Privacy Service MUST populate the hi-targeted-to-uri with an anonymous URI with a domain of anonymous.invalid (e.g., anonymous@anonymous.invalid). Any other priv-values in the Privacy header field in the hi-entries MUST be ignored. In any case, the Privacy Service MUST remove the Privacy header field from the hi-entries prior to forwarding.

10.2. Reason in the History-info Header Field

If the retargeting is due to receipt of an explicit SIP response and the response contains any Reason header fields (see [RFC3326]), then the SIP entity MUST include the Reason header fields in the hi-targeted-to-uri containing the URI of the request that was retargeted, unless the hi-targeted-to-uri is a Tel-URI. If the SIP response does not contain a Reason header field, the SIP entity MUST include a Reason header field, containing the SIP Response Code that triggered the retargeting, in the hi-targeted-to-uri containing the URI of the request that was retargeted, except in the case that the hi-targeted-to-uri is a Tel-URI.

If a request has timed out (instead of being explicitly rejected), the SIP entity MUST include a Reason header field, containing a SIP

error response code of 408 "Request Timeout" in hi-targeted-to-uri containing the URI of the request that was retargeted. The SIP entity MAY also include a Reason header field in the hi-targeted-to-uri containing the URI of the request that was retargeted as a result of internal retargeting.

If additional Reason headers are defined in the future per [RFC3326], the use of these Reason headers for the History-Info header field MUST follow the same rules as described above.

10.3. Indexing in the History-Info Header Field

In order to maintain ordering and accurately reflect the retargeting of the request, the SIP entity MUST add an hi-index to each hi-entry. Per the syntax in Section 5, the hi-index consists of a series of digits separated by dots (e.g., 1.1.2). Each dot reflects a SIP forwarding hop. The digit following each dot reflects the order in which a request was retargeted at the hop. The highest digit at each hop reflects the number of entities to which the request has been retargeted at the specific hop (i.e., the number of branches). Thus, the indexing results in a logical tree representation for the history of the request.

The first index in a series of History-Info entries MUST be set to 1. In the case that a SIP entity (intermediary or UAS) adds an hi-entry on behalf of the previous hop, the hi-index MUST be set to 1. For each forward hop (i.e., each new level of indexing), the hi-index MUST start at 1. An increment of 1 MUST be used for advancing to a new branch.

The basic rules for adding the hi-index are summarized as follows:

1. Basic Forwarding: In the case of a request that is being forwarded, the hi-index reflects the increasing length of the branch. In this case, the SIP entity MUST read the value from the History-info header field in the received request and MUST add another level of indexing by appending the dot delimiter followed by an initial hi-index for the new level of 1. For example, if the hi-index in the last History-info header field in the received request is 1.1, a proxy would add an hi-entry with an hi-index to 1.1.1 and forward the request.

2. Retargeting within a processing entity - 1st instance: For the first instance of retargeting within a processing entity, the SIP entity MUST calculate the hi-index as prescribed for basic forwarding.

3. Retargeting within a processing entity - subsequent instance: For each subsequent retargeting of a request by the same SIP entity, the SIP entity MUST add another branch. The SIP entity MUST calculate the hi-index for each new branch by incrementing the value from the hi-index in the last hi-entry at the current level. Per the example above, the hi-index in the next request forwarded by this same SIP entity would be 1.1.2.

4. Retargeting based upon a Response: In the case of retargeting due to a specific response (e.g., 302), the SIP entity MUST calculate the hi-index calculated per rule 3. That is, the lowest/last digit of the hi-index MUST be incremented (i.e., a new branch is created), with the increment of 1. For example, if the hi-index in the History-Info header of the sent request is 1.2 and the response to the request is a 302, then the hi-index in the History-Info header field for the new hi-targeted- to-URI would be 1.3.

5. Forking requests: If the request forwarding is done in multiple forks (sequentially or in parallel), the SIP entity MUST set the hi-index for each hi-entry for each forked request per the rules above, with each new request having a unique index. Each index MUST be sequentially assigned. For example, if the index in the last History-Info header field in the received request is 1.1, this processing entity would initialize its index to 1.1.1 for the first fork, 1.1.2 for the second, and so forth (see Figure 1 for an example). Note that for each individual fork, only the hi-entry corresponding to that fork is included (e.g., the hi-entry for fork 1.1.1 is not included in the request sent to fork 1.1.2, and vice-versa).

10.4. Mechanism for Target Determination in the History-Info Header Field

This specification defines two header field parameters, "rc" and "mp", indicating two non-inclusive mechanisms by which a new target for a request is determined. Both parameters contain an index whose value is the hi-index of the hi-entry with an hi-targeted-to-uri that represents the Request-URI that was retargeted.

The SIP entity MUST determine the specific parameter field to be included in the History-info header field as the targets are added to the target set per the procedures in section 16.5 of [RFC3261] or per section 8.1.3.4 [RFC3261] in the case of 3xx responses. In the latter case, the specific header parameter field in the Contact header becomes the header field parameter that is used in the hi-entry when the request is retargeted. If the Contact header field does not contain an "rc" or "mp" header field parameter, then the SIP

entity MUST NOT include an "rc" or "mp" in the hi-entry when the request is retargeted.

The SIP entity (intermediary or redirect server) determines the specific header field parameter to be used based on the following criteria:

- "rc": The target was determined based on a contact that is bound to an AOR in an abstract location service for the Request-URI being retargeted.

- "mp": The target was determined based on a mapping to a user other than the user associated with the Request-URI being retargeted.

Note that there are two scenarios by which the "mp" parameter can be derived.

- The mapping was done by the receiving entity on its own authority, in which case the mp-value is the parent index of the hi-entry's index.

- The mapping was done due to receiving a 3xx response, in which case the mp-value is an earlier sibling of the hi-entry's index, that of the downstream request which received the 3xx response.

11. Application Considerations

History-Info provides a very flexible building block that can be used by intermediaries and UAs for a variety of services. Prior to any application usage of the History-Info header field parameters, the SIP entity that processes the hi-entries MUST evaluate the hi-entries. The SIP entity MUST determine if there are gaps in the indices. Gaps are possible if the request is forwarded through intermediaries that do not support the History-info header field and are reflected by the existence of multiple hi-entries with an index of "1". Gaps are also possible in the case of parallel forking if there is an outstanding request at the time the SIP entity sends a response as described in Section 9.4. Thus, if gaps are detected, the SIP entity MUST NOT treat this as an error, but rather indicate to any applications that there are gaps. The most complete information available to the application is the History-Info entries starting with the last hi-entry with an index of "1". The interpretation of the information in the History-info header field depends upon the specific application; an application might need to provide special handling in some cases where there are gaps.

