Lemonade HTTP Binding

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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

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

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

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

Abstract

As part of the LEMONADE work to define extensions to the IMAPv4 Rev1 protocol [RFC3501] and SMTP that provide optimizations in a variety of settings, this document describes an alternative, optional binding showing how HTTP can be used to transfer IMAPv4 and SMTP commands and responses. This binding is intended to facilitate the use of IMAP and SMTP in deployments involving a variety of intermediaries.

Conventions used in this document

In examples, "C:" and "S:" indicate lines sent by the client and server respectively.
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].

An implementation is not compliant if it fails to satisfy one or more of the MUST or REQUIRED level requirements for the protocol(s) it implements. An implementation that satisfies all the MUST or REQUIRED level and all the SHOULD level requirements for a protocol is said to be "unconditionally compliant" to that protocol; one that satisfies all the MUST level requirements but not all the SHOULD level requirements is said to be "conditionally compliant." When describing the general syntax, some definitions are omitted as they are defined in [RFC3501], [RFC821], and related documents.

Table of Contents

Status of this Memo.............................................1
Abstract.....................................................................1
Conventions used in this document...........................1
Table of Contents..................................................2
1. Introduction and motivation.........................2
   2. Using HTTP as an alternative binding for IMAP.........4
      2.1. Non-Persistent HTTP for In-response Connectivity Mode..5
      2.2. Using Persistent HTTP/HTTPS + Chunked Transfer Encoding for In-band Connectivity Mode........6
      2.3. Using HTTP CONNECT...................................8
      2.4. Using HTTP as a binding for SMTP....................8
3. Security Considerations.................................8
4. References..................................................9
5. Future Work...............................................10
6. Version History...........................................10
Acknowledgments................................................11
Authors Addresses..............................................11
Intellectual Property Statement..........................13
Full Copyright Statement..................................13

1. Introduction and motivation

As part of the LEMONADE goal to define extensions to the IMAPv4 Rev1 protocol [RFC3501] for providing optimizations in a variety of settings, this document describes how HTTP can optionally be used to transfer IMAP and SMTP commands and responses. This binding is intended to facilitate the use of IMAP and SMTP in deployments involving a variety of intermediaries, and offers a standardized alternative to existing proprietary implementations of such a feature.
The need for an optional HTTP binding is driven by the needs of the mobile network operator community (see [MEAMAIL][OMA-ME-RD]), where the reuse of a widely deployed and well-understood technology will allow operators to reuse their experience in solving practical deployment issues. Specifically, HTTP allow operators to reuse a similar setup and model that is already used for many other similar and related services, such as certain proprietary push e-mail and synchronization offerings, OMA Data Synchronization, Web services and Web access.

Using HTTP/HTTPS can simplify deployment in a corporate network through the potential use of a reverse proxy to achieve end-to-end encryption. This also has the advantage of not requiring changes to any firewall configurations and reduces the concerns that this often presents to corporations. In general the solution is compatible with any existing firewall. A reverse proxy can also support deployment models that offer roles to other service providers in the value chain, as discussed in [OMA-ME-AD].

Another advantage is that the confidentiality, integrity, and compression capabilities used with HTTP and already implemented in a wide range of existing mobile devices can also be reused.

Studies have also shown that a persistent HTTP session has usually proven more resilient than an IMAP IDLE over TCP connection over an unreliable bearer such as a GPRS-based mobile network. It is conjectured that this results from the properties and settings of the gateways and equipment in the operator’s core network infrastructure that have HTTP / HTTPS ports time out differently that other ports. It is unclear if this is easily addressable by changing settings or configurations.

The use of HTTP as an underlying protocol for other application protocols has received much attention (see [RFC3205]). In particular, the concern exists that this circumvents firewall security policies. Another concern is the potential misuse or neglect of HTTP semantics by the application protocol that uses HTTP as a substrate.

