SMTP Service Extension for Priority Message Handling

draft-schmeing-smtp-priorities-04.txt

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.

This Internet-Draft will expire on August 5, 2006.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This memo defines an extension to the SMTP (Simple Mail Transfer Protocol) service whereby messages are sent with a priority to achieve a certain order in which the messages are transferred by an MTA (Message Transfer Agent). This priority or precedence order is used instead of the first-come-first-serve rule. This extension is
not to be confused with "Importance of a Message" which is widely 
deployed using an email header such as Importance or even Priority or 
Precedence with common values of HIGH, NORMAL and LOW. Importance of 
a Message does not affect the priority of the transport itself in any 
way. Nevertheless, there may be policy defined relations between 
priorities and importance indicators.

This extension uses the term priority in the meaning of expedited 
treatment of a message by the server according to its priority.

Table of Contents

1. Introduction ............................................ 4
2. Terminology ........................................... 5
3. Framework for the Priority Extension ..................... 6
4. The Priority Service Extension ........................... 7
   4.1. Expedited Transfer ................................. 7
       4.1.1. Preemption of sessions or transactions ........ 8
       4.1.2. Handling of emails with multiple recipients .... 8
   4.2. Timely Delivery ................................... 9
   4.3. Resolving conflicts for the sending order of messages 
        with the same priority ............................ 9
   4.4. Size Limitation .................................. 9
   4.5. Further Constraints ................................. 10
5. Recipient Dependent Priority ............................. 11
   5.1. Maillists, Aliases and Forwarding ................. 11
6. Priority Policies ....................................... 12
   6.1. Conflicts with external constraints ................ 13
   6.2. The Non-priority .................................. 14
   6.3. Handling Non-priority Servers and Mismatching Policies . 15
   6.4. Invalid priority levels ............................ 16
   6.5. Default Policy .................................... 16
       6.5.1. Number and names of priorities ................ 16
       6.5.2. Message size constraints ....................... 17
       6.5.3. Delivery time constraints ....................... 18
       6.5.4. Usage of network layer priorities ............... 18
       6.5.5. Delivery Failures .............................. 18
       6.5.6. Copy and blind copy recipients ................ 19
       6.5.7. Handling of non-priority servers ............... 19
       6.5.8. Handling servers with different policies ....... 20
7. Example ............................................... 21
8. Security Considerations ................................ 22
9. IANA Considerations .................................... 23
10. List of abbreviations .................................... 24
11. References ........................................... 26
    11.2. Informative Reference ............................ 25
    11.3. Normative References .............................. 25
1. Introduction

Military Message Handling Systems (MMHS) have high requirements in their functionality and reliability. As examinations in [1] show the SMTP (Simple Mail Transfer Protocol) [7], including some SMTP extensions, provides most of the features requested by the military. But one of the most important requirements of MMHS is not provided by SMTP. This is the requirement for priorities or precedences. This document defines an SMTP Service Extension offering such a service allowing Mail Transfer Agents (MTAs) to determine which emails require expedited handling.
2. Terminology

The key words "REQUIRED", "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", and "MAY" in this document are to be interpreted as described in "Key words for use in RFCs to Indicate Requirement Levels" [5].

The terms SMTP client and SMTP server are used with the same definition as given in section 2.3.2 of RFC 2821 [7]:

- The SMTP client is the (computer) process initiating an SMTP session and controlling it issuing commands to the server.
- The SMTP server is the process waiting for clients to connect and executing the commands from the client.

As this document is concerned with SMTP only, the terms client and server may as well be used without the SMTP prefix.

An email is waiting to be sent, if it resides in the queue of an MTA and can be send to the next hop or delivered to its final recipient(s) once available resources at the sending MTA allow this. Emails having their processing delayed for some reason are NOT waiting to be sent during this delay. The most important reason for emails to be delayed is a transient error response from the next MTA to which the email must be transferred.

An email is ready to be sent, if it is waiting to be sent and either no emails with higher priority are waiting to be sent or available resources allow to send more emails in parallel than the number of emails with higher priorities that are waiting to be sent. Note that an email may be ready to be sent but the transfer or delivery process can not yet be initiated, because the number of emails ready to be sent exceeds the number of emails that can be processed in parallel.

Additionally, this document will use the terms "default policy", "custom policy" and "local policy". These are defined as follows:

- The "default policy" is the policy defined in Section 6.5.
- A "custom policy" is any other policy regulating the use of priorities for emails.
- A "local policy" is the policy applicable for an actual client, server, MTA, site or network. It may be either the default policy or a custom policy.
3. Framework for the Priority Extension

- The textual name of this extension is "Priority Message Handling".

- The EHLO-Keyword is PRIORITY.

- One optional parameter is used with this keyword. This parameter is an absolute Uniform Resource Identifier (URI) as defined in RFC3986 [14] in section 4.3. The resource thus identified MUST be a document which describes the priority policy. If this parameter is not given the default policy defined in Section 6.5 is applied. The syntax for this value is:

  priority-policy ::= absolute-URI

  This policy defines the supported levels of priority, their semantics and optionally their names.

- No new SMTP verbs are defined.

- One optional parameter using the keyword "PRIORITY" is added to the RCPT TO command. The value associated with this parameter is a decimal integer number greater than or equal to 0 (zero) indicating the priority of the email for the given recipient. The syntax of the value is as follows:

  priority-value ::= [1*3DIGIT]

  A value of 0 indicates an email from a client/network not supporting priorities or intended to be sent to such a server/network. Any other number identifies a priority level defined by the policy. Higher numbers mean higher priority. This parameter may be set for each recipient independently.

- The maximum length of a RCPT TO command line is increased by 12 characters by the possible addition of the PRIORITY keyword and value.

- As one of the most likely instances to assign transport priorities is the submitting party of an email (i.e. the originator or sender), this extension is valid for message submission according to RFC 2476 [6].
4. The Priority Service Extension

The priority of a message expresses itself in the order they are transferred from the client to the server. This is largely independent from the order in which they where received by the server. The Priority Service Extension increases the possibilities of SMTP service extensions such as Deliver-By and Delivery Status Notification or (non-standard) header fields such as Importance.

In military scenarios, priorities usually come with additional associated constraints. Examples are limitations of the message size or the allowed delivery time.

4.1. Expedited Transfer

The main service provided by the Priority Message Handling SMTP Service Extension is expedited transfer of emails with a higher priority. Therefore a client that has more than one email to send at a given time MUST send those with a higher priority before those with a lower one.

Priorities are assigned on a per-recipient basis. The priority of an email is the highest priority assigned to any of the yet unprocessed recipients. Thus the priority of the email may vary while it is processed by an MTA or UA and may be different at different MTAs. The priority of any given recipient is nevertheless constant.

As long as there are emails with higher priorities waiting to be sent a client MUST NOT initiate transactions for emails with lower priorities. It MAY however send an email with highest priority even to recipients with lower priorities if this can be done within the same transaction as the higher priorities.

The handling of messages with the same priority level is described in Section 4.3.

Especially in networks with limited available data rate the actual transfer over the network may create a significant portion of the overall delivery time. Besides the actions taken at the application level it can thus be important to deploy priority or precedence mechanisms offered by the network itself to ensure timely delivery of the emails. One example of such a mechanism is the "Type of Service" field defined in the IP (Internet Protocol) header of RFC 791. If such services are available, it is a matter of local policy to decide whether to use them. The mapping from the priorities defined at the SMTP level to those offered by the underlying network is as well to be defined in the local policy.
4.1.1. Preemption of sessions or transactions

Most current SMTP MTAs are capable of handling several inbound and outbound connections at once. With this feature it should be possible to start additional outbound connections for emails with higher priorities even if there are already several connections running for other emails. If no additional connection is possible, a client MUST abort a running session for emails with lower priority no later than directly after the current transaction. The client even MAY interrupt an active transaction and SHOULD do this, if otherwise constraints such as delivery time would be violated for the email with higher priority. This preliminary termination of sessions or transactions is called preemption.

If preemption of running transactions occurs, the client MUST preempt the lowest number of transactions sufficient to process the higher priority emails. It must chose the transactions for the emails with the lowest priorities currently processed. Local policies MAY add additional criteria to choose the transaction to be preempted in the case that more transactions than required would qualify for preemption due to the priority of the emails. If after applying the priority test and all criteria defined by the local policy still the number of transactions to preempt is greater than needed, the decision is left to the implementation.