The following summarizes the categories of information that

applications can use:

1. Complete history information - e.g., for debug or other operational and management aspects, optimization of determining targets to avoid retargeting to the same URI, etc. This information is relevant to proxies, UACs and UASs.

2. Hi-entry with the index that matches the value of the last hi-entry with a "rc" header parameter in the Request received by a UAS - i.e., the Request URI associated with the destination of the request was determined based on an AOR-to-contact binding in an abstract location service.

3. Hi-entry with the index that matches the value of the last hi-entry with a "mp" header parameter in the Request received by a UAS - i.e., the last Request URI that was mapped to reach the destination.

4. Hi-entry with the index that matches the value of the first hi-entry with a "rc" header parameter in the Request received by a UAS. Note, this would be the original AoR if all the entities involved support the History-info header field and there is absence of a "mp" header parameter prior to the "rc" header parameter in the History-info header field. However, there is no guarantee that all entities will support History-Info, thus the first hi-entry with an "rc" header parameter within the domain associated with the target URI at the destination is more likely to be useful.

5. Hi-entry with the index that matches the value of the first hi-entry with a "mp" header parameter in the Request received by a UAS. Note, this would be the original mapped URI if all entities supported the History-info header field. However, there is no guarantee that all entities will support History-Info, thus the first hi-entry with an "mp" header parameter within the domain associated with the target URI at the destination is more likely to be useful.

In many cases, applications are most interested in the information within a particular domain(s), thus only a subset of the information is required.

Some applications may use multiple types of information. For example, an Automatic Call Distribution (ACD)/Call center application that utilizes the hi-entry who index matches the index of the first History-Info entry with an hi-target value of "mp", may also display other agents, reflected by other History-Info entries prior to entries with hi-target values of "rc", to whom the call was targeted

prior to its arrival at the current agent. This could allow the agent the ability to decide how they might forward or reroute the call if necessary (avoiding agents that were not previously available for whatever reason, etc.).

Since support for History-info header field is optional, a service MUST define default behavior for requests and responses not containing History-Info headers. For example, an entity may receive only partial History-Info entries or entries which are not tagged appropriately with an hi-target parameter. This may not impact some applications (e.g., debug), however, it could require some applications to make some default assumptions in this case. For example, in an ACD scenario, the application could select the oldest hi-entry with the domain associated with the ACD system and display that as the original called party. Depending upon how and where the request may have been retargeted, the complete list of agents to whom the call was targeted may not be available.

12. Security Considerations

The security requirements for this document are specified in Appendix A.1.

This document defines a header for SIP. The use of the Transport Layer Security (TLS) protocol [RFC5246] as a mechanism to ensure the overall confidentiality of the History-Info headers (SEC-req-4) is strongly RECOMMENDED. This results in History-Info having at least the same level of security as other headers in SIP that are inserted by intermediaries. With TLS, History-Info headers are no less, nor no more, secure than other SIP headers, which generally have even more impact on the subsequent processing of SIP sessions than the History-info header field.

Note that while using the SIPS scheme (as per [RFC5630]) protects History-Info from tampering by arbitrary parties outside the SIP message path, all the intermediaries on the path are trusted implicitly. A malicious intermediary could arbitrarily delete, rewrite, or modify History-Info. This specification does not attempt to prevent or detect attacks by malicious intermediaries.

13. IANA Considerations

This document requires several IANA registrations detailed in the following sections.

This document updates [RFC4244] but uses the same SIP header field

name and option tag. The IANA registry needs to update the references to [RFC4244] with [RFCXXXX].

13.1. Registration of New SIP History-Info Header Field

This document defines a SIP header field name: History-Info and an option tag: histinfo. The following changes have been made to http:///www.iana.org/assignments/sip-parameters The following row has been added to the header field section:.

The following row has been added to the header field section:

Header Name	Compact Form	Reference
History-Info	none	[RFCXXXX]

The following has been added to the Options Tags section:

Name	Description	Reference
histinfo	When used with the Supported header, this option tag indicates the UAC supports the History Information to be captured for requests and returned in subsequent responses. This tag is not used in a Proxy-Require or Require header field since support of History-Info is optional.	[RFCXXXX]

Note to RFC Editor: Please replace RFC XXXX with the RFC number of this specification.

13.2. Registration of "history" for SIP Privacy Header Field

This document defines a priv-value for the SIP Privacy header field: history The following changes have been made to http://www.iana.org/assignments/sip-priv-values The following has been added to the registration for the SIP Privacy header field:

Name	Description	Registrant	Reference
history	Privacy requested for History-info header fields(s)	Mary Barnes mary.barnes@polycom.com	[RFCXXXX]

Note to RFC Editor: Please replace RFC XXXX with the RFC number of this specification.

13.3. Registration of Header Field Parameters

This specification defines the following new SIP header field parameters in the SIP Header Field parameter sub-registry in the SIP Parameter Registry, http:/www.iana.org/assignments/sip-parameters.

Header Field	Parameter Name	Predefined Values	Reference
History-Info	mp	No	[RFC xxxx]
History-Info	rc	No	[RFC xxxx]
Contact	mp	No	[RFC xxxx]
Contact	rc	No	[RFC xxxx]

Note to RFC Editor: Please replace RFC XXXX with the RFC number of this specification.

14. Acknowledgements

Jonathan Rosenberg et al produced the document that provided additional use cases precipitating the requirement for the new header parameters to capture the method by which a Request URI is determined. The authors would like to acknowledge the constructive feedback provided by Ian Elz, Paul Kyzivat, John Elwell, Hadriel Kaplan and Dale Worley.

Mark Watson, Cullen Jennings and Jon Peterson provided significant input into the initial work that resulted in the development of of [RFC4244]. The editor would like to acknowledge the constructive feedback provided by Robert Sparks, Paul Kyzivat, Scott Orton, John Elwell, Nir Chen, Palash Jain, Brian Stucker, Norma Ng, Anthony Brown, Jayshree Bharatia, Jonathan Rosenberg, Eric Burger, Martin Dolly, Roland Jesske, Takuya Sawada, Sebastien Prouvost, and Sebastien Garcin in the development of [RFC4244].