Note that if the suppression of IMAP (or indeed any other application) traffic on HTTP/HTTPS is an issue, firewall administrators can still prevent such passage and this can provide incentives to re-configure firewalls to allow solutions on other transports (e.g. TLS) or offer the HTTP-based solution using another provisioned ports (e.g. manually, out of band or via instructions like XGETIPLPREFS (see [NOTIFICATIONS])). The aim, therefore, is to allow for the use of this solution in the widest possible set of circumstances by codifying a standard way to do so that works with existing, deployed (i.e., HTTP only) firewalls, while explicitly allowing the possibility of detecting and filtering such traffic.
using the HTTP Content-Type header in deployments where this is not permitted.

2. Using HTTP as an alternative binding for IMAP

To use HTTP/HTTPS as the transfer protocol for IMAP commands and responses between the IMAP client and server, the client MUST send an HTTP POST request to the server, and embed IMAP commands (commands to an IMAPv4 Rev1 server or IMAP servers supporting Lemonade extensions) in the body of the request. A server MUST reject a HTTP GET request from the client. The content-type header of the POST request MUST be set to "application/vnd.lemonade". Multiple IMAP commands may be included in one POST request.

In what follows, the term Lemonade client/server is used to refer to a client/server that supports both IMAPv4 Rev1 as well as any LEMONADE extensions.

When the HTTP binding is used, the Lemonade server listens on whatever port has been configured for this.

The following is an example of a possible Lemonade HTTP request:

```
POST /lemonadePath HTTP/1.1 <CRLF>
Content-Type: application/vnd.lemonade <CRLF>
[other headers] <CRLF>
<tag> SP <Lemonade command> <CRLF>
[<tag> SP <Lemonade command> <CRLF>] <CRLF>
```

The Lemonade command MUST be plain text (7bit).

Multiple Lemonade commands MAY be sent on the same request. Thus Lemonade commands must be tagged. The client must be able to deal with recovering from errors when commands are batched. See RFC2442 Batch SMTP for a further discussion.

The Content-Type header is the only HTTP headers that MUST be sent to a Lemonade server. Other headers such as Cache-Control MAY be included.

When the Lemonade server sends back a response it MUST be in the following format:

```
HTTP/1.1 <HTTP Status Code> <CRLF>
Content-Type: text/plain <CRLF>
<CRLF>
```
Notes:
The Lemonade Server uses the following HTTP status codes, and what each code indicates is given below:
- 200
  - This indicates normal execution of the Lemonade commands from a IMAP perspective. The client should further parse the response body to get the tagged responses to the commands and process those accordingly.
- 500
  - This indicates that at least one command caused an internal server error, meaning the Lemonade Server failed to execute the command. In conforming to HTTP semantics, this means the IMAP server responses such as BAD or NO IMAP generate a HTTP 500 response code.

When using HTTP to transfer IMAP commands and responses, the client SHOULD utilize built-in features of HTTP to their advantage. For example, the client SHOULD use HTTPS instead of HTTP whenever possible, since HTTPS has built in encryption and MAY use its compression capabilities. STARTTLS should not be needed in this case, as it just adds overhead without providing any additional benefit.

HTTP can be used in both in-response and in-band modes. Details about these transport modes are given in the following two subsections.

2.1.
Non-Persistent HTTP for In-response Connectivity Mode

If the client uses a traditional HTTP connection (either by establishing a different socket for each HTTP request to the Lemonade server, or by reusing the same socket for all HTTP requests, but sending each request under its own header), it has in-response connectivity to the server. The client can issue as many commands as it would like in one HTTP request to the server, and the server responds by sending back one HTTP response with all the responses to all the commands in the HTTP request. With this connectivity mode, the IDLE command cannot be issued. Other commands that use a continuation response cannot be issued unless the LITERAL+ [RFC2088] extension is supported.

In order for the server to identify separate HTTP requests as belonging to the same session, an in-response HTTP client needs to
accept cookies. A session-id is passed in the cookie to identify the session.

Thus, the headers for a HTTP In-response Response after the client has issued its first HTTP request to the server.

HTTP/1.1 <HTTP Status Code> <CRLF>
Content-Type: text/plain <CRLF>
Set-Cookie: JSESSIONID=94571a8530d91e1913bfydafa;
path=/lemonade<CRLF>
<CRLF>

The client must then save this cookie and send it back to the server with the next request in order for the server to reattach these commands to the same session as the previous commands.

