

**A Mechanism for Content Indirection in Session Initiation Protocol  
(SIP) Messages  
draft-ietf-sip-content-indirect-mech-03**

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on December 1, 2003.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

This document proposes an extension to the URL MIME External- Body Access-Type to satisfy the content indirection requirements for SIP. These extensions are aimed at allowing any MIME part in a SIP message to be referred to indirectly via a URI.

## Table of Contents

<a href="#">1.</a>	Terminology . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Introduction . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Example Use Cases . . . . .	<a href="#">6</a>
<a href="#">3.1</a>	Presence Notification . . . . .	<a href="#">6</a>
<a href="#">3.2</a>	Document Sharing . . . . .	<a href="#">7</a>
<a href="#">4.</a>	Requirements . . . . .	<a href="#">8</a>
<a href="#">5.</a>	Application of <a href="#">RFC2017</a> to the Content Indirection Problem .	<a href="#">9</a>
<a href="#">5.1</a>	Specifying support for content indirection . . . . .	<a href="#">9</a>
<a href="#">5.2</a>	Mandatory support for HTTP URI . . . . .	<a href="#">9</a>
<a href="#">5.3</a>	Rejecting content indirection . . . . .	<a href="#">9</a>
<a href="#">5.4</a>	Specifying the location of the content via a URI . . . . .	<a href="#">9</a>
<a href="#">5.5</a>	Specifying versioning information for the URI . . . . .	<a href="#">10</a>
<a href="#">5.6</a>	Specifying the lifetime of the URI . . . . .	<a href="#">10</a>
<a href="#">5.7</a>	Specifying the type of the indirect content . . . . .	<a href="#">10</a>
<a href="#">5.8</a>	Specifying the size of the indirect content . . . . .	<a href="#">11</a>
<a href="#">5.9</a>	Specifying the purpose of the indirect content . . . . .	<a href="#">11</a>
<a href="#">5.10</a>	Specifying multiple URIs for content indirection . . . . .	<a href="#">12</a>
<a href="#">5.11</a>	Supplying additional comments about the indirect content . .	<a href="#">12</a>
<a href="#">5.12</a>	Relationship to Call-Info, Error-Info, and Alert-Info Headers . . . . .	<a href="#">13</a>
<a href="#">6.</a>	Examples . . . . .	<a href="#">14</a>
<a href="#">6.1</a>	Single Content Indirection . . . . .	<a href="#">14</a>
<a href="#">6.2</a>	Multipart MIME with Content Indirection . . . . .	<a href="#">14</a>
<a href="#">7.</a>	Security Considerations . . . . .	<a href="#">16</a>
	References . . . . .	<a href="#">17</a>
	Author's Address . . . . .	<a href="#">17</a>
	Intellectual Property and Copyright Statements . . . . .	<a href="#">18</a>



## **1. 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 [RFC 2119](#) [[1](#)].

## **2. Introduction**

The purpose of the Session Initiation Protocol [2] (SIP) is to create, modify, or terminate sessions with one or more participants. SIP messages, like HTTP, are syntactically composed of a start line, one or more headers, and an optional body. Unlike HTTP, SIP is not designed as a general purpose transport of data.

There are numerous reasons why it might be desirable to indirectly specify the content of the SIP message body. For bandwidth limited applications such as cellular wireless, indirection provides a means to annotate the (indirect) content with meta-data which may be used by the recipient to determine whether or not to retrieve the content over the resource limited link.

It is also possible that the content size to be transferred might potentially overwhelm intermediate signaling proxies, thereby unnecessarily increasing network latency. For time-sensitive SIP applications, this may be unacceptable. Indirect content can remedy this by moving the transfer of this content out of the SIP signaling network and into a potentially separate data transfer channel.

There may also be scenarios where the session related data (body) that needs to be conveyed does not directly reside on the endpoint or User Agent. In such scenarios, it is desirable to have a mechanism whereby the SIP message can contain an indirect reference to the desired content. The receiving party would then use this indirect reference to retrieve the content via a non-SIP transfer channel such as HTTP, FTP, or LDAP.

The purpose of content indirection is purely to provide an alternative transport mechanism for SIP MIME body parts. With the exception of the transport mechanism, indirected body parts are equivalent, and should have the same treatment, as in-line body parts.

Previous attempts at solving the content indirection problem made use of the text/uri-list [7] MIME type. While attractive for its simplicity (a list of URIs delimited by end-of-line markers), it fails to satisfy a number of the requirements for a more general purpose content indirection mechanism in SIP. Most notably lacking is the ability to specify various attributes on a per-URI basis. These attributes might include version information, the MIME type of the referenced content, etc.

In searching for a replacement for the text/uri-list MIME type, [RFC2017](#) defines a strong candidate. [RFC2017](#) defines an extension to the message/external-body MIME type originally defined in [RFC2046](#)



[5]. The extension that [RFC2017](#) makes is to allow a generic URI to specify the location of the content rather than protocol specific parameters for FTP, etc. as originally defined in [RFC2046](#). While providing most of the functionality needed for a SIP content indirection mechanism, [RFC2017](#) by itself is not a complete solution. This document will specify the usage of [RFC2017](#) necessary to fulfill the requirements outlined for content indirection.

The requirements can be classified as applying either to the URI which indirectly references the desired content or to the content itself. Where possible, existing MIME parameters and entity headers will be used to satisfy those requirements. MIME (Content-Type) parameters will be the preferred manner of describing the URI while entity headers will be the preferred manner of describing the (indirect) content. See [RFC 2045](#) [4] for a description of most of these entity headers and MIME parameters.





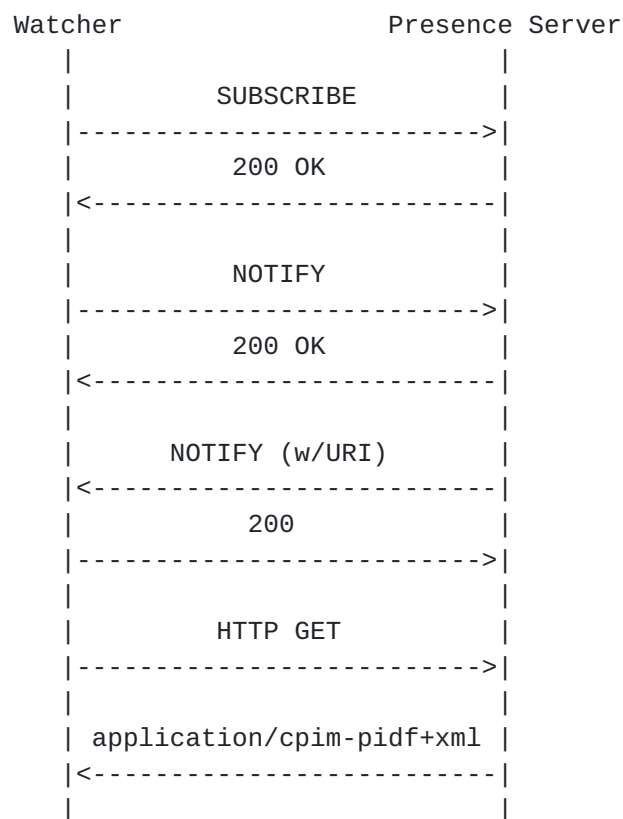
### 3. Example Use Cases

There are several example users of such a content indirection mechanism. These are examples only and are not intended to limit the scope or applicability of the mechanism.

#### 3.1 Presence Notification

The information carried in a presence document could potentially exceed the recommended size for a SIP (NOTIFY) request, particularly if the document carries aggregated information from multiple endpoints. In such a situation, it would be desirable to send the NOTIFY request with an indirect pointer to the presence document which could then be retrieved by, for example, HTTP.

Figure 1: Example information flow for presence notification



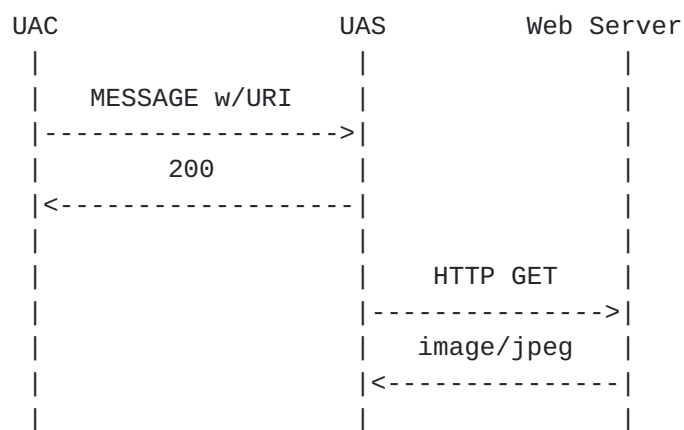
In this example, the presence server returns an HTTP URI pointing to a presence document on the presence server which the watcher can then fetch using an HTTP GET.



### 3.2 Document Sharing

During an instant messaging conversation, a useful service is document sharing wherein one party sends an IM (MESSAGE request) with an indirect pointer to a document which is meant to be rendered by the remote party. Carrying such a document directly in the MESSAGE request is not appropriate for most documents. Furthermore, the document to be shared may reside on a completely independent server from the originating party.

Figure 2: Example information flow for document sharing



In this example, a user wishes to exchange a JPEG image that she has stored on her web server with another user she has a IM conversation with. The JPEG is intended to be rendered inline in the IM conversation. The recepiant of the MESSAGE request launches a HTTP GET request to the web server to retrieve the JPEG image.



#### **4. Requirements**

It MUST be possible to specify the location of content via a URI [3].

It MUST be possible to specify the length of the indirect content.

It MUST be possible to specify the type of the indirect content.

It MUST be possible to specify the disposition of each URI independently.

It MUST be possible to label each URI to identify if and when the content referred to by that URI has changed. Applications of this mechanism may send the same URI more than once. The intention of this requirement is to allow the receiving party to determine if the content referenced by the URI has changed without having to actually retrieve that content. Example ways the URI could be labelled include a sequence number, timestamp, version number, etc.

It MUST be possible to specify the timespan for which a given URI is valid. This may or may not be the same as the lifetime for the content itself.

It MUST be possible for the UAC and the UAS to indicate support of this content indirection mechanism. A fallback mechanism SHOULD be specified in the event that one of the parties is unable to support content indirection.

It MUST be possible for the UAC and UAS to negotiate the type of the indirect content when using the content indirection mechanism.

It MUST be possible for the UAC and UAS to negotiate support for URI scheme(s) to be used in the content indirection mechanism. This is in addition to the ability to negotiate the content type.

It SHOULD be possible to ensure the integrity and privacy of the URI when it is received by the remote party.

It MUST be possible to process the content indirection without human intervention.

It MUST allow for indirect transference of content in any SIP message which would otherwise carry that content as a body.



## **5. Application of [RFC2017](#) to the Content Indirection Problem**

The following text describes the application of [RFC2017](#) to the requirements for content indirection.

### **5.1 Specifying support for content indirection**

A UAC/UAS may indicate support for content indirection through an Accept header containing the message/external-body MIME type. The UAC/UAS must supply additional values in the Accept header to indicate the content types that it is willing to accept either directly or through content indirection. User-Agents supporting content indirection **MUST** support content indirection of the application/sdp MIME type.

For example:

```
Accept: message/external-body, image/*, application/sdp
```

### **5.2 Mandatory support for HTTP URI**

Applications which use this content indirection mechanism **MUST** support at least the HTTP URI scheme. Additional URI schemes **MAY** be used, but a UAC/UAS **MUST** support receiving a HTTP URI for indirect content if it advertises support for content indirection.

The intention is to establish a baseline of support to further strengthen interoperability. Implementors may design for the most common case (HTTP) without having to worry about negotiation of support for this particular URI scheme.

### **5.3 Rejecting content indirection**

If a UAS receives a SIP request which contains a content indirection payload, and the UAS cannot or does not wish to support such a content type, it **MUST** reject the request with a 415 Unsupported Media Type response as defined in [section 21.4.13](#) of SIP [2]. In particular, the UAC should note the absence of the message/external-body MIME type in the Accept header of this response to indicate that the UAS does not support content indirection.

### **5.4 Specifying the location of the content via a URI**

The URI for the indirect content is specified in a "URI" parameter of the message/external-body MIME type. An access-type parameter indicates that the external content is referenced by a URI.





For example:

```
Content-Type: message/external-body;  
             access-type="URL";  
             URL="http://www.volcano.com/the-indirect-content"
```

### **5.5 Specifying versioning information for the URI**

In order to determine whether or not the content indirectly referenced by the URI has changed, a Content-ID entity header is used. The syntax of this header is defined in [RFC2045](#) [4]. Changes in the underlying content referred to by a URI MUST result in a change in the Content-ID associated with that URI. Multiple SIP messages carrying URI that refer to the same content SHOULD reuse the same Content-ID to allow the receiver to cache this content and avoid unnecessary retrievals. The Content-ID is intended to be globally unique and SHOULD be temporally unique across SIP dialogs.

For example:

```
Content-ID: <4232423424@www.volcano.com>
```

### **5.6 Specifying the lifetime of the URI**

The URI supplied by in Content-Type header is not required to be accessible or valid for an indefinite period of time. Rather, the supplier of the URI MUST specify the time period for which this URI is valid and accessible. This is done through an "EXPIRATION" parameter of the Content-Type. The format of this expiration parameter is a [RFC1123](#) date-time value. This is further restricted in this application to use only GMT time, consistent with the Date: header in SIP. This is a mandatory parameter. Note that the date-time value can range from minutes to days or even years.

For example:

```
Content-Type: message/external-body;  
             expiration="Mon, 24 June 2002 09:00:00 GMT"
```

### **5.7 Specifying the type of the indirect content**

To support existing SIP mechanisms for the negotiation of content



types, a Content-Type entity header SHOULD be present in the entity (payload) itself. If the protocol (scheme) of the URI supports its own content negotiation mechanisms (e.g. HTTP), this header may be omitted. The sender MUST however be prepared for the receiving party to reject content indirection if the receiver is unable to negotiate an appropriate MIME type using the underlying protocol for the URI scheme.

For example:

```
Content-Type: message/external-body; access-type="URL";
              expiration="Mon, 24 June 2002 09:00:00 GMT";
              URL="http://www.volcano.com/the-indirect-content"
<CRLF>
Content-Type: application/sdp
<CRLF>
```

### **5.8 Specifying the size of the indirect content**

When known in advance, the size of the indirect content should be supplied via a size parameter on the Content-Type header. This is an extension of [RFC2017](#) but in line with other access types defined for the message/external-body MIME type in [RFC2046](#). The content size is useful for the receiving party to make a determination about whether or not to retrieve the content. As with directly supplied content, a UAS may return a 513 error response in the event the content size is too large. This is an optional parameter.

For example:

```
Content-Type: message/external-body; access-type="URL";
              expiration="Mon, 24 June 2002 09:00:00 GMT";
              URL="http://www.volcano.com/the-indirect-content";
              size=4123
```

### **5.9 Specifying the purpose of the indirect content**

A Content-Disposition entity header SHOULD be present for all indirect content. In the absence of an explicit Content-Disposition header, a content disposition of "session" should be assumed.

For example:



```
Content-Type: message/external-body; access-type="URL";
              expiration="Mon, 24 June 2002 09:00:00 GMT";
              URL="http://www.volcano.com/the-indirect-content"
<CRLF>
Content-Type: image/jpeg
Content-Disposition: render
```

### **5.10 Specifying multiple URIs for content indirection**

If there is a need to send multiple URIs for the purpose of content indirection, an appropriate multipart MIME type [5] should be used. Each URI should be contained in a single entity. Indirect content may be mixed with directly supplied content. This is particularly useful with the multipart/alternative MIME type.

For example:

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary=boundary42

--boundary42
Content-Type: text/plain; charset=us-ascii

The company announcement for June, 2002 follows:
--boundary42
Content-Type: message/external-body;
              access-type="URL";
              expiration="Mon, 24 June 2002 09:00:00 GMT";
              URL="http://www.volcano.com/announcements/07242002";
              size=4123

Content-Type: text/html
Content-Disposition: render

--boundary42--
```

### **5.11 Supplying additional comments about the indirect content**

Optional, freeform text may be supplied to comment on the indirect content. This should be supplied in a Content-Description entity header.

For example:



```
Content-Type: message/external-body;  
             access-type="URL";  
             expiration="Mon, 24 June 2002 09:00:00 GMT";  
             URL="http://www.volcano.com/the-indirect-content";  
             size=52723  
  
<CRLF>  
Content-Description: Multicast gaming session
```

### **[5.12](#) Relationship to Call-Info, Error-Info, and Alert-Info Headers**

SIP [2] defines three headers which are used to supply additional information with regard to a session, a particular error response, or alerting. All three of these headers allow the UAC or UAS to indicate additional information through a URI. They may be considered a form of content indirection. The content indirection mechanism defined in this document is not intended as a replacement for these headers. Rather, the headers defined in SIP MUST be used in preference to this mechanism where applicable because of the well defined semantics of those headers.





## **6. Examples**

### **6.1 Single Content Indirection**

```
INVITE sip:boromir@volcano.com SIP/2.0
From: <sip:gandalf@nwt.com>;tag=347242
To: <sip:boromir@volcano.com>
Call-ID: 3573853342923422@nwt.com
CSeq: 2131 INVITE
Accept: message/external-body application/sdp
Content-Type: message/external-body;
             ACCESS-TYPE=URL;
             URL="http://www.nwt.com/party/06/2002/announcement";
             EXPIRATION="Sat, 20 Jun 2002 12:00:00 GMT"
             size=231
Content-Length: ...

Content-Type: application/sdp
Content-Disposition: session
Content-ID: <4e5562cd1214427d@nwt.com>
```

### **6.2 Multipart MIME with Content Indirection**

```
MESSAGE sip:boromir@volcano.com SIP/2.0
From: <sip:gandalf@nwt.com>;tag=34589882
To: <sip:boromir@volcano.com>
Call-ID: 9242892442211117@nwt.com
CSeq: 388 MESSAGE
Accept: message/external-body, text/html, text/plain, image/*, text/x-
emoticon
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary=zz993453

--zz993453
Content-Type: message/external-body;
             access-type="URL";
             expiration="Mon, 24 June 2002 09:00:00 GMT";
             URL="http://www.nwt.com/company_picnic/image1.png"
             size=234422

Content-Type: image/png
Content-ID: <9535035333@nwt.com>
Content-Disposition: render
Content-Description: Kevin getting dunked in the wading pool
```



--zz993453

Content-Type: message/external-body;  
    access-type="URL";  
    expiration="Mon, 24 June 2002 09:00:00 GMT";  
    URL="http://www.nwt.com/company\_picnic/image2.png"  
    size=233811

Content-Type: image/png  
Content-ID: <1134299224244@nwt.com>  
Content-Disposition: render  
Content-Description: Peter on his tricycle

--zz993453--



## **7. Security Considerations**

Any content indirection mechanism introduces additional security concerns. By its nature, content indirection requires an extra processing step and information transfer. There are a number of potential abuses of a content indirection mechanism:

Content indirection allows the initiator to choose an alternative protocol with weaker security or known vulnerabilities for the content transfer. For example, asking the recipient to issue an HTTP request which results in a Basic authentication challenge.

Content indirection allows the initiator to ask the recipient to consume additional resources in the information transfer and content processing, potentially creating an avenue for denial of service attacks. For example, an active FTP URL consuming 2 connections for every indirect content message.

Content indirection could be used as a form of port scanning attack where the indirect content URL is actually a bogus URL pointing to an internal resource of the recipient. The response to the content indirection request could reveal information about open (and vulnerable) ports on these internal resources.

A content indirection URL can disclose sensitive information about the initiator such as an internal user name (as part of an HTTP URL) or possibly geolocation information.

Fortunately, all of these potential threats can be mitigated through careful screening of both the indirect content URIs that are received as well as those that are sent. Integrity and privacy protection of the indirect content URI can prevent additional attacks as well.

For confidentiality, integrity, and authentication, this content indirection mechanism relies on the security mechanisms outlined in [RFC3261](#). In particular, the usage of S/MIME as defined in [section 23 of RFC3261](#) provides the necessary mechanism to ensure integrity protection and privacy of the indirect content URI and associated parameters.

Securing the transfer of the indirect content is the responsibility of the underlying protocol used for this transfer. It is RECOMMENDED that applications implementing this content indirection method support the HTTPS URI scheme for secure transfer of content.

Access control to the content referenced by the URI is not defined by this specification. Access control mechanisms may be defined by the protocol for the scheme of the indirect content URI.



## References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [2] 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.
- [3] Berners-Lee, T., Fielding, R. and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", [RFC 2396](#), August 1998.
- [4] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", [RFC 2045](#), November 1996.
- [5] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", [RFC 2046](#), November 1996.
- [6] Freed, N. and K. Moore, "Definition of the URL MIME External-Body Access-Type", [RFC 2017](#), October 1996.
- [7] Daniel, R., "A Trivial Convention for using HTTP in URN Resolution", [RFC 2169](#), June 1997.

## Author's Address

Sean Olson  
Microsoft  
One Microsoft Way  
Redmond, WA 98052  
US

Phone: +1-425-707-2846  
EMail: [seanol@microsoft.com](mailto:seanol@microsoft.com)  
URI: <http://www.microsoft.com/rtc>





## Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in [BCP-11](#). Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

## Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION



HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF  
MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

#### Acknowledgement

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