Independent Submission
Request for Comments: 8494
Category: Informational
ISSN: 2070-1721

D. Wilson
A. Melnikov, Ed.
Isode Ltd

November 2018

Multicast Email (MULE) over Allied Communications Publication (ACP) 142

Abstract

Allied Communications Publication (ACP) 142 defines P_MUL, which is a protocol for reliable multicast suitable for bandwidth-constrained and delayed acknowledgement (Emissions Control or "EMCON") environments running over UDP. This document defines MULE (Multicast Email), an application protocol for transferring Internet Mail messages (as described in RFC 5322) over P_MUL (as defined in ACP 142). MULE enables transfer between Message Transfer Agents (MTAs). It doesn't provide a service similar to SMTP Submission (as described in RFC 6409).

This document explains how MULE can be used in conjunction with SMTP (RFC 5321), including some common SMTP extensions, to provide an alternate MTA-to-MTA transfer mechanism.

This is not an IETF specification; it describes an existing implementation. It is provided in order to facilitate interoperable implementations and third-party diagnostics.

Status of This Memo

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

This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8494.

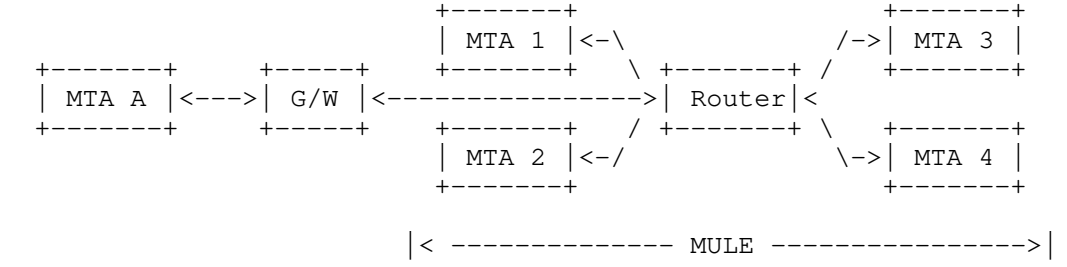
Table of Contents

1. Introduction

P_MUL [ACP142A] is a transport protocol for reliable multicast in bandwidth-constrained and delayed acknowledgement environments running on top of UDP. This document defines MULE, an application protocol for transferring Internet Mail messages [RFC5322] over ACP 142 P_MUL. The objectives of MULE are 1) to take advantage of the bandwidth-saving feature of using the multicast service as supported by modern computer networks and 2) to allow message transfer under EMCON (Emissions Control) conditions. EMCON or "radio silence" means that although receiving nodes are able to receive messages, they are not able to acknowledge the receipt of messages.

The objective of this protocol is to take advantage of multicast communication for the transfer of messages between MTAs (Message Transfer Agents) on a single multicast network under normal (i.e., dialog-oriented) communication conditions and under EMCON conditions. An "EMCON condition" means that a receiving node is able to receive messages but cannot acknowledge the received messages for a relatively long time (hours or even days).

Figure 1 illustrates a simple multicast scenario, where the same message has to be sent from MTA A (through G/W) to MTA 1, MTA 2, MTA 3, and MTA 4.



Note: The gateway (G/W) and Router might or might not be running on the same system.

Figure 1: Typical MULE Deployment

Due to multicast use (instead of a unicast communication service) in the above MTA configuration, only one message transmission from the gateway to the Router is required in order to reach MTA 1, MTA 2, MTA 3, and MTA 4, instead of four as required with unicast. This saves the transmission three message transactions and thus results in savings in bandwidth utilization. Depending on the network bandwidth

(in some radio networks, it is less than 9.6 Kb/s), this savings can be of vital importance. The savings in bandwidth utilization become even greater with every additional receiving MTA.

P_MUL employs a connectionless transport protocol to transmit messages. This guarantees reliable message transfer (through ACP 142 retransmissions) even in cases where one or more of the receiving MTAs are not able or allowed to acknowledge completely received messages for a certain period of time.

This protocol specification requires fixed multicast groups and knowledge of the group memberships in one or more multicast groups of each participating node (MTA). Membership in multicast groups needs to be established before MULE messages can be sent.

MULE enables MTA-to-MTA transfer. It doesn't provide service similar to SMTP Submission [RFC6409].

2. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

This document also uses terminology from [RFC5321] and [RFC5598].

3. MULE

MULE is an electronic mail transport of Internet Mail messages [RFC5322] over an ACP 142 P_MUL network. It provides service similar to MTA-to-MTA SMTP [RFC5321]. This document doesn't define a service similar to SMTP Submission [RFC6409].

An important feature of MULE is its capability to transport mail across multiple networks, referred to as "MULE mail relaying". A network consists of the nodes that are mutually accessible by ACP 142. Using MULE, a process can transfer mail to another process on the same ACP 142 network or to some other ACP 142 network via a relay or gateway process accessible to both networks.

MULE reuses the ESMTP extension framework defined in [RFC5321]. MULE servers MUST support the following ESMTP extensions: DSN [RFC3461], SIZE [RFC1870], 8BITMIME [RFC6152], MT-PRIORITY [RFC6710], DELIVERBY [RFC2852], BINARYMIME [RFC3030], and CHUNKING [RFC3030]. (As the

message content size can always be determined from the compression wrapper and the size of the envelope, no special handling is needed for binary messages.)

Relaying a message using MULE is performed as follows:

1. The message is reassembled from one or more DATA_PDUs [ACP142A].

2. If the contentType-ShortForm value is 25, the BSMTP-like payload is extracted from the compressedContent field and uncompressed (the reverse of the compression process specified in Section 3.2). If the contentType-ShortForm value is not 25, it is handled as described in [ACP142A]. This document doesn't further discuss any cases where the contentType-ShortForm value is not 25.

3. The list of recipients is extracted from RCPT-lines (see Section 3.1). If the receiving node is not responsible (directly or indirectly) for any of the recipients, the message is discarded and no further processing is done.

4. The relay adds trace header fields, e.g., the Received header field. See [RFC7601] and Section 4.4 of [RFC5321].

5. The set of ACP 142 destinations for the message is created by extracting right-hand sides (hostnames) of each RCPT-line, eliminating duplicates, and then converting each hostname into the next ACP 142 destination using static configuration.

6. For each unique ACP 142 destination, the following steps are performed:

   A. A new BSMTP-like payload is formed, as described in Section 3.1, that only contains RCPT-lines that correspond to recipients that can receive mail through the ACP 142 destination.

   B. The created payload is compressed and encoded as specified in Section 3.2.

   C. The compressed payload is sent by P_MUL as a series of an Address_PDU and one or more DATA_PDUs. When the message has an associated MT-PRIORITY value [RFC6710], the MappedPriority(value) is included as the Priority field of the corresponding ACP 142 PDUs, including Address_PDUs, DATA_PDUs, and DISCARD_MESSAGE_PDUs. Here, MappedPriority(x) is defined as "6 - x".

3.1. BSMTP-Like Payload Construction

MULE uses a BSMTP-like payload that differs from Batch SMTP (BSMTP) [RFC2442] in that it eliminates unnecessary information. As with BSMTP, ESMTP capability negotiation is not used, since receiver EMCON restrictions prohibit such real-time interaction. For that reason, there is no point in including EHLO capabilities. "MAIL FROM:" and "RCPT TO:" prefixes are also excluded in order to save a few bytes.

For each received message, the corresponding BSMTP-like payload is constructed as follows. Note that lines are terminated using CR LF.

1. The first line is what would be used for the data following "MAIL FROM:" in the SMTP dialog, i.e., it contains the return-path address (including the angle brackets -- "<" and ">") followed by any ESMTP extension parameters to the MAIL FROM command.

2. After that, there is a separate line for each recipient of the message. The value is what would follow "RCPT TO:" in the SMTP dialog, i.e., the recipient address (including the angle brackets -- "<" and ">") followed by any ESMTP extension parameters to the corresponding RCPT TO command.

3. The list of recipients is terminated by an empty line (i.e., just CR LF).

4. The message content follows the empty line. There is no need for transparency ("dot stuffing") or terminating with a sequence "CR LF . CR LF", as the end of the message content is indicated by the end of the data (see Section 3.2 for more details).

The following is an example of a BSMTP-like payload:

```
<from@example.com> MT-PRIORITY=4 BODY=8BITMIME RET=HDRS ENVID=QQ314159
<to1@example.net> NOTIFY=FAILURE ORCPT=rfc822;Bob@ent.example.net
<to2@example.net> NOTIFY=SUCCESS,FAILURE

From: from@example.com
To: To1 <to1@example.net>, To2 <to2@example.net>
Date: 27 Apr 2017 16:17 +0100
Subject: a test
MIME-Version: 1.0
Content-type: text/plain; charset=utf-8
Content-transfer-encoding: 8bit

This is worth <poundsign>100
```

ABNF [RFC5234] for the BSMTP-like payload is:

```
bsmtp-like-payload = envelope CRLF payload
envelope = FROM-line 1*RCPT-line
FROM-line = reverse-path [SP mail-parameters] CRLF
RCPT-line = forward-path [SP rcpt-parameters] CRLF

payload = *OCTET
          ; Conforms to message syntax as defined in RFC 5322
          ; and extended in MIME

OCTET = <any 0-255 octet value>
reverse-path = <as defined in RFC 5321>
forward-path = <as defined in RFC 5321>
mail-parameters = <as defined in RFC 5321>
rcpt-parameters = <as defined in RFC 5321>
```

3.2. Payload Compression

A BSMTP-like payload (Section 3.1) is first compressed using zlibCompress [RFC1950]. This compressed payload is placed in the compressedContent field of the CompressedContentInfo element defined in Section 4.2.6 of [STANAG-4406]. This is then encoded as BER encoding [ITU.X690.2002] of the CompressedData ASN.1 structure. For convenience, the original definition of the CompressedData ASN.1 structure is included below. The contentType-ShortForm value used by MULE MUST be 25. (The contentType-OID alternative is never used by MULE.)

The above procedure is similar to how X.400 messages are sent using Annex E of [STANAG-4406]. This makes it easier to implement MTAs that support both Internet messages and X.400 messages in the same code base.

The Compressed Data Type (CDT) consists of content of any type that is compressed using a specified algorithm. The following object identifier identifies the CDT:

```
id-mmhs-CDT ID ::= { iso(1) identified-organization(3) nato(26)
                     stanags(0) mmhs(4406) object-identifiers(0)
                     id-mcont(4) 2 }
```

The CDT is defined by the following ASN.1 type. Note that this definition is copied from [STANAG-4406] and is only reproduced here for the reader's convenience.

```
DEFINITIONS ::=
BEGIN
CompressedData ::= SEQUENCE {
                   compressionAlgorithm CompressionAlgorithmIdentifier,
                   compressedContentInfo CompressedContentInfo
                   }
CompressionAlgorithmIdentifier ::= CHOICE {
                     algorithmID-ShortForm [0] AlgorithmID-ShortForm,
                     algorithmID-OID [1] OBJECT IDENTIFIER
                   }
AlgorithmID-ShortForm ::= INTEGER { zlibCompress (0) }
CompressedContentInfo ::= SEQUENCE {
                     CHOICE {
                       contentType-ShortForm [0] ContentType-ShortForm,
                       contentType-OID [1] OBJECT IDENTIFIER
                     },
                     compressedContent [0] EXPLICIT OCTET STRING
                   }
ContentType-ShortForm ::= INTEGER {
                     unidentified (0),
                     external (1), -- identified by the
                                   -- object-identifier
                                   -- of the EXTERNAL content
                     p1 (2),
                     p3 (3),
                     p7 (4)
                   }
END
```

This document effectively adds another enumeration choice to the ContentType-ShortForm definition. The updated definition looks like this:

```
ContentType-ShortForm ::= INTEGER {
                       unidentified (0),
                       external (1), -- identified by the
                                     -- object-identifier
                                     -- of the EXTERNAL content
                       p1 (2),
                       p3 (3),
                       p7 (4),
                       mule (25)
                     }
```

3.3. Error Handling

MULE doesn't allow a next-hop Message Transfer Agent / Mail Delivery Agent (MTA/MDA) to return immediate Response Codes for the FROM-line or any of the recipients in the RCPT-line. Therefore, when MTAs/MDAs that are compliant with this specification receive a message that can't be relayed further or delivered, they MUST generate a non-delivery DSN report [RFC6522] message that includes the message/delivery-status body part [RFC3464] and submit it using MULE to the FROM-line return-path address.

MULE relays (unlike MULE MDAs) don't need to verify that they understand all FROM-line and/or RCPT-line parameters. This keeps relay-only implementations simpler and avoids the need to upgrade them when MULE MDAs are updated to support extra SMTP extensions.

4. Gatewaying from Internet Mail to MULE

A gateway from Internet Mail to MULE acts as an SMTP server on the receiving side and as a MULE client on the sending side.

When the content type for a message is an Internet message content type (which may be 7-bit, 8-bit, or binary MIME), this is transported using ACP 142 [ACP142A] as follows:

1. For each mail message, a BSMTP-like payload is formed, as described in Section 3.1.

2. The created payload is compressed and encoded, as specified in Section 3.2.

3. The compressed payload is sent by P_MUL as a series of an Address_PDU and one or more DATA_PDUs. When the message has an associated MT-PRIORITY value [RFC6710], the MappedPriority(value) is included as the Priority field of the corresponding ACP 142 PDUs, including Address_PDUs, DATA_PDUs, and DISCARD_MESSAGE_PDUs. Here, MappedPriority(x) is defined as "6 - x".

The set of ACP 142 destinations for the message is derived from the next-hop MTAs for each of the recipients.

4.1. Use of BDAT

If a message is received by a gateway through SMTP transfers using the CHUNKING [RFC3030] extension, the message is rebuilt by the receiving MTA into its complete form and is then used as a single MULE message payload. Use of the BINARYMIME [RFC3030] extension is conveyed by inclusion of the BODY=BINARY parameter in the FROM-line.

5. Gatewaying from MULE to Internet Mail

A gateway from MULE to Internet Mail acts as a MULE server on the receiving side and as an SMTP client on the sending side.

Gatewaying from an ACP 142 environment to Internet Email is the reverse of the process specified in Section 4.

1. The ACP 142 message is reassembled from one or more DATA_PDUs.

2. If the contentType-ShortForm value is 25, the BSMTP-like payload is extracted from the compressedContent field and uncompressed (the reverse of the compression process specified in Section 3.2). If the contentType-ShortForm value is not 25, it is handled as described in [ACP142A].

3. The BSMTP-like payload is converted to an SMTP transaction (see Section 3.1). (The first line of the BSMTP-like payload is prepended with "MAIL FROM:", and each following line (until the empty line is encountered) is prepended with "RCPT TO:". After skipping the empty delimiting line, the rest of the payload is the message body. This can be sent using either DATA or a series of BDAT commands, depending on the capabilities of the receiving SMTP system. For example, the presence of the BODY=BINARY parameter in the FROM-line would necessitate the use of BDAT or down-conversion of the message to 7-bit compatible representation.)

5.1. Handling of ESMTP Extensions and Errors

ESMTP extension parameters to MAIL FROM and RCPT TO SMTP commands obtained from a BSMTP-like payload are processed according to specifications of the corresponding ESMTP extensions. This includes dealing with the absence of support for ESMTP extensions that correspond to MAIL FROM and RCPT TO parameters found in the BSMTP-like payload.

Failures to extract or uncompress BSMTP-like payloads should result in the receiver discarding such payloads.

6. IANA Considerations

IANA has created a new "Multicast Email SMTP Extensions" registry under the "MAIL Parameters" registry. The registration procedure for this new registry is "Specification Required" [RFC8126]. The designated expert(s) will be appointed and managed by the editors of this document together with the Independent Submissions Editor. Selected designated expert(s) should (collectively) have a good knowledge of SMTP (and its extensions and extensibility mechanisms), as well as ACP 142 and its limitations. The subsections below provide more details: Section 6.1 specifies instructions for the designated expert(s), and Section 6.2 defines the initial content of the registry.

6.1. Instructions for Designated Experts

The designated expert(s) for the new "Multicast Email SMTP Extensions" registry verifies that:

1. The requested SMTP extension is already registered in the "SMTP Service Extensions" registry under the "MAIL Parameters" registry on the IANA website or is well documented on a stable, publicly accessible web page.

2. The requested SMTP extension has the correct status as specified in Section 6.2. When deciding on status, the designated expert(s) is provided with the following guidelines:

   A. If the SMTP extension only affects commands other than MAIL FROM and RCPT TO, then the status should be "N/A".

   B. If the SMTP extension only applies to SMTP Submission [RFC6409] (and not to SMTP relay or final SMTP delivery), then the status should be "N/A".

   C. If the SMTP extension changes which commands are allowed during an SMTP transaction (e.g., if it adds commands alternative to DATA or declares commands other than MAIL FROM, RCPT TO, DATA, and BDAT to be a part of SMTP transaction), then the status should be "Disallowed" or "Special".

   D. If the SMTP extension adds extra round trips during SMTP transaction, then the status should be "Disallowed" or "Special".

Registration requests should include the SMTP extension name, status (see Section 6.2), and specification reference. They may also include an optional note.

6.2. SMTP Extension Support in MULE

The following table summarizes how different SMTP extensions can be used with MULE. Each extension has one of the following statuses:

- Required - support by MULE relays, SMTP-to-MULE gateway, or MULE-to-SMTP gateway is required.
- Disallowed - incompatible with MULE.
- N/A - not relevant because the extension affects commands other than MAIL FROM and/or RCPT TO or is only defined for SMTP Submission [RFC6409]. Such extensions can still be used on the receiving SMTP side of an SMTP-to-MULE gateway.
- Supported - can be used with MULE but requires bilateral agreement between sender and receiver.
- Special - needs to be accompanied by an explanation.

SMTP Extension Keyword	Status	Reference
SIZE	Required	[RFC1870]
8BITMIME	Required	[RFC6152]
DSN	Required	[RFC3461]
MT-PRIORITY	Required	[RFC6710]
DELIVERBY	Required	[RFC2852]
BINARYMIME	Required	[RFC3030]
CHUNKING	Special (*)	[RFC3030]
ENHANCEDSTATUSCODES	Special (**)	[RFC2034]
RRVS	Supported	[RFC7293]
SUBMITTER	Supported	[RFC4405]
PIPELINING	N/A	[RFC2920]
STARTTLS	N/A	[RFC3207]
AUTH	Special (***)	[RFC4954]
BURL	N/A	[RFC4468]
NO-SOLICITING	N/A	[RFC3865]
CHECKPOINT	Disallowed	[RFC1845]
CONNEG	Disallowed	[RFC4141]

Table 1: Initial Content of Multicast Email SMTP Extensions Registry

(*) - SMTP CHUNKING MUST be supported on the receiving SMTP side of an SMTP-to-MULE gateway and MAY be used on the sending side of a MULE-to-SMTP gateway. A MULE relay doesn't need to do anything special for this extension.

(**) - The ENHANCEDSTATUSCODES extension is supported by including relevant status codes in DSN [RFC3461] reports.

(***) - The AUTH parameter to the MAIL FROM command is "Supported", but the rest of the AUTH extension is not applicable to MULE.

Note that the above table is not exhaustive. Future RFCs can define how SMTP extensions not listed above can be used in MULE.

7. Security Considerations

As MULE provides a service similar to SMTP, many of the security considerations from [RFC5321] apply to MULE as well; in particular, Sections 7.1, 7.2, 7.4, 7.6, 7.7, and 7.9 of [RFC5321] apply to MULE.

As MULE doesn't support capability negotiation or the SMTP HELP command, Section 7.5 of [RFC5321] ("Information Disclosure in Announcements") doesn't apply to MULE.

As MULE doesn't support the VRFY or EXPN SMTP commands, Section 7.3 of [RFC5321] ("VRFY, EXPN, and Security"), which discusses email harvesting, doesn't apply to MULE.

