

Internet Engineering Task Force (IETF)
Request for Comments: 6758
Category: Informational
ISSN: 2070-1721

A. Melnikov
Isode Ltd
K. Carlberg
G11
October 2012

Tunneling of SMTP Message Transfer Priorities

Abstract

This memo defines a mechanism for tunneling of SMTP (Simple Mail Transfer Protocol) Message Transfer Priority values through MTAs (Message Transfer Agents) that don't support the MT-PRIORITY SMTP extension.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <http://www.rfc-editor.org/info/rfc6758>.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
2. Conventions Used in This Document	3
3. Handling of Messages Received via SMTP	4
3.1. Handling of the MT-PRIORITY Parameter by the Receiving SMTP Server	4
3.2. Relay of Messages to Other Conforming SMTP/LMTP Servers	4
3.3. Relay of Messages to Non-Conforming SMTP/LMTP Servers	5
3.4. Mailing Lists and Aliases	5
3.5. Gatewaying a Message into a Foreign Environment	5
3.6. Interaction with the DSN SMTP Extension	5
4. Header Field: MT-Priority	5
5. Example	6
6. IANA Considerations	7
7. Security Considerations	7
7.1. Modification of the MT-Priority Header Field and DKIM	9
8. References	9
8.1. Normative References	9
8.2. Informative References	10
Appendix A. Acknowledgements	11

1. Introduction

The SMTP Message Transfer Priorities extension [RFC6710] specifies a mechanism to allow messages to be given a label to indicate preferential handling, to enable mail handling nodes to take this into account for onward processing. However, as with all SMTP extensions, all SMTP Message Transfer Agents (MTAs) between the source and the destination must support the extension in order for it to be successfully used. This document describes an application-layer tunneling of message priority, to convey the priority of the messages through MTAs that do not support the Message Transfer Priorities extension. The tunneling is done by adding a new message header field to the Internet Message Format specified in [RFC5322].

A number of other header fields are already in use, mostly in Message User Agents (MUAs), to convey meanings related to importance or priority of messages. Examples of such header fields are Importance [RFC2156], Priority [RFC2156], and X-Priority (undocumented). Considering sometimes subtle and sometimes significant differences in the meaning of these header fields and widely different syntax, this document defines a new header field.

This document is motivated by 2 main deployment scenarios: (1) an MUA talking to a non-MT-PRIORITY-aware Message Submission Agent (MSA), and (2) the use of an unextended MUA to talk to an MT-PRIORITY-aware MSA. These 2 use cases are discussed in more detail below.

Use case (1) is about an MT-PRIORITY-capable MUA talking to a non-MT-PRIORITY-capable MSA [RFC6409], which in turn is talking to an MT-PRIORITY-capable MTA [RFC5321]. Both the MSA and MTA are within the same Administrative Management Domain (ADMD) and are on a fast network; however, some recipients are accessible via the MTA that is talking over a slow link to the next MTA. Communications over that slow link can benefit from the use of the MT-PRIORITY SMTP extension.

In use case (2), a widely deployed client (such as a desktop client) is talking to an MT-PRIORITY-capable MSA. The client might be extendable via a plug-in API provided by the client developers; however, existing APIs frequently allow easy manipulation of email header fields, while not allowing for addition of SMTP protocol features. In such a case, installing a plug-in on the client that can set the MT-Priority header field could provide easier and earlier deployment of the MT-PRIORITY SMTP extension in an organization without requiring changes to desktop clients.

We note that the above use cases are not exhaustive and that other use cases -- variations of the above -- may exist. The purpose of this document is not to consider every scenario, but rather examples that reinforce the need to consider a tunneling mechanism that can deal with SMTP-capable devices that do not support [RFC6710].

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 [RFC2119] when they appear in ALL CAPS. These words also appear in this document in lower case as plain English words, absent their normative meanings.

The formal syntax uses the Augmented Backus-Naur Form (ABNF) [RFC5234] notation, including the core rules defined in Appendix B of RFC 5234 [RFC5234].

In examples, "C:" and "S:" indicate lines sent by the client and server, respectively. Line breaks that do not start with a new "C:" or "S:" exist for editorial reasons and are not a part of the protocol.

This document uses the term "priority" specifically in relation to the internal treatment of a message by the server. Messages with higher priorities may be given expedited handling, and those with lower priorities may be handled only as resources become available.

3. Handling of Messages Received via SMTP

The subsections of this section update the corresponding subsections of Section 4 of [RFC6710].

3.1. Handling of the MT-PRIORITY Parameter by the Receiving SMTP Server

This specification inserts the following between steps 4 and 5 in Section 4.1 of [RFC6710]:

- 4a. If the sending SMTP client hasn't specified the MT-PRIORITY parameter to the MAIL FROM command, but the message has a single syntactically valid MT-Priority header field (see Section 4), then the value of this header field is the message priority.
- 4b. In the absence of both the MT-PRIORITY MAIL FROM parameter and the MT-Priority header field, other message header fields, such as Priority [RFC2156] and X-Priority, MAY be used for determining the priority under this "Priority Message Handling" SMTP extension. Note, however, that the Importance [RFC2156] header field MUST NOT be used for determining the priority under this "Priority Message Handling" SMTP extension, as it has different semantics: the Importance header field is aimed at the user recipient and not at the nodes responsible for transferring the message.

3.2. Relay of Messages to Other Conforming SMTP/LMTP Servers

This specification inserts the following between steps 1 and 2 in Section 4.2 of [RFC6710].

- 1a. Note that rule 1 also applies to messages that didn't have any priority explicitly specified using the MT-PRIORITY MAIL FROM parameter or the MT-Priority header field.

3.3. Relay of Messages to Non-Conforming SMTP/LMTP Servers

This specification appends the following after step 1 in Section 4.3 of [RFC6710]:

2. The relaying MTA MUST first remove any and all existing MT-Priority header fields from the message. (Please see Section 7 for additional considerations related to removal of the MT-Priority header field.)
3. If the incoming message had an MT-PRIORITY parameter specified in the MAIL FROM command *or* there was an MT-Priority header field removed in step 2 above, then the relaying MTA MUST add its own MT-Priority header field with the value determined by the procedure in Section 3.1. The syntax of the MT-Priority header field is specified in Section 4.

3.4. Mailing Lists and Aliases

This specification makes no changes to Section 4.4 of [RFC6710].

3.5. Gatewaying a Message into a Foreign Environment

This specification inserts the following between steps 1 and 2 in Section 4.5 of [RFC6710].

- 1a. Note that if the destination environment doesn't support the transport of an arbitrary header field, the requirement in Section 3.3 to add an MT-Priority header field doesn't apply.

3.6. Interaction with the DSN SMTP Extension

This specification makes no changes to Section 4.6 of [RFC6710].

4. Header Field: MT-Priority

Applicable protocol: mail [RFC5322]
Status: standard
Author/change controller: Alexey Melnikov / IESG (iesg@ietf.org)
on behalf of the IETF
Specification document(s): RFC 6758

The MT-Priority header field conveys message transfer priority when relaying a message through MTAs that don't support the MT-PRIORITY SMTP extension.

The ABNF for this header field is defined as follows:

```
priority-header-field = "MT-Priority:"
                        [CFWS] priority-value [CFWS] CRLF
```

where "priority-value" is defined in [RFC6710].

Example:

```
MT-Priority: -3
```

Example:

```
MT-Priority: 4 (ultra)
```

5. Example

Note that the following example of an SMTP transaction with 2 recipients is also making use of the STARTTLS [RFC3207] and Delivery Status Notification (DSN) [RFC3461] SMTP extensions, even though there is no requirement that these other extensions are to be supported when the MT-PRIORITY SMTP extension is implemented.

```
S: 220 example.net SMTP server here
C: EHLO example.com
S: 250-example.net
S: 250-DSN
S: 250-STARTTLS
S: 250 MT-PRIORITY STANAG4406
C: STARTTLS
[...TLS negotiation...]
C: MAIL FROM:<eljefe@example.com> ENVID=QQ314159
    MT-PRIORITY=3
S: 250 <eljefe@example.com> sender ok
C: RCPT TO:<topbanana@example.net>
S: 250 <topbanana@example.net> recipient ok
C: RCPT TO:<Dana@Ivory.example.net> NOTIFY=SUCCESS,FAILURE
    ORCPT=rfc822;Dana@Ivory.example.net
S: 250 <Dana@Ivory.example.net> recipient ok
C: DATA
S: 354 okay, send message
C: (message goes here)
C: .
S: 250 message accepted
C: QUIT
S: 221 goodbye
```

Here, the receiving SMTP server supports the "STANAG4406" Priority Assignment Policy [RFC6710] with 6 priority levels, so it will use the priority value 4 internally (the next supported priority higher

or equal to 3) and will communicate the priority value 3 when relaying it to the next hop (if necessary). When relaying the message to the next hop that doesn't support the MT-PRIORITY SMTP extension, the transaction might look like this:

```
S: 220 example.org SMTP server here
C: EHLO example.net
S: 250-example.org
S: 250-DSN
S: 250-STARTTLS
S: 250 SIZE
C: STARTTLS
[...TLS negotiation...]
C: MAIL FROM:<eljefe@example.com> ENVID=QQ314159
S: 250 <eljefe@example.com> sender ok
C: RCPT TO:<topbanana@example.net>
S: 250 <topbanana@example.net> recipient ok
C: RCPT TO:<Dana@Ivory.example.net> NOTIFY=SUCCESS,FAILURE
  ORCPT=rfc822;Dana@Ivory.example.net
S: 250 <Dana@Ivory.example.net> recipient ok
C: DATA
S: 354 okay, send message
C: MT-Priority: 3
C: (the rest of the message goes here)
C: .
S: 250 message accepted
C: QUIT
S: 221 goodbye
```

6. IANA Considerations

IANA has added the following list of header field names to the "Permanent Message Header Field Names" registry (in <<http://www.iana.org/assignments/message-headers/perm-headers.html>>):

```
Header field: MT-Priority
Applicable protocol: mail
Status: standard
Author/change controller: Alexey Melnikov / IESG (iesg@ietf.org)
  on behalf of the IETF
Specification document(s): RFC 6758
```

7. Security Considerations

This document allows a message priority to be tunneled through MTAs that don't support the MT-PRIORITY SMTP extension by specifying how it can be represented in the message itself (using the MT-Priority header field). Thus, it is important to ensure that an MTA receiving

a message containing the MT-Priority header field can trust that it was set by an authorized agent. The use of technologies such as DomainKeys Identified Mail (DKIM) [RFC6376] or S/MIME to sign the MT-Priority header field value can enable a recipient to verify whether the specified priority value was generated by a trusted agent. In particular, DKIM signing allows a recipient to verify that the specified priority value was present when the message was signed, and to verify who signed the message. Note, however, that the DKIM signer might not be the same agent that generated the MT-Priority header field.

MSAs ought to only accept message transfer priorities (whether by using the MT-PRIORITY parameter to the MAIL FROM command or the MT-Priority header field in the message itself) from users (or only certain groups of such users) who are authenticated and authorized in some way that's acceptable to the MSA. As part of this policy, they can also restrict maximum priority values that different groups of users can request and can override the priority values specified by MUAs. When relaying to non-MT-PRIORITY-capable SMTP/LMTP (Local Mail Transfer Protocol) servers, such MSAs are required to replace any MT-Priority header field values that don't satisfy this policy. See Section 7.1 for more details on what the consequences of such changes might be.