The editor would like to acknowledge the significant input from Rohan Mahy on some of the normative aspects of the ABNF for [RFC4244], particularly around the need for and format of the index and around the security aspects.

15. Changes from RFC 4244

This RFC replaces [RFC4244].

Deployment experience with [RFC4244] over the years has shown a number of issues, warranting an update:

- In order to make [RFC4244] work in "real life", one needs to make "assumptions" on how History-Info is used. For example, many implementations filter out many entries, and only leave specific entries corresponding, for example, to first and last redirection. Since vendors uses different rules, it causes significant interoperability isssues.

- [RFC4244] is overly permissive and evasive about recording entries, causing interoperability issues.

- The examples in the call flows had errors, and confusing because they often assume "loose routing".

- [RFC4244] has lots of repetitive and unclear text due to the combination of requirements with solution.

- [RFC4244] gratuitously mandates the use of TLS on every hop. No existing implementation enforces this rule, and instead, the use of TLS or not is a general SIP issue, not an [RFC4244] issue per se.

- [RFC4244] does not include clear procedures on how to deliver current target URI information to the UAS when the Request-URI is replaced with a contact.

- [RFC4244] does not allow for marking History-Info entries for easy processing by User Agents.

The following summarizes the functional changes between this specification and [RFC4244]:

1. Added header field parameters to capture the specific method by which a target is determined to facilitate processing by users of the History-info header field entries. A specific header field parameter is captured for each of the target URIs as the target set is determined (per section 16.5 of [RFC3261]). The header field parameter is used in both the History-Info and the Contact header fields.

2. Rather than recommending that entries be removed in the case of certain values of the Privacy header field, the entries are

anonymized.

3. Updated the security section to be equivalent to the security recommendations for other SIP headers inserted by intermediaries.

The first 2 changes are intended to facilitate application usage of the History-info header field and eliminate the need to make assumptions based upon the order of the entries and ensure that the most complete set of information is available to the applications.

In addition, editorial changes were done to both condense and clarify the text, moving the requirements to an appendix and removing the inline references to the requirements. The examples were simplified and updated to reflect the protocol changes. Several of the call flows in the appendix were removed and put into a separate document that includes additional use cases that require the new header parameters.

15.1. Backwards compatibility

This specification is backwards compatible since [RFC4244] allows for the addition of new optional parameters. This specification adds an optional SIP header field parameter to the History-Info and Contact headers. Entities that have not implemented this specification MUST ignore these parameters, however, per [RFC4244] an entity MUST NOT remove this parameter from an hi-entry.

16. Changes since last Version

NOTE TO THE RFC-Editor: Please remove this section prior to publication as an RFC.

Changes from 03 to 04:

1. Reorganization of sections per John Elwell’s comments - i.e., a common section for building HI referenced by the UA, Intermediary and Redirect server sections.

2. Removing the use of "escape" when describing the handling of the Privacy and Reason header fields.

3. Clarification of TEL URIs in terms of not having a Privacy or Reason header field in the hi-targeted-to-uri.

Changes from 02 to 03:

1. Lots of editorial:

   A. Reorganized sections similar to the RFC 4244 order - i.e., introduce header field parameters and syntax first, then describe how the functional entities use the header. This removes redundant (and often inconsistent) text describing the parameters.

   B. Expanded use of "header" to "header field"

   C. More precision in terms of "escaping" of the Privacy and Reason headers in the hi-targeted-to-uri (versus "adding"/"setting"/etc. them to the hi-entry).

   D. Consistent use of parameter names (i.e., hi-entry versus entry, hi-target versus target, etc.)

   E. Moved item 6 in the Index section to the section on Response handling

   F. Removed last remaining vestiges of inline references to requirements.

2. Clarifications of functionality/applicability including:

   A. which messages may contain History-Info

   B. removing security text with regards to being able to figure out if there are missing entries when using TLS (issue #44)

   C. More complete information on the new header field parameters as they relate to the hi-target parameter.

   D. Changed wording from passive to active for normative statements in many cases and removed superfluous normative language.

3. Rewrite of the Privacy section to address issues and splitting into the setting of the Privacy header fields and the processing/ application of the privacy header field priv-values.

4. Rewrite of the Reason header field section - simplifying the text and adding back the RFC 4244 text with regards to the use of the Reason header field in cases of internal retargeting.

Changes from 01 to 02:

1. Editorial nits/clarifications. [Issues: 1,6,17,18,21-23,25,26,30-33,35-37,39,40]

2. Removing extraneous 4244 text - e.g., errors in flows, "stronger" security, "session" privacy. [Issues: 3,5,7,11]

3. Updated definition of "retarget" to be all encompassing - i.e., also includes internal changes of target URI. Clarified text for "internal retarging" in proxy section. [Issues: 2,8,9]

4. Clarified that the processing for Proxies is equally applicable to other SIP intermediaries. [Issue: 9].

5. Changed more SHOULDs to MUSTs. [Issue: 10]

6. Fixes to Application considerations section. [Issues: 12-15]

7. Changed language in the procedure for Indexing to normative language.

8. Clarifications for UAC processing:

   * MUST add hi-entry. [Issue: 28]

   * Clarify applicability to B2BUA. [Issue: 29]

   * Fixed text for indexing for UAC in case of 3xx.

9. Changed "hit" URI parameter to header parameters: [Issues:4,40]

   * Added index to all target header parameters. [Issues: 41]

   * Updated all the relevant sections documenting setting and use of new header parameters. [Issue: 40]

10. Updated/clarified privacy handling. [Issue: 16]

11. Updated Redirect Server section to allow adding History-info header fields. [Issue: 24]

12. Added text around restrictions for Tel-URIs - i.e., no privacy or reason. [Issues: 4, 12]

13. Updated text for forking - what goes in response. [Issues: 19,20]

Changes from 00 to 01:

1. Moved examples (except first) in appendix to a new (informational) document.

2. Updated UAS and UAC sections to clarify and expand on the handling of the History-info header field.

3. Updated the Application considerations section:

   * Included more detail with regards to how applications can make use of the information, in particular based on the new tags.

   * Removed privacy consideration (2nd bullet) since privacy is now accomplished by anonymizing rather than removal of entries.

Changes from (individual) barnes-sipcore-4244bis-03 to (WG) ietf-sipcore-4244bis-00:

1. Added a new SIP/SIPS URI parameter to tag the URIs as they are added to the target list and those returned in the contact header in a 3xx response.