Arguably, it is more difficult to cause an application-layer denial-of-service attack on a MULE server than on an SMTP server. This is partially due to the fact that ACP 142 is used in radio/wireless networks with relatively low bandwidth and very long round-trip time (especially if EMCON is in force). However, as MULE is using multicast, multiple MULE nodes can receive the same message and spend CPU resources processing it, even if the message is addressed to recipients that are not going to be handled by such nodes. As MULE lacks transport-layer source authentication, this can be abused by malicious senders.

For security considerations related to use of zlib compression, see [RFC6713].

Due to the multicast nature of MULE, it cannot use TLS or DTLS. Accordingly, it does not support STARTTLS [RFC3207]. Users should not depend on hop-by-hop confidentiality or integrity protection of mail transferred among MULE MTAs (in the same way they can't generally rely on the use of STARTTLS on SMTP MTA-to-MTA links) and should consider the use of end-to-end protection, such as S/MIME [RFC5750] [RFC5751].

S/MIME signatures and/or encryption survive gatewaying between MULE and SMTP environments.

8. References

8.1. Normative References

[ACP142A] CCEB, "P_Mul - A Protocol for Reliable Multicast in Bandwidth Constrained and Delayed Acknowledgement (EMCON) Environments", ACP 142(A), October 2008.

[ITU.X690.2002] ITU-T, "Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T Recommendation X.690, August 2015.

[RFC1870] Klensin, J., Freed, N., and K. Moore, "SMTP Service Extension for Message Size Declaration", STD 10, RFC 1870, DOI 10.17487/RFC1870, November 1995, <https://www.rfc-editor.org/info/rfc1870>.

[RFC1950] Deutsch, P. and J-L. Gailly, "ZLIB Compressed Data Format Specification version 3.3", RFC 1950, DOI 10.17487/RFC1950, May 1996, <https://www.rfc-editor.org/info/rfc1950>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC2852] Newman, D., "Deliver By SMTP Service Extension", RFC 2852, DOI 10.17487/RFC2852, June 2000, <https://www.rfc-editor.org/info/rfc2852>.

[RFC3030] Vaudreuil, G., "SMTP Service Extensions for Transmission of Large and Binary MIME Messages", RFC 3030, DOI 10.17487/RFC3030, December 2000, <https://www.rfc-editor.org/info/rfc3030>.

[RFC3461] Moore, K., "Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)", RFC 3461, DOI 10.17487/RFC3461, January 2003, <https://www.rfc-editor.org/info/rfc3461>.

[RFC3464] Moore, K. and G. Vaudreuil, "An Extensible Message Format for Delivery Status Notifications", RFC 3464, DOI 10.17487/RFC3464, January 2003, <https://www.rfc-editor.org/info/rfc3464>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/info/rfc5234>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <https://www.rfc-editor.org/info/rfc5321>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <https://www.rfc-editor.org/info/rfc5322>.

[RFC5598] Crocker, D., "Internet Mail Architecture", RFC 5598, DOI 10.17487/RFC5598, July 2009, <https://www.rfc-editor.org/info/rfc5598>.

[RFC6152] Klensin, J., Freed, N., Rose, M., and D. Crocker, Ed., "SMTP Service Extension for 8-bit MIME Transport", STD 71, RFC 6152, DOI 10.17487/RFC6152, March 2011, <https://www.rfc-editor.org/info/rfc6152>.

[RFC6522] Kucherawy, M., Ed., "The Multipart/Report Media Type for the Reporting of Mail System Administrative Messages", STD 73, RFC 6522, DOI 10.17487/RFC6522, January 2012, <https://www.rfc-editor.org/info/rfc6522>.

[RFC6710] Melnikov, A. and K. Carlberg, "Simple Mail Transfer Protocol Extension for Message Transfer Priorities", RFC 6710, DOI 10.17487/RFC6710, August 2012, <https://www.rfc-editor.org/info/rfc6710>.

[RFC6713] Levine, J., "The 'application/zlib' and 'application/gzip' Media Types", RFC 6713, DOI 10.17487/RFC6713, August 2012, <https://www.rfc-editor.org/info/rfc6713>.