POST /lemonadePath HTTP/1.1 <CRLF>
Content-Type: application/vnd.lemonade <CRLF>
Cookie: JSESSIONID=94571a8530d91e1913bfydafa
[other headers]
<CRLF>
<tag> SP <Lemnade Server response> <CRLF>
[[untagged responses]]
<tag> SP <Lemonade Server response> <CRLF>
]

2.2.
Using Persistent HTTP/HTTPS + Chunked Transfer Encoding for In-band Connectivity Mode

It is possible to use persistent HTTP or persistent HTTPS plus chunked-transfer-encoding so that the server can instantly send notifications to the client while a session is open. The client needs to open a persistent connection and keep it active. In this case, the HTTP headers must be sent the first time the client device opens the connection to the Lemonade Server and these headers MUST set the transfer coding to be chunk-encoded [RFC2616, Sec. 3.6.1]. All subsequent client-server requests are written to the open connection, without needing any additional headers negotiations. The server can use this open channel to push events to the client device at any time. In this case, the client SHOULD NOT accept cookies.

The client must send the HTTP headers one time only:

POST /lemonadeServletPath HTTP/1.1 <CRLF>
Content-Type: application/vnd.lemonade <CRLF>
Connection: keep-alive <CRLF>
Pragma: no-cache <CRLF>
Transfer-Encoding: chunked <CRLF>

The server responds with the following header:

HTTP/1.1 <HTTP Status Code> <CRLF>
Cache-Control: private
Keep-Alive: timeout=15, max=100 (or other suitable setting)
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/plain

Then the client can send a command anytime it wants with the following format:

<length of Lemonade command, including bytes in CRLF> <CRLF>
<tag> SP <Lemonade command> <CRLF>
<CRLF>

And example of an actual client command is:

e <CRLF>
2 CAPABILITY<CRLF>
<CRLF>

The server responds to each command with as many untagged responses as needed, and one tagged response, where each response is in the format that follows:

<length of a single response, including bytes in CRLF> <CRLF>
<tagged or untagged response> <CRLF>
<CRLF>

An actual Server response might be:

d5 <CRLF>
* CAPABILITY IMAP4REV1 AUTH=LOGIN NAMESPACE SORT MULTIAPPEND LITERAL+ UIDPLUS IDLE XORACLE X-ORACLE-LIST X-ORACLE-COMMENT X-ORACLE-QUOTA X-ORACLE-PREF X-ORACLE-MOVE X-ORACLE-DELETE ACL X-ORACLE-PASSWORD LDELIVER LZIP LCONVERT LFILTER LSETPREF LGETPREF <CRLF> 1b <CRLF>
2 OK CAPABILITY completed <CRLF>
<CRLF>

Note however that the HTTP protocol is in general not meant to be used in such a way. To maintain such an open channel might be a practical challenge to proxies/firewalls, which might not forward the requests chunk by chunk to the server, and meanwhile route responses back to the client chunk by chunk. Consequently the session closes. Chunked transfer encoding requests may not always be honored by an
HTTP server. In cases where such requests are denied, the client SHOULD be prepared to use the non-chunked encoding technique from section 2.1

The same challenges exist for a TCP session.

In any case, the session can be automatically started again by the client after a lost connection or by the server through out-of-band; after some defined time-out.

2.3. Using HTTP CONNECT

If a HTTP proxy server is available to the client which supports the HTTP CONNECT method, and the IMAP server the user wishes to reach allows external connections from outside the destination network’s firewall, the client may wish to tunnel a regular TCP connection through the HTTP proxy. See [LUOTONEN] or section 5.2 of [RFC2817] for a detailed description of the technique.

Note that HTTP Proxy servers may not honor all CONNECT requests, and may in fact, limit CONNECT requests to a small number of common ports, such as 80, 443, 8080, etc. It is advised that networks wishing to allow their users to use this feature allow clients within their network to CONNECT to ports 25, 143, 587, and 993.

2.4. Using HTTP as a binding for SMTP

All of the techniques described in sections 2.1, 2.2, and 2.3 may be used for SMTP as well. The only difference between IMAP and SMTP will be the HTTP URL used. Servers implementing the HTTP binding are expected to differentiate between IMAP and SMTP protocol bodies via the URL.