2. Updated description of "target" parameter to use the new URI parameter value in setting the value for the parameter.

3. Clarified privacy.

4. Changed handling at redirect server to include the use of the new URI parameter and to remove the functionality of adding the History-Info entries (basically reverting to core 4244 processing).

5. Additional text to clarify that a service such as voicemail can be done in multiple ways.

6. Editorial changes including removal of some vestiges of tagging all entries (including the "aor" tag).

Changes from barnes-sipcore-4244bis-02 to 03:

1. Fixed problem with indices in example in voicemail example.

2. Removed oc and rt from the Hi-target parameter.

3. Removed aor tag

4. Added index parameter to "mp"

5. Added use-cases and call-flows from target-uri into appendix.

Changes from barnes-sipcore-4244bis-01 to 02:

1. Added hi-aor parameter that gets marked on the "incoming" hi-entry.

2. Hi-target parameter defined to be either rc, oc, mp, rt, and now gets included when adding an hi-entry.

3. Added section on backwards compatibility, as well as added the recognition and handling of requests that do not support this specification in the appropriate sections.

4. Updated redirect server/3xx handling to support the new parameters - i.e., the redirecting entity must add the new hi-entry since the proxy does not have access to the information as to how the Contact was determined.

5. Added section on normative differences between this document and RFC 4244.

6. Restructuring of document to be more in line with current IETF practices.

7. Moved Requirements section into an Appendix.

8. Fixed ABNF to remove unintended ordering requirement on hi-index that was introduced in attempting to illustrate it was a mandatory parameter.

Changes from barnes-sipcore-4244bis-00 to 01 :

1. Clarified "retarget" definition.

2. Removed privacy discussion from optionality section - just refer to privacy section.

3. Removed extraneous text from target-parameter (leftover from sip-4244bis). Changed the terminology from the "reason" to the "mechanism" to avoid ambiguity with parameter.

4. Various changes to clarify some of the text around privacy.

5. Reverted proxy response handling text to previous form - just changing the privacy aspects to anonymize, rather than remove.

6. Other editorial changes to condense and simplify.

7. Moved Privacy examples to Appendix.

8. Added forking to Basic call example.

Changes from barnes-sipcore-4244bis-00 to 01 :

1. Clarified "retarget" definition.

2. Removed privacy discussion from optionality section - just refer to privacy section.

3. Removed extraneous text from target-parameter (leftover from sip-4244bis). Changed the terminology from the "reason" to the "mechanism" to avoid ambiguity with parameter.

4. Various changes to clarify some of the text around privacy.

5. Reverted proxy response handling text to previous form - just changing the privacy aspects to anonymize, rather than remove.

6. Other editorial changes to condense and simplify.

7. Moved Privacy examples to Appendix.

8. Added forking to Basic call example.

Changes from barnes-sip-4244bis-00 to barnes-sipcore-4244bis-00:

1. Added tags for each type of retargeting including proxy hops, etc. - i.e., a tag is defined for each specific mechanism by which the new Request-URI is determined. Note, this is extremely helpful in terms of backwards compatibility.

2. Fixed all the examples. Made sure loose routing was used in all of them.

3. Removed example where a proxy using strict routing is using History-Info for avoiding trying same route twice.

4. Remove redundant Redirect Server example.

5. Index is now mandated to start at "1" instead of recommended.

6. Updated 3xx behavior as the entity sending the 3XX response MUST add the hi-target attribute to the previous hi-entry to ensure that it is appropriately tagged (i.e., it’s the only one that

knows how the contact in the 3xx was determined.)

7. Removed lots of ambiguity by making many "MAYs" into "SHOULDs" and some "SHOULDs" into "MUSTs".

8. Privacy is now recommended to be done by anonymizing entries as per RFC 3323 instead of by removing or omitting hi-entry(s).

9. Requirement for TLS is now same level as per RFC 3261.

10. Clarified behavior for "Privacy" (i.e., that Privacy is for Hi-entries, not headers).

11. Removed "OPTIONALITY" as specific requirements, since it's rather superflous.

12. Other editorial changes to remove redundant text/sections.

Changes from RFC4244 to barnes-sip-4244bis-00:

1. Clarified that HI captures both retargeting as well as cases of just forwarding a request.

2. Added descriptions of the usage of the terms "retarget", "forward" and "redirect" to the terminology section.

3. Added additional examples for the functionality provided by HI for core SIP.

4. Added hi-target parameter values to HI header to ABNF and protocol description, as well as defining proxy, UAC and UAS behavior for the parameter.

5. Simplified example call flow in section 4.5. Moved previous call flow to appendix.

6. Fixed ABNF per RFC4244 errata "dot" -> "." and added new parameter.

17. References

17.1. Normative References

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

[RFC3326] Schulzrinne, H., Oran, D., and G. Camarillo, "The Reason Header Field for the Session Initiation Protocol (SIP)", RFC 3326, December 2002.

[RFC3323] Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)", RFC 3323, November 2002.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC4244] Barnes, M., "An Extension to the Session Initiation Protocol (SIP) for Request History Information", RFC 4244, November 2005.

17.2. Informative References

[RFC5627] Rosenberg, J., "Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)", RFC 5627, October 2009.

[RFC5630] Audet, F., "The Use of the SIPS URI Scheme in the Session Initiation Protocol (SIP)", RFC 5630, October 2009.

[RFC3087] Campbell, B. and R. Sparks, "Control of Service Context using SIP Request-URI", RFC 3087, April 2001.

[RFC4240] Burger, E., Van Dyke, J., and A. Spitzer, "Basic Network Media Services with SIP", RFC 4240, December 2005.

[RFC3969] Camarillo, G., "The Internet Assigned Number Authority (IANA) Uniform Resource Identifier (URI) Parameter Registry for the Session Initiation Protocol (SIP)", BCP 99, RFC 3969, December 2004.

[RFC3966] Schulzrinne, H., "The tel URI for Telephone Numbers", RFC 3966, December 2004.

Appendix A. Request History Requirements

The following list constitutes a set of requirements for a "Request History" capability.

1. CAPABILITY-req: The "Request History" capability provides a capability to inform proxies and UAs involved in processing a request about the history/progress of that request. Although this is inherently provided when the retarget is in response to a SIP redirect, it is deemed useful for non-redirect retargeting scenarios, as well.

2. GENERATION-req: "Request History" information is generated when the request is retargeted.

   A. In some scenarios, it might be possible for more than one instance of retargeting to occur within the same Proxy. A proxy MUST also generate Request History information for the 'internal retargeting'.

   B. An entity (UA or proxy) retargeting in response to a redirect or REFER MUST include any Request History information from the redirect/REFER in the new request.

3. ISSUER-req: "Request History" information can be generated by a UA or proxy. It can be passed in both requests and responses.

4. CONTENT-req: The "Request History" information for each occurrence of retargeting shall include the following:

   A. The new URI or address to which the request is in the process of being retargeted,

   B. The URI or address from which the request was retargeted, and wether the retarget URI was an AOR

   C. The mechanism by which the new URI or address was determined,

   D. The reason for the Request-URI or address modification,

   E. Chronological ordering of the Request History information.

5. REQUEST-VALIDITY-req: Request History is applicable to requests not sent within an early or established dialog (e.g., INVITE, REGISTER, MESSAGE, and OPTIONS).

6. BACKWARDS-req: Request History information may be passed from the generating entity backwards towards the UAC. This is needed to enable services that inform the calling party about the dialog establishment attempts.

7. FORWARDS-req: Request History information may also be included by the generating entity in the request, if it is forwarded onwards.

A.1. Security Requirements

The Request History information is being inserted by a network element retargeting a Request, resulting in a slightly different problem than the basic SIP header problem, thus requiring specific consideration. It is recognized that these security requirements can be generalized to a basic requirement of being able to secure information that is inserted by proxies.

The potential security problems include the following:

1. A rogue application could insert a bogus Request History-Info entry either by adding an additional hi-entry as a result of retargeting or entering invalid information.

2. A rogue application could re-arrange the Request History information to change the nature of the end application or to mislead the receiver of the information.

3. A rogue application could delete some or all of the Request History information.

Thus, a security solution for "Request History" must meet the following requirements:

1. SEC-req-1: The entity receiving the Request History must be able to determine whether any of the previously added Request History content has been altered.

2. SEC-req-2: The ordering of the Request History information must be preserved at each instance of retargeting.

3. SEC-req-3: The entity receiving the information conveyed by the Request History must be able to authenticate the entity providing the request.

4. SEC-req-4: To ensure the confidentiality of the Request History information, only entities that process the request SHOULD have visibility to the information.

It should be noted that these security requirements apply to any entity making use of the Request History information.

A.2. Privacy Requirements

Since the Request-URI that is captured could inadvertently reveal information about the originator, there are general privacy requirements that MUST be met:

1. PRIV-req-1: The entity retargeting the Request must ensure that it maintains the network-provided privacy (as described in [RFC3323]) associated with the Request as it is retargeted.

2. PRIV-req-2: The entity receiving the Request History must maintain the privacy associated with the information. In addition, local policy at a proxy may identify privacy requirements associated with the Request-URI being captured in the Request History information.

3. PRIV-req-3: Request History information subject to privacy shall not be included in ougoing messages unless it is protected as described in [RFC3323].

Appendix B. Example call flows

The scenarios in this section provide sample use cases for the History-info header field for informational purposes only. They are not intended to be normative. A basic forking use case is included, along with two use cases illustrating the use of the privacy.

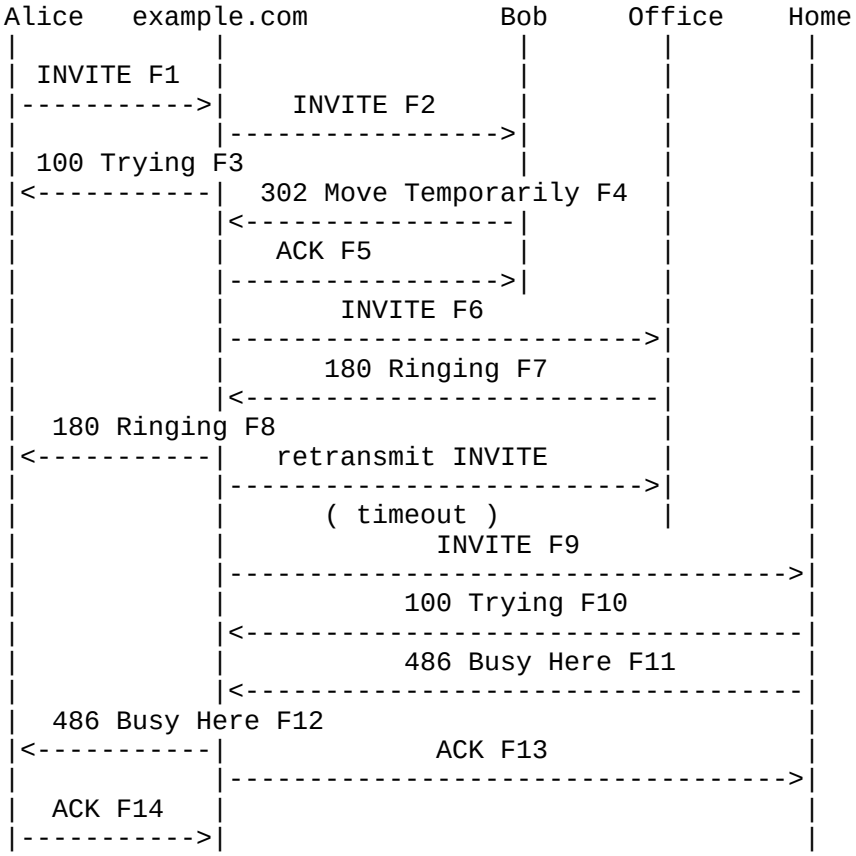
B.1. Sequentially Forking (History-Info in Response)

This scenario highlights an example where the History-Info in the response is useful to an application or user that originated the request.

Alice sends a call to Bob via sip:example.com. The proxy sip: example.com sequentially tries Bob on a SIP UA that has bound a contact with the sip:bob@example.com AOR, and then several alternate addresses (Office and Home) unsuccessfully before sending a response to Alice. The hi-entry containing the initial contact is the hi-entry just prior to the first hi-entry tagged with an hi-target value of "rc". In this example, the Office and Home are not the same AOR as sip:bob@example.com, but rather different AORs that have been configured as alternate addresses for Bob in the proxy. In other words, Office and Bob are not bound through SIP Registration with Bob’s AOR. This type of arrangement is common for example when a "routing" rule to a PSTN number is manually configured in a Proxy. These hi-entries are identified by the index contained in the hi-target "mp" parameter in the hi-entries.

This scenario illustrates that by providing the History-Info to Alice, the end-user or an application at Alice could make a decision on how best to attempt finding Bob without sending multiple requests to the same destination. Upon receipt of the response containing the History-Info entries, the Request URIs for the History-Info entries

tagged with "mp" are extracted. Those Request-URIs can be compared to other URIs (if any) that might be attempted in order to establish the session with Bob. Thus, avoiding another INVITE to Bob's home phone. Without this mechanism, Alice might well attempt to reach Bob at his office phone, which would then retarget the request to Bob's home phone. When that attempt failed, then Alice might attempt to reach Bob directly at his home phone, unknowingly for a third time.



Message Details

F1 INVITE alice -> example.com

```
INVITE sip:alice@example.com SIP/2.0
Via: SIP/2.0/TCP 192.0.2.3:5060
From: Alice <sip:alice@example.com>
To: Bob <sip:bob@example.com>
Supported: histinfo
Call-Id: 12345600@example.com
CSeq: 1 INVITE
History-Info: <sip:bob@example.com>;index=1
Contact: Alice <sip:alice@192.0.2.3>
Content-Type: application/sdp
Content-Length: <appropriate value>
<!-- SDP Not Shown -->
```

F2 INVITE example.com -> Bob

```
INVITE sip:bob@192.0.2.4 SIP/2.0
Via: SIP/2.0/TCP proxy.example.com:5060
Via: SIP/2.0/TCP 192.0.2.3:5060
From: Alice <sip:alice@example.com>
To: Bob <sip:bob@example.com>
Supported: histinfo
Call-Id: 12345600@example.com
CSeq: 1 INVITE
Record-Route: <sip:proxy.example.com;lr>
History-Info: <sip:bob@example.com>;index=1
History-Info: <sip:bob@192.0.2.4>;index=1.1;rc=1
Contact: Alice <sip:alice@192.0.2.3>
Content-Type: application/sdp
Content-Length: <appropriate value>
<!-- SDP Not Shown -->
```

F3 100 Trying example.com -> alice

```
SIP/2.0 100 Trying
Via: SIP/2.0/TCP 192.0.2.3:5060
From: Alice <sip:alice@example.com>
To: Bob <sip:bob@example.com>
Call-Id: 12345600@example.com
CSeq: 1 INVITE
Content-Length: 0
```

F4 302 Moved Temporarily Bob -> example.com

```
SIP/2.0 302 Moved Temporarily
Via: SIP/2.0/TCP proxy.example.com:5060
Via: SIP/2.0/TCP 192.0.2.3:5060
From: Alice <sip:alice@example.com>
To: Bob <sip:bob@example.com>;tag=3
Call-Id: 12345600@example.com
CSeq: 1 INVITE
Record-Route: <sip:proxy.example.com;lr>
History-Info: <sip:bob@example.com>;index=1
History-Info: <sip:bob@192.0.2.4>;index=1.1;rc=1
Contact: <sip:office@example.com>;mp=1
Content-Length: 0
```

F5 ACK 192.0.2.4 -> Bob

```
ACK sip:home@example.com SIP/2.0
Via: SIP/2.0/TCP proxy.example.com:5060
From: Alice <sip:alice@example.com>
To: Bob <sip:bob@example.com>
Call-Id: 12345600@example.com
CSeq: 1 ACK
Content-Length: 0
```

F6 INVITE example.com -> office

```
INVITE sip:office@192.0.2.3.com SIP/2.0
Via: SIP/2.0/TCP proxy.example.com:5060;branch=2
Via: SIP/2.0/TCP 192.0.2.3:5060
From: Alice <sip:alice@example.com>
To: Bob <sip:bob@example.com>
Supported: histinfo
Call-Id: 12345600@example.com
Record-Route: <sip:proxy.example.com;lr>
History-Info: <sip:bob@example.com>;index=1
History-Info: <sip:bob@192.0.2.4?Reason=SIP%3Bcause%3D302>;\
              index=1.1;rc=1
History-Info: <sip:office@example.com>;index=1.2;mp=1
History-Info: <sip:office@192.0.2.5>;index=1.2.1
CSeq: 1 INVITE
Contact: Alice <sip:alice@192.0.2.3>
Content-Type: application/sdp
Content-Length: <appropriate value>
```

```
   <!-- SDP Not Shown -->


   F7 180 Ringing office -> example.com

   SIP/2.0 180 Ringing
   Via: SIP/2.0/TCP proxy.example.com:5060;branch=2
   Via: SIP/2.0/TCP 192.0.2.3:5060
   From: Alice <sip:alice@example.com>
   To: Bob <sip:bob@example.com>;tag=5
   Supported: histinfo
   Call-ID: 12345600@example.com
   Record-Route: <sip:proxy.example.com;lr>
   History-Info: <sip:bob@example.com>;index=1
   History-Info: <sip:bob@192.0.2.4?Reason=SIP%3Bcause%3D302>;\
                 index=1.1;rc=1
   History-Info: <sip:office@example.com>;index=1.2;mp=1
   History-Info: <sip:office@192.0.2.5>;index=1.2.1
   CSeq: 1 INVITE
   Content-Length: 0


   F8 180 Ringing example.com -> alice

   SIP/2.0 180 Ringing
   Via: SIP/2.0/TCP example.com:5060
   From: Alice <sip:alice@example.com>
   To: Bob <sip:bob@example.com>
   Supported: histinfo
   Call-Id: 12345600@example.com
   History-Info: <sip:bob@example.com>;index=1
   History-Info: <sip:bob@192.0.2.4?Reason=SIP%3Bcause%3D302>;\
                 index=1.1;rc=1
   History-Info: <sip:office@example.com>;index=1.2;mp=1
   History-Info: <sip:office@192.0.2.5>;index=1.2.1
   CSeq: 1 INVITE
   Content-Length: 0
```