If the client has an option to interrupt transactions in a way that it can be restarted at the interruption point later, it SHOULD deploy it. An example for a mechanism providing such a service is the "SMTP Service Extension for Checkpoint/Restart" defined in RFC 1845 [3]

If a client opts for the preemption of sessions instead of transactions, it MUST preempt the next session that reaches the end of a transaction independent of the priority of the emails being processed.

4.1.2. Handling of emails with multiple recipients

If a client has to send an email with multiple recipients bearing different priorities to the same server, it SHOULD do so in one transaction treating the email according to the highest priority set for any of the recipients.

The reorganization of the transfer order MUST NOT alter or even corrupt the emails, therefore allowing safe transmission of all emails in dependency of their priority.
4.2. Timely Delivery

An important constraint usually associated especially with higher priority levels is, that messages with that priority have to reach its destination within a defined period of time. Usually, higher priorities mean shorter maximum allowed time of delivery.

As the SMTP does not natively offer a service for timely delivery, the decision whether to use delivery time constraints for any or all priority levels is left to the local policy.

The "Deliver By SMTP Service Extension" (Deliver-By Extension) defined in [8] is an example of an SMTP extension providing a service that can be used to implement such constraints.

If the local policy does not specify time constraints for a given priority, no such constraints are applied.

4.3. Resolving conflicts for the sending order of messages with the same priority

If two or more emails with the same priority are ready to be sent at the same time, clients SHOULD send them in parallel if possible. Local policies MAY define rules to determine the order in which emails of the same priority are sent if the number of emails ready to be sent exceeds the number of emails that can be processed in parallel.

If all applicable rules to determine the sending order from this memo and local policy still leave more emails ready to be sent than can be processed in parallel, the final decision is left to the implementation.

4.4. Size Limitation

The larger a message, the longer the time required to send it over a given connection. In constrained networks this can impair the possibility of the MTS to deliver large messages with high priorities in time. Therefore, policies governing priorities usually have size constraints for the messages at least for higher priorities.

These constraints can always be enforced independent of the SMTP Service Extensions supported by the server receiving the email. It is always possible for the server to count the number of received octets after the client indicated the end of the email and base the decision to accept or reject the email on this number.

Therefor, after completely receiving the content of the email the
server MUST check that the actual received size does not exceed the lowest size limitation allowed by the priorities set for all recipients. If the actual size is too big for at least one recipient, the server MUST NOT send a successful reply but MUST reject the email with an error code of "556 Priority defined size limit exceeded". If the client uses an SMTP Service Extension which allows to transmit the content in several chunks, such as [9], the server SHOULD check the current size after every chunk and SHOULD abort the email with the above error code as soon as the size constraint applicable for the email is violated.

In addition to just counting the received octets while the email is being transmitted, a client and server may also deploy mechanisms, that allow for an earlier detection of size violations. An example for such a service is the "SMTP Service Extension for Message Size Declaration" (SIZE Extension) from RFC 1870 [4].

The SIZE Extension allows a client to declare the size of the email with an optional parameter to the MAIL FROM: SMTP command. This parameter can be used for example to decide for each individual recipient whether the email fulfils the size constraints. Whether the email or only the recipients for which the priority induced size constraint would be violated are rejected is a matter of local policy.

If the server indicated for individual recipients that they can not be accepted with the given priority for any reason, local policy MAY allow to nevertheless transmit the email to the remaining recipients.

If the local policy does not address size constraints, the default is that emails may be of arbitrary size. Constraints imposed by other circumstances such as available storage space or general limitations are, of course, unaffected by this.

4.5. Further Constraints

Depending on the actual scenario in which this priority extension is deployed, it may be necessary to add further constraints to certain priority levels. Although it is strongly believed that limiting the delivery time and email size should be sufficient for most if not all purposes, local policy may add further constraints such as limitations on content types or security classifications.

For example, in military applications of priorities, messages without classification or with low classification may only be sent at the lower priority levels.
5. Recipient Dependent Priority

Often, not all recipients need to receive the message with the same (high) priority. For example, copy (CC, carbon copy) and blind copy (BCC, blind carbon copy) recipients usually can accept a lower priority than the primary recipient(s) because they do not have to act on the message but receive it only for informational purposes.

Limiting the high-priority messages only to the primary recipient complies with the basic principle of using high priorities only if really necessary. So, the number of high-priority messages is reduced to a minimum. Assigning every recipient an individual priority could be realized by sending the same message several times. This is unnecessary, non-practical, and a waste of resources. Binding the priority to the recipient allows to deploy the multiple recipient per transaction feature of SMTP even when having different priorities for different recipients of the message.

To lower the burden on the network, an MTA SHOULD send any message to as many recipients as possible with one transaction, even if the recipients have different priorities bound to them. In this case, the MTA MUST treat the email according to the highest priority bound to any of the recipients and MUST retain the original priority values for each recipient.

A recipient address, that has a priority other than the non-priority (see Section 6.2) set, is called a prioritized recipient (address).

5.1. Maillists, Aliases and Forwarding

Several options exist to translate the address of an email recipient into one or more other addresses. Examples for this are aliases, maillist or email redirections e.g. via a .forward file.

Priorities are assigned for a reason. Therefore, if a prioritized recipient address is to be translated or expanded as explained above, the translating or expanding entity (maillist manager, MTA etc.) SHOULD retain the original priority if possible and SHOULD set it for all expanded or translated addresses. Local policy however MAY deviate from this behavior for good reason.
6. Priority Policies

This memo defines a default policy in Section 6.5. A server indicates support for this policy by omitting the optional parameter to the PRIORITY EHLO keyword. An SMTP server MUST NOT use the PRIORITY keyword without argument if it does not support the default priority. Servers MUST NOT indicate support for more than one policy to a client at a time. However a server MAY indicate different policies to clients coming from different addresses or connecting at different times.

Although the policy identifier must be a syntactically valid URL, this memo does not define whether it is a machine readable definition or just a textual description meant for implementors of the policy. The URL nevertheless MUST point to a document defining the policy in some way.

The following constraints apply to all policies governing priority message handling:

- A priority policy MUST at least define the supported priority levels and SHOULD determine the size constraints for each defined level. If no size constraints are defined for a level, emails of that level may be of arbitrary size.
- The priorities MUST be denominated by decimal integer numbers greater than or equal to 1 but MAY additionally be assigned symbolic names. Higher values mean higher priority.
- If a policy defines symbolic names it SHOULD define a name for every one but MAY omit any. If a name is assigned to the non-priority, it SHOULD reflect that this priority is not a regular one.
- Priority values SHOULD be assigned in consecutive order. The total number of defined priority levels MUST be kept to the possible minimum to remain manageable.
- Priority level 0 (zero) is considered to be the "non-priority" value for recipients that can not be reached via MTAs supporting priorities or for emails coming in from clients not supporting the priority policy of the receiving server or not supporting priorities at all.
- The definitions and constraints for the special priority 0 are explained in Section 6.2.
o If a priority mechanism of the underlying network should be used, mappings from the SMTP priority level to the priority levels of the network MUST be defined. If no mapping is defined, servers SHOULD use the default level for the network connection but MAY use higher ones. This does not change the SMTP priority level.

o In some cases it is possible to determine that an individual recipient can not be accepted because of a violation of the priority policy directly when the respective RCPT TO SMTP command is issued. A priority policy SHOULD define how to handle the emails in this case. Possible options are to completely reject the email or to send it to the remaining recipients. The default is to send the emails to the remaining recipients, if no other conditions require the email to be rejected completely.

o In other cases the decision to reject an individual recipient can only be made after the respective RCPT TO: SMTP command has been confirmed with a 2xx SMTP reply code but the final 250 SMTP reply code accepting the email has not yet been sent. In these cases the whole email MUST be rejected with an appropriate error code.

6.1. Conflicts with external constraints

If there is a conflict between a priority induced constraint and a constraint from some other sources (external constraint), the more restrictive constraint always has precedence over the less constrictive one. If an email is rejected because of constraints not induced by the priority policy, the error message MUST NOT indicate a priority policy violation.

To illustrate this, consider the following example:

o An email with a size of 2 M-Byte is to be sent.

o The highest priority set for any of the recipients is n >= 1.

o The maximum size for emails with priority n is 3 M-Byte.

o At the server to which the email should be submitted, the parameter to the SIZE EHLO keyword limits emails to 1 M-Byte in size due to limited spool storage.

From the perspective of the priority policy this email would be acceptable because it is smaller than the 3 M-Bytes allowed for messages with priority n. Nevertheless, the constraints defined by the SIZE Extension set a limit of 1 M-Byte, which is more restrictive than the constraint set by the priority policy. Thus the constraint set by the SIZE Extension takes precedence and the email can not be
accepted by the server. The server would respond as defined in RFC 1870 [4] and send the appropriate error code for overly large messages.

If on the other hand the priority policy would set the 1 M-Byte limit and the storage space of the server would allow 3 M-Byte emails, the email would still be unacceptable. But this time it would be a priority policy violation that would be indicated with the error code defined in section Section 4.4 of this memo.

If both, external and policy induced constraints would make an email unacceptable, the error message must be created according to the more restrictive constraint. If, in the above example, the email would have a size of 4 M-Byte, it would not be acceptable due to both the limitation defined with the EHLO keyword and the limitation of the priority policy. As the limitation of the EHLO keyword is more restrictive the email would still not be a policy violation.

The determination of what error code to create does not discriminate between transient (i.e. error codes in the 4xx range) and permanent errors (i.e. error codes in the 5xx range). If the 1M-Byte restriction of the EHLO keyword would be due to a temporary shortage of storage space, the 4 M-Byte email from the previous paragraph for example could be rejected with a transient error from the EHLO keyword while the shortage lasts. If there would be enough storage space afterwards, it would still be rejected, but this time with a permanent error from the priority policy.

Local policy MAY allow for permanent errors to take precedence over transient ones to lessen the burden on the network. In this case the 4 M-Byte email would be rejected with a permanent error due to a policy violation on the first attempt to transfer it to the MTA.

6.2. The Non-priority

The priority 0 bears a special meaning: It is the priority automatically assigned to emails coming in to a server supporting priorities from a client not supporting them. It is the default priority assigned to recipients for which no priority is set explicitly. It is as well the priority that SHOULD be used for recipients behind an MTA not supporting priorities. This priority MUST always be used for this purpose. Policies MUST NOT impose constraints such as delivery or size restrictions to this priority but MAY assign a name to it. Other SMTP Service Extensions such as the Deliver-By or SIZE Extensions may still define additional constraints.

Servers MUST allow to explicitly set the non-priority for any or all
recipients of an email.

Clients MUST be able to set the non-priority for a recipient. It MUST be able to set priorities for only some of the recipients. If priorities have been set for any recipients, clients SHOULD set the non-priority for any recipient, for which no priority has been set. They MAY always set the non-priority to recipients for which no priority has been set if the receiving server indicates support for this extension, even if the supported policies of the client and server do not match.

Emails in which no other priority than the non-priority has been set MUST always be delivered normally, even if this means transfer to servers that do not support priority handling or have a different policy.

If an email is not rejected for other reasons, sending it to non-compliant servers for recipients that have the non-priority set MUST NOT be considered an error. Instead the email MUST be delivered. In this context a non-compliant server is one not supporting this extension at all or having a different policy.

Recipients, for whom no priority or the non-priority is set, are called non-priority recipients. Emails, that have only non-priority recipients are called non-priority emails.

6.3. Handling Non-priority Servers and Mismatching Policies

Not all servers will support the Priority Message Handling Extension nor will all that do have the same policy. Servers that support a different policy than the client are called mismatching servers; servers not indicating support for priorities (independent of whether they actually do or do not support them) are called non-priority servers.

By default, only emails for non-priority recipients are delivered to non-priority or mismatching servers. If recipients with priorities other than the non-priority require sending the email to mismatching on non-priority servers, this is treated as an error. The email MUST NOT be relayed but the MTA MUST send a error code of "557 Receiving server not supporting compliant priority policy".

The local policy of a client MAY however define priorities other than the non-priority to be routable to non-priority servers. It MAY define arbitrary actions to be taken in this case or define it as normal operation. This can be defined for each priority independently. An example for an action to take is the sending of warning emails to the originator and/or recipient of the email.
informing them of the loss of priorities. Another example is to write log information to the system protocol.

A policy at a client MAY as well define a mapping to another policy, thus enabling transfer of emails to a server using this policy. As with non-priority servers, it MAY define arbitrary actions to be taken in this case or define it as normal operation.

It is impossible for a server to know the policy used by a client. A server thus can not refuse accepting emails based