[RFC7601] Kucherawy, M., "Message Header Field for Indicating Message Authentication Status", RFC 7601, DOI 10.17487/RFC7601, August 2015, <https://www.rfc-editor.org/info/rfc7601>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[STANAG-4406] NATO, "Military Message Handling System", STANAG 4406 Ed. 2, March 2005.

8.2. Informative References

[RFC1845] Crocker, D., Freed, N., and A. Cargille, "SMTP Service Extension for Checkpoint/Restart", RFC 1845, DOI 10.17487/RFC1845, September 1995, <https://www.rfc-editor.org/info/rfc1845>.

[RFC2034] Freed, N., "SMTP Service Extension for Returning Enhanced Error Codes", RFC 2034, DOI 10.17487/RFC2034, October 1996, <https://www.rfc-editor.org/info/rfc2034>.

[RFC2442] Freed, N., Newman, D., Belissent, J., and M. Hoy, "The Batch SMTP Media Type", RFC 2442, DOI 10.17487/RFC2442, November 1998, <https://www.rfc-editor.org/info/rfc2442>.

[RFC2920] Freed, N., "SMTP Service Extension for Command Pipelining", STD 60, RFC 2920, DOI 10.17487/RFC2920, September 2000, <https://www.rfc-editor.org/info/rfc2920>.

[RFC3207] Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security", RFC 3207, DOI 10.17487/RFC3207, February 2002, <https://www.rfc-editor.org/info/rfc3207>.

[RFC3865] Malamud, C., "A No Soliciting Simple Mail Transfer Protocol (SMTP) Service Extension", RFC 3865, DOI 10.17487/RFC3865, September 2004, <https://www.rfc-editor.org/info/rfc3865>.

[RFC4141] Toyoda, K. and D. Crocker, "SMTP and MIME Extensions for Content Conversion", RFC 4141, DOI 10.17487/RFC4141, November 2005, <https://www.rfc-editor.org/info/rfc4141>.

[RFC4405] Allman, E. and H. Katz, "SMTP Service Extension for Indicating the Responsible Submitter of an E-Mail Message", RFC 4405, DOI 10.17487/RFC4405, April 2006, <https://www.rfc-editor.org/info/rfc4405>.

[RFC4468] Newman, C., "Message Submission BURL Extension", RFC 4468, DOI 10.17487/RFC4468, May 2006, <https://www.rfc-editor.org/info/rfc4468>.

[RFC4954] Siemborski, R., Ed. and A. Melnikov, Ed., "SMTP Service Extension for Authentication", RFC 4954, DOI 10.17487/RFC4954, July 2007, <https://www.rfc-editor.org/info/rfc4954>.

[RFC5750] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling", RFC 5750, DOI 10.17487/RFC5750, January 2010, <https://www.rfc-editor.org/info/rfc5750>.

[RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, DOI 10.17487/RFC5751, January 2010, <https://www.rfc-editor.org/info/rfc5751>.

[RFC6409] Gellens, R. and J. Klensin, "Message Submission for Mail", STD 72, RFC 6409, DOI 10.17487/RFC6409, November 2011, <https://www.rfc-editor.org/info/rfc6409>.

[RFC7293] Mills, W. and M. Kucherawy, "The Require-Recipient-Valid-Since Header Field and SMTP Service Extension", RFC 7293, DOI 10.17487/RFC7293, July 2014, <https://www.rfc-editor.org/info/rfc7293>.

Acknowledgements

Thank you to Steve Kille for suggestions, comments, and corrections on this document. An additional thank you goes to Barry Leiba, Sean Turner, Dave Crocker, and Nick Hudson for reviews and comments on this document.

Some text was borrowed from "P_Mul: An Application Protocol for the Transfer of Messages over Multicast Subnetworks and under EMCON Restrictions" (September 1997); we gratefully acknowledge the work of the authors of that document.

Authors' Addresses

David Wilson
Isode Ltd
14 Castle Mews
Hampton, Middlesex TW12 2NP
United Kingdom

Email: David.Wilson@isode.com

Alexey Melnikov (editor)
Isode Ltd
14 Castle Mews
Hampton, Middlesex TW12 2NP
United Kingdom

Email: Alexey.Melnikov@isode.com