F9 INVITE example.com -> home

```
INVITE sip:home@192.0.2.6 SIP/2.0
Via: SIP/2.0/TCP proxy.example.com:5060;branch=3
Via: SIP/2.0/TCP 192.0.2.3:5060
From: Alice <sip:alice@example.com>
To: Bob <sip:bob@example.com>
Supported: histinfo
Call-Id: 12345600@example.com
Record-Route: <sip:proxy.example.com;lr>
History-Info: <sip:bob@example.com>;index=1
History-Info: <sip:bob@192.0.2.4?Reason=SIP%3Bcause%3D302>;\
              index=1.1;rc=1
History-Info: <sip:office@example.com>;index=1.2;mp=1
History-Info: <sip:office@192.0.2.5?Reason=SIP%3Bcause%3D408>;\
              index=1.2.1>;index=1.2.1
History-Info: <sip:home@example.com>;index=1.3;mp=1
History-Info: <sip:home@192.0.2.6>;index=1.3.1
CSeq: 1 INVITE
Contact: Alice <sip:alice@192.0.2.3>
Content-Type: application/sdp
Content-Length: <appropriate value>
<!-- SDP Not Shown -->
```

F10 100 Trying home -> example.com

```
SIP/2.0 100 Trying
Via: SIP/2.0/TCP proxy.example.com:5060;branch=3
Via: SIP/2.0/TCP 192.0.2.3:5060
From: Alice <sip:alice@example.com>
To: Bob <sip:bob@example.com>
Call-Id: 12345600@example.com
CSeq: 1 INVITE
Content-Length: 0
```

F11 486 Busy Here home -> example.com

```
SIP/2.0  486 Busy Here
Via: SIP/2.0/TCP proxy.example.com:5060;branch=3
Via: SIP/2.0/TCP 192.0.2.3:5060
From: Alice <sip:alice@example.com>
To: Bob <sip:bob@example.com>
Call-Id: 12345600@example.com
Record-Route: <sip:proxy.example.com;lr>
History-Info: <sip:bob@example.com>;index=1
History-Info: <sip:bob@192.0.2.4?Reason=SIP%3Bcause%3D302>;\
              index=1.1;rc=1
History-Info: <sip:office@example.com>;index=1.2;mp=1
History-Info: <sip:office@192.0.2.5?Reason=SIP%3Bcause%3D408>;\
              index=1.2.1>;index=1.2.1
History-Info: <sip:home@example.com>;index=1.3;mp=1
History-Info: <sip:home@192.0.2.6>;index=1.3.1
CSeq: 1 INVITE
Content-Length: 0
```

F12 486 Busy Here example.com -> alice

```
SIP/2.0  486 Busy Here
Via: SIP/2.0/TCP 192.0.2.3:5060
From: Alice <sip:alice@example.com>
To: Bob <sip:bob@example.com>
Call-Id: 12345600@example.com
History-Info: <sip:bob@example.com>;index=1
History-Info: <sip:bob@192.0.2.4?Reason=SIP%3Bcause%3D302>;\
              index=1.1;rc=1
History-Info: <sip:office@example.com>;index=1.2;mp=1
History-Info: <sip:office@192.0.2.5?Reason=SIP%3Bcause%3D408>;\
              index=1.2.1>;index=1.2.1
History-Info: <sip:home@example.com>;index=1.3;mp=1
History-Info: <sip:home@192.0.2.6>;index=1.3.1
CSeq: 1 INVITE
Content-Length: 0
```

F13 ACK example.com -> home

```
ACK sip:home@example.com SIP/2.0
Via: SIP/2.0/TCP proxy.example.com:5060
From: Alice <sip:alice@example.com>
To: Bob <sip:bob@example.com>
Call-Id: 12345600@example.com
CSeq: 1 ACK
Content-Length: 0
```

F14 ACK alice -> example.com

```
ACK sip:bob@example.com SIP/2.0
Via: SIP/2.0/TCP 192.0.2.3:5060
From: Alice <sip:alice@example.com>
To: Bob <sip:bob@example.com>
Call-Id: 12345600@example.com
Route: <sip:proxy.example.com;lr>
CSeq: 1 ACK
Content-Length: 0
```

B.2. History-Info with Privacy Header Field

This example provides a basic call scenario without forking. Alice has indicated that she wants Privacy associated with the History-Info header field entries. In addition, sip:biloxi.example.com adds Privacy header fields indicating that the History-info header field information is anonymized outside the biloxi.example.com domain. Note, that if the atlanta.example.com proxy had added privacy header fields to all its hi-entries, then all the hi-entries in the response would be anonymous.

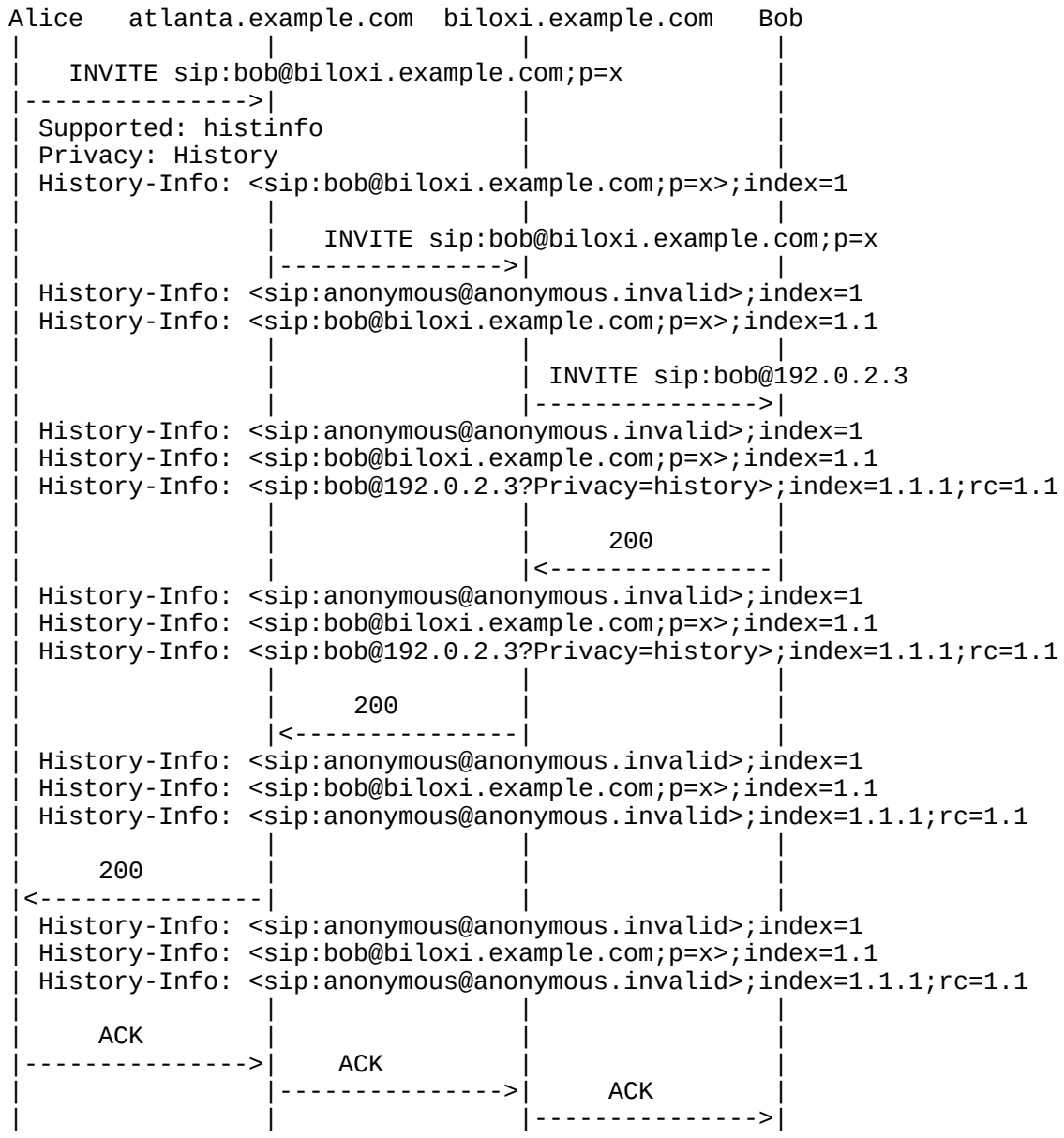


Figure 2: Example with Privacy Header Fields

B.3. Privacy for a Specific History-Info Entry

This example provides a basic call scenario similar to Appendix B.2, however, due to local policy at sip:biloxi.example.com, only the final hi-entry in the History-Info, which is Bob’s local URI, contains a privacy header field with a priv-value of "history", thus providing Alice with some information about the history of the request, but anonymizing Bob’s local URI.

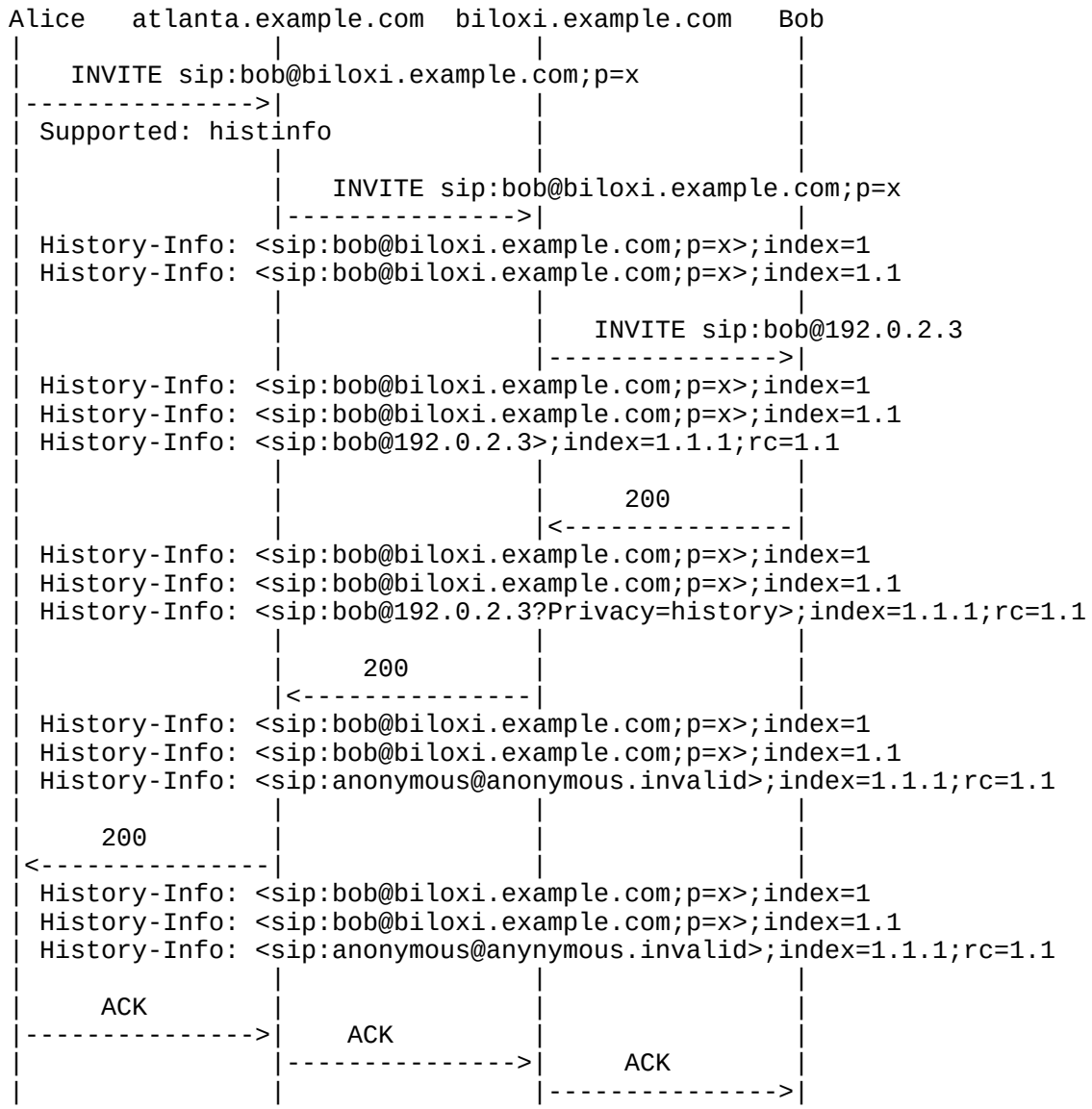


Figure 3: Example with Privacy Header Field for Specific URI

Authors' Addresses

Mary Barnes
Polycom
TX
US

Email: mary.ietf.barnes@gmail.com

Francois Audet
Skype

Email: francois.audet@skype.net

Shida Schubert
NTT

Email: shida@agnada.com

Hans Erik van Elburg
Detecon International Gmbh
Oberkasseler str. 2
Bonn,
Germany

Email: ietf.hanserik@gmail.com

Christer Holmberg
Ericsson
Hirsalantie 11, Jorvas
Finland

Email: christer.holmberg@ericsson.com