Internet Draft
Document: draft-ietf-sipping-req-history-03.txt

Mary Barnes,Editor
Mark Watson
Nortel Networks
Cullen Jennings
Cisco Systems
Jon Peterson
NeuStar, Inc.

Category: Informational
Expires November 2003

May 2003

SIP Generic Request History Capability û Requirements

Status of this Memo

Copyright Notice

Abstract

Many services that SIP is anticipated to support require the ability to determine why and how the call 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 URLs on a web page, "call history/logging" style services within intelligent "call management" software for SIP UAs and calls to voicemail servers and call centers. While SIP implicitly provides the redirect/retarget capabilities that enable calls to be routed to chosen applications, there is currently no standard mechanism within SIP for communicating the history of such a request. This "request history" information allows the receiving application to determine hints about how and why the call arrived at the application/user.

SIP Generic Request History Capability - Requirements May 2003

This draft discusses the motivations in support of a mechanism for recording the "request history", and proposes detailed requirements for such a generic "request history" capability.

Table of Contents

1. Introduction: Why define a Generic "Request History" capability?

SIP implicitly provides redirect/retarget capabilities that enable calls to be routed to specific applications as defined in [1]. The term retarget will be used henceforth in this draft to refer to the process of a Proxy Server/UAC changing a URI in a request and thus changing the target of the request. This term is chosen to avoid associating this request history only with the specific SIP Redirect Server capability that provides for a response to be sent back to a UAC requesting that the UAC should retarget the original request to an alternate URI. The rules for determining request targets as described in section 16.5 of [1] are consistent with the use of the retarget term in this draft.

The motivation for the request history is that in the process of retargeting old routing information can be forever lost. This lost information may be important history that allows elements to which the call is retargeted to process the call in a locally defined, application specific manner. The proposal in this draft is to provide a mechanism for transporting the request history. It is not

proposing any behavior for a Proxy or UA upon receipt of the information. Indeed, such behavior should be a local decision for the recipient application.

Current network applications provide the ability for elements involved with the call to exchange additional information relating to

how and why the call 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 which 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 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:

4. Some diagnostic information for debugging SIP requests.

5. A stronger security solution for SIP. A side effect is that each proxy which captures the "request history" information in a secure manner provides an additional means (without requiring signed keys) for the original requestor to be assured that the request was properly retargeted.

This draft summarizes the requirements for defining a generic mechanism for the transport of request history information. Example scenarios are provided in the appendix illustrating how a SIP building block that provides request history information could be used by some applications. It is not the intent, nor is it within the

scope, of this requirement's draft to prescribe a complete solution for any of these applications.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119.

3. "Request History" Requirements

The following list constitutes a set of requirements for a "Request History" capability. It is anticipated that some of these

requirements can be met using existing elements within SIP; whether and what SIP extensions would be needed to meet these requirements is out of scope of this draft.

1) CAPABILITY-req: The "Request History" capability will provide a capability to inform proxies and UAs involved in processing a request about the history/progress of that request. While 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) OPTIONALITY-req: The "Request History" information is optional.

2.1) In many cases, it is anticipated that whether the history is added to the Request would be a local policy decision enforced by the specific application, thus no specific protocol element is needed.

2.2) Due to the capability being "optional" from the SIP protocol perspective, the impact to an application of not having the "Request History" must be described. Applicability guidelines to be addressed by applications using this capability must be provided as part of the solution to these requirements.

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

3.1) In some scenarios, it might be possible for more than one instance of retargeting to occur within the same Proxy. A proxy

should also generate Request History information for the 'internal retargeting'.

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

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

5) CONTENT-req: The "Request History" information for each occurrence of retargeting, shall include the following:

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

5.2) The URI or address from which the request was retargeted,

5.3) The reason for the Request-URI modification,

5.4) Chronological ordering of the Request History information.

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

7) 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.

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

4. Security Considerations

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 entry either by adding an additional entry as a result of retargeting or entering invalid information.

2) Loss of privacy associated with forwarding a specific Request URI in the Request History.

3) 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.

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 source of the information.

4) SEC-req-4: To ensure the confidentiality of the Request History information, only entities which 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, either by retargeting and capturing the information, or as an application making use of the information in a Request or Response.

5. Privacy Considerations

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 [2]) 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 Request History information. Request History information subject to privacy requirements shall not be included in outgoing messages unless it is protected as described in [2].

6. IANA Considerations

This document does not have any implications for IANA.

7. References

[1] J. Rosenberg et al, "SIP: Session initiation protocol," RFC 3261, June, 2002.

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

8. Contributors

Robert Sparks contributed excellent feedback and direction for the Security considerations section of this document. In addition, he highlighted the importance of addressing the optionality aspects of the "Request History" capability.

9. Acknowledgments

The editor would like to thank Sanjoy Sen, Ben Campbell, Rohan Mahy, Jonathan Rosenberg and John Elwell for providing useful comments and suggestions related to this draft.

Authors' Addresses

Mary Barnes
Nortel Networks
2380 Performance Drive
Richardson, Texas 75082
USA

Phone: +1 972-684-5432
EMail: mbarnes@nortelnetworks.com

Mark Watson
Nortel Networks
Maidenhead Office Park (Bray House)
Westacott Way
Maidenhead, Berkshire
England

Phone: +44 (0)1628-434456
EMail: mwatson@nortelnetworks.com

Cullen Jennings
Cisco Systems
170 West Tasman Drive
MS: SJC-21/3
San Jose, CA 95134
USA

Phone: +1 408-527-9132
EMail: fluffy@cisco.com

Jon Peterson
NeuStar, Inc.

1800 Sutter Street, Suite 570
Concord, CA 94520
USA

Phone: +1 925-363-8720
EMail: Jon.Peterson@NeuStar.biz

10. Appendix A - Scenarios

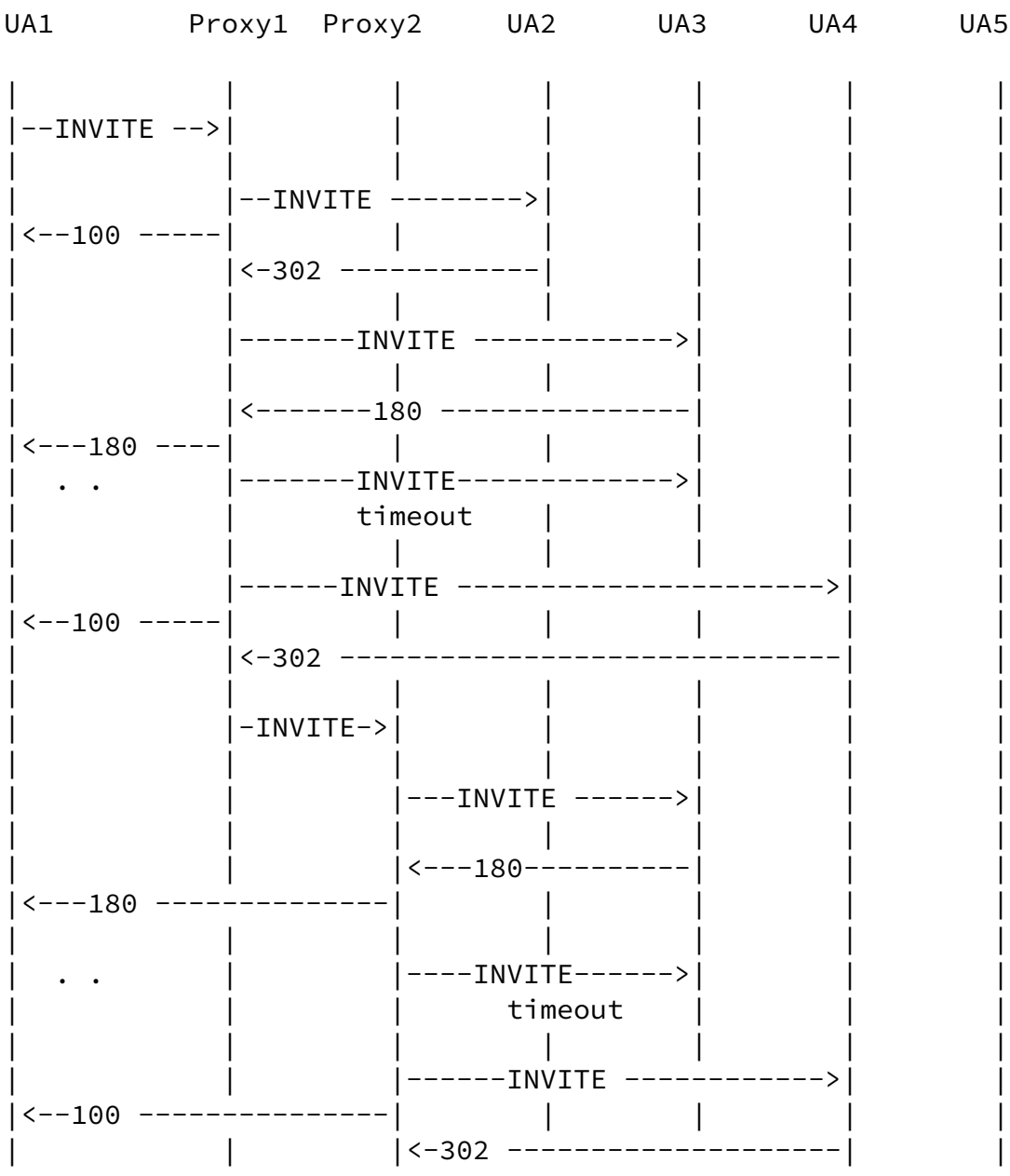
This section highlights some scenarios under which the Request History Capability could be applicable.

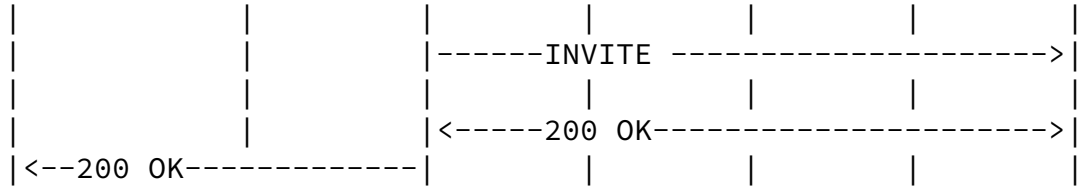
Certainly, various other solutions can be applied in some fashion to each of these scenarios. However, the objective of this draft has been to abstract the requirements from these scenarios towards providing a more robust solution for each and at the same time providing fundamental building block(s) applicable to future applications.

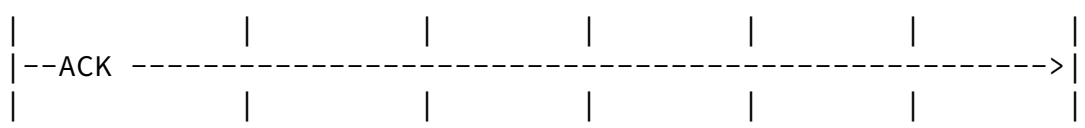
10.1 Sequentially forking with Retargeting

This scenario is as follows:

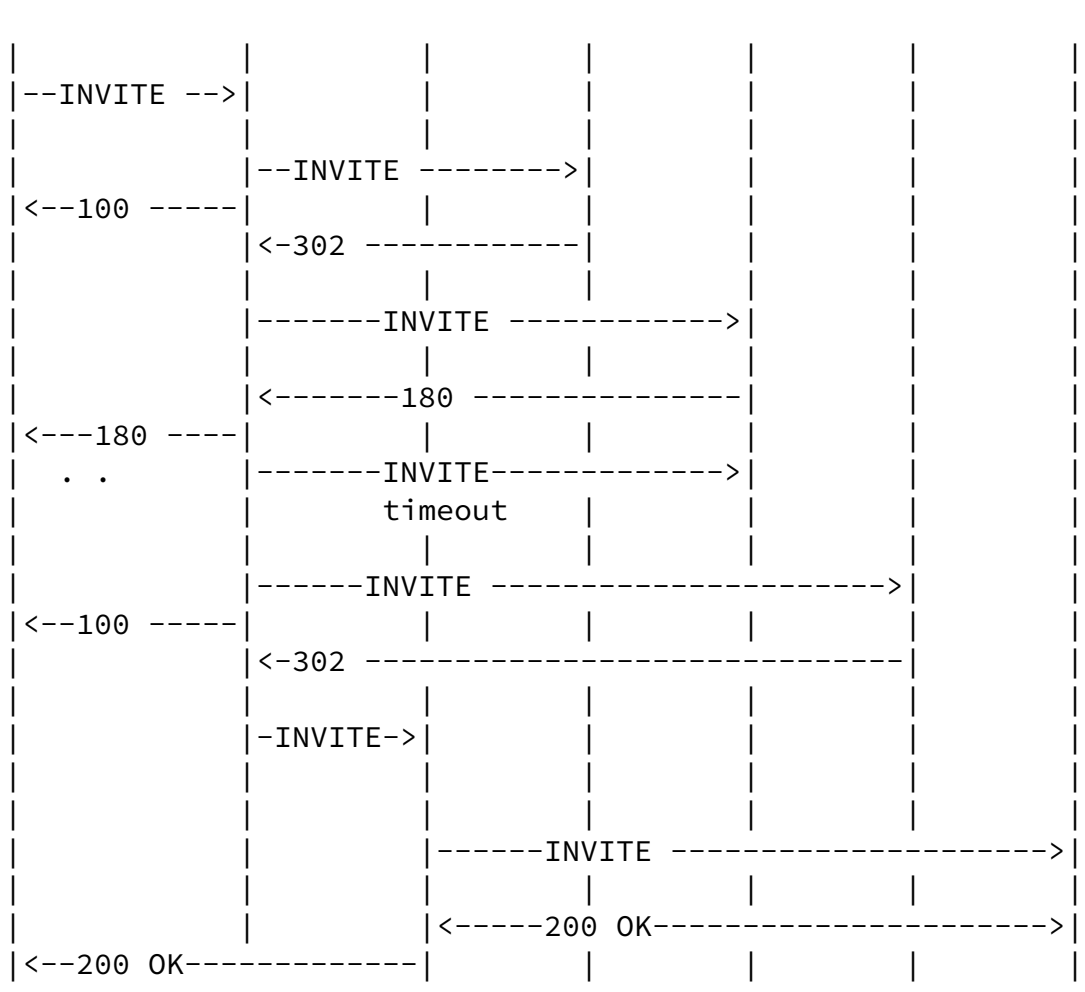
UA 1 sends a call to proxy 1. Proxy 1 sequentially tries several places (UA2, UA3 and UA4) before retargeting the call to Proxy 2. Proxy 2 unfortunately tries several of the same places (UA3 and UA4), before completing at UA5.

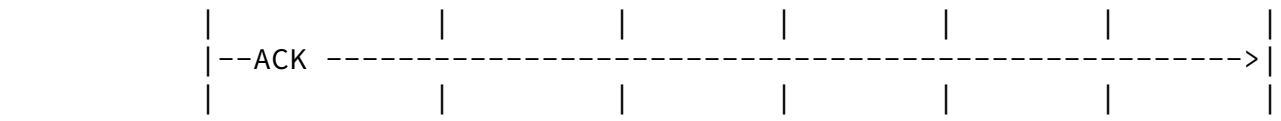






This scenario is provided to show the duplication of messaging when there isn't sufficient knowledge to optimize a sequential attempt at reaching an end user. With the "Request History" capability, this flow could be optimized as follows:

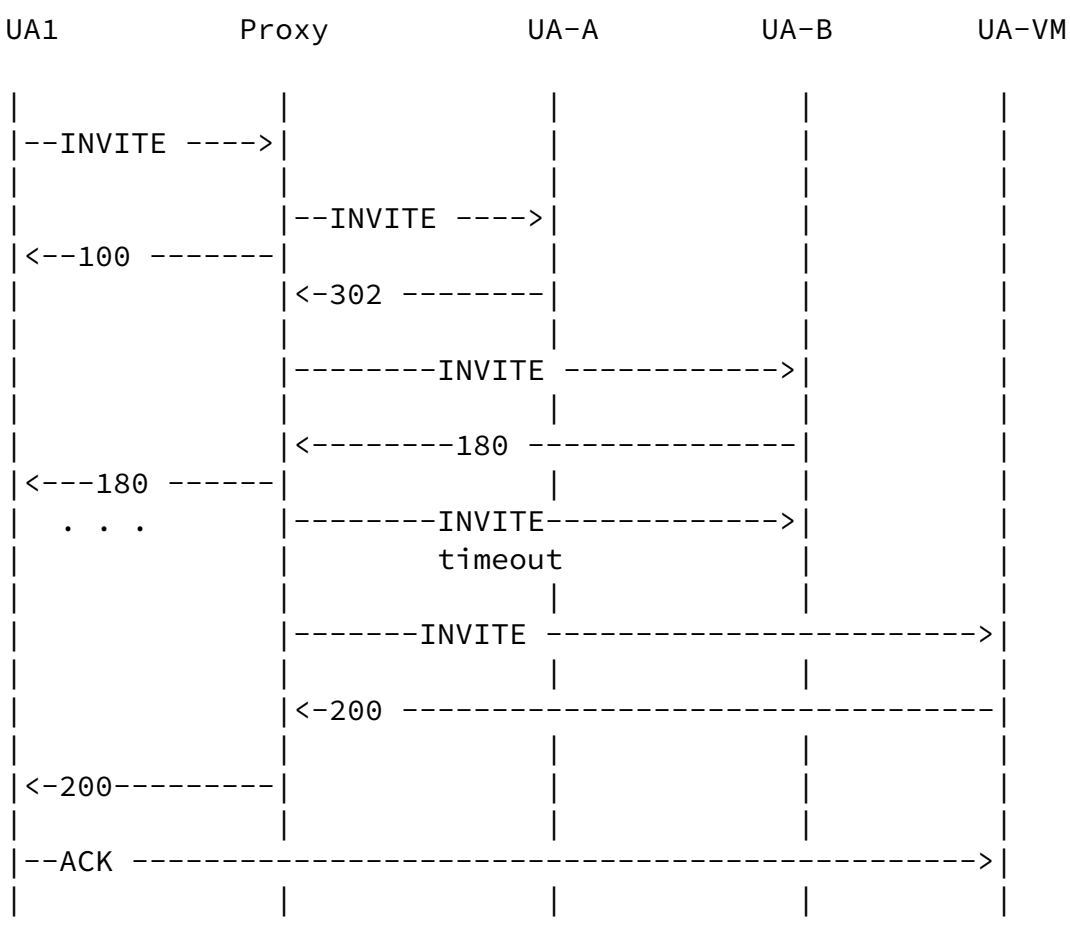




10.2 Voicemail

This scenario is as follows:

UA 1 called UA A which had been forwarded to UA B which forwarded to a UA VM (voicemail server) which needs information (e.g. reason the call was retargeted, original Request URI) to make a policy decision about what mailbox to use, which greeting to play etc. This scenario shows that something like the "Request History" capability must be used for this service to function.



Certainly, another valid scenario for the support of voicemail would be that this 'policy decision' on which mailbox to use (etc.) is made by the UA which forwarded to voicemail (UA B), or by the Proxy which performed the forwarding on behalf of B. In this case, the UA or Proxy can put all the information that the Voicemail server needs to identity the correct mailbox, etc., into the Request-URI. This fits with the SIP service paradigm where the Request-URI identifies the resource (namely, the particular mailbox/greeting etc.) that is required.

However, whilst this model is certainly applicable and required in SIP, it places service intelligence away from the system providing the key aspect of the service (the VM server).

The proposal in this draft is to rely on generic information-providing capabilities in the UA/Proxy, allowing the Voicemail system to provide more and better voicemail-related services without relying on specific capabilities in the UA/Proxy. This would allow voicemail service providers to innovate independently of the particular UA/Proxy that their customers are using, and its capabilities. Presently, with the information loss problem, VM service providers, and any other similar service providers, are limited in the services they can provide because they do not have complete information about how the call reached them. They rely on the UA/proxy of their customers having the necessary capabilities to formulate a Request-URI identifying exactly what should happen next. Finally, there is obviously a desire to use existing voicemail platforms based on PSTN/ISDN technology, which operate according to the paradigm in this example.