Similarly, MTAs ought to only accept message transfer priorities (whether by using the MT-PRIORITY parameter to the MAIL FROM command or the MT-Priority header field in the message itself) from senders (or only certain groups of such senders) who are authenticated and authorized in some way that's acceptable to the MTA. As part of this policy, they can also restrict maximum priority values that different groups of senders can request and can override the priority values specified by them. When relaying to non-MT-PRIORITY-capable SMTP/LMTP servers, such MTAs are required to replace any MT-Priority header field values that don't satisfy this policy. See Section 7.1 for more details on what the consequences of such changes might be.

In the absence of the policy enforcement mentioned above, an SMTP server (whether an MSA or an MTA) implementing the MT-PRIORITY SMTP extension might be susceptible to a denial-of-service attack. For example, malicious clients (MUAs/MSAs/MTAs) can try to abuse this feature by always requesting priority 9.

To protect the MT-Priority header field from modification or insertion, MUAs, MSAs, and MTAs inserting it into messages SHOULD use a message header protection mechanism such as DKIM [RFC6376]; however, see Section 7.1 for more information.

7.1. Modification of the MT-Priority Header Field and DKIM

An MSA/MTA that receives a message with an MT-Priority header field protected by DKIM and that wants to change the message priority due to its policy is forced to choose between

- a. breaking DKIM signatures (by replacing the MT-Priority header value),
- b. leaving the message as is (and using the MT-PRIORITY MAIL FROM parameter), relying on the fact that all downstream MTAs are compliant with this specification, and
- c. rejecting the message.

None of these choices are perfect. They work in a particular situation, so these choices should be carefully considered during implementation and deployment.

If the MSA/MTA decides to alter the message, it SHOULD re-sign the message with DKIM.

8. References

8.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC3461] Moore, K., "Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)", RFC 3461, January 2003.
- [RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.
- [RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, October 2008.
- [RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, October 2008.
- [RFC6409] Gellens, R. and J. Klensin, "Message Submission for Mail", STD 72, RFC 6409, November 2011.
- [RFC6710] Melnikov, A. and K. Carlberg, "Simple Mail Transfer Protocol Extension for Message Transfer Priorities", RFC 6710, August 2012.

8.2. Informative References

- [RFC2156] Kille, S., "MIXER (Mime Internet X.400 Enhanced Relay): Mapping between X.400 and RFC 822/MIME", RFC 2156, January 1998.
- [RFC3207] Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security", RFC 3207, February 2002.
- [RFC6376] Crocker, D., Hansen, T., and M. Kucherawy, "DomainKeys Identified Mail (DKIM) Signatures", RFC 6376, September 2011.
- [SMTP-PRI-OLD] Schmeing, M., Brendecke, J., and K. Carlberg, "SMTP Service Extension for Priority Message Handling", Work in Progress, August 2006.

Appendix A. Acknowledgements

This document copies lots of text from "SMTP Service Extension for Priority Message Handling" [SMTP-PRI-OLD]. Therefore, the authors of this document would like to acknowledge contributions made by the authors of that document: Michael Schmeing and Jan-Wilhelm Brendecke.

Many thanks for input provided by Steve Kille, David Wilson, John Klensin, Dave Crocker, Graeme Lunt, Alessandro Vesely, Barry Leiba, Bill McQuillan, Murray Kucherawy, SM, Glenn Parsons, Pete Resnick, Chris Newman, Ned Freed, Claudio Allocchio, Martin Thomson, and Joseph Yee.

Special thanks to Barry Leiba for agreeing to shepherd this document.

Authors' Addresses

Alexey Melnikov
Isode Ltd
5 Castle Business Village
36 Station Road
Hampton, Middlesex TW12 2BX
UK

EEmail: Alexey.Melnikov@isode.com

Ken Carlberg
G11
1601 Clarendon Blvd, #203
Arlington, VA 22209
USA

EEmail: carlberg@g11.org.uk