3. Security Considerations

This binding has the same security requirements as IMAP when using an in-response or inband connectivity mode.

The HTTPS protocol can be used to provide end-to-end security.

Proxy-based implementations may still require payload encryption for end-to-end security.

Caching is a concern. The client SHOULD use the HTTP Cache-Control directive (no-cache, no-store, must-revalidate, or combinations thereof) to inform proxy servers, origin servers, and client libraries not to cache or store the HTTP response. To deal with HTTP
1.0 servers that may exist in the network, Pragma: no-cache should be used as well.

Firewall administrators wishing to block stealth deployments of HTTP IMAP bindings may block HTTP requests with Content-Type application/vnd.lemonade via an application level firewall.

4. References


[LUOTONEN] Luotonen, A., ÂTunneling TCP based protocols through Web proxy serversÂ, draft-luotonen-web-proxy-tunneling-01.txt, August 1998


Future Work

[1] Should an OPTIONS HTTP request be supported to allow a client to probe HTTP binding capabilities, such as which protocol a given URL is bound to, or whether chunking is supported?

[2] Should separate content types exist for IMAP and SMTP since the entity body in the HTTP request is different?

[3] Standardizing the form of the URL for the binding may permit firewall administrations to impose better filtering.

[4] Evaluating possible binding recommendations for SOAP, REST and / or WebDAV.

Version History

Release 03
New section on CONNECT
Added SMTP and Future Work
Updated security section with caching and firewall administration
Clarified caching policy.
Update of reference section

Release 02
Removed material on Notifications and connectivity models
Updated introduction with motivation
Editorial corrections
New section that allows to select the HTTP URL.

Editorial updates

Release 01
Detail updates of the text throughout the document following lessons learned so far in P-IMAP 07 [P-IMAP].

Release 00

Acknowledgments

The authors want to thank all who have contributed key insight and extensively reviewed and discussed the concepts of HTTP Bindings and its early introduction in P-IMAP [P-IMAP].

Authors Addresses

Stephane H. Maes
Oracle Corporation
500 Oracle Parkway
M/S 4op634
Redwood Shores, CA 94065
USA
Phone: +1-650-607-6296
Email: stephane.maes@oracle.com

Rafiul Ahad
Oracle Corporation
500 Oracle Parkway
Redwood Shores, CA 94065
USA

Eugene Chiu
Oracle Corporation
500 Oracle Parkway
Redwood Shores, CA 94065
USA

Ray Cromwell
Oracle Corporation
500 Oracle Parkway
Redwood Shores, CA 94065
USA

Jia-der Day
Oracle Corporation
500 Oracle Parkway
Redwood Shores, CA 94065
USA

Wook-Hyun Jeong
Samsung Electronics, CO., LTD
416, Maetan-3dong, Yeongtong-gu,
Suwon-city, Gyeonggi-do,
Korea 442-600
Tel: +82-31-279-8289
E-mail: wh75.jeong@samsung.com

Chang Kuang
Oracle Corporation
500 Oracle Parkway
Redwood Shores, CA 94065
USA

Rodrigo Lima
Oracle Corporation
500 Oracle Parkway
Redwood Shores, CA 94065
USA

Nilo Mitra
Ericsson
Tel: +1 212-843-8451
Email: nilo.mitra@ericsson.com

Gustaf Rosell
Sony Ericsson
P.O. Box 64
SE-164 94 Kista,
Sweden
Tel: +46 8 508 780 00

Jean Sini
6480 Via Del Oro
San Jose, CA 95119
USA

Sung-Mu Son
LG Electronics
Mobile Communication Technology Research Lab.
Tel: +82-31-450-1910
E-Mail: sungmus@lge.com

Fan Xiaohui
Product Development Division
R&D CENTER
CHINA MOBILE COMMUNICATIONS CORPORATION (CMCC)
ADD: 53A, Xibianmennei Ave., Xuanwu District, Beijing, 100053, China
TEL: +86 10 66006688 EXT 3137
Zhao Lijun
CMCC R&D
ADD: 53A, Xibianmennei Ave., Xuanwu District, Beijing, 100053, China
TEL: 8610.66006688.3041

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 implementers 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.

Acknowledgement

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

Full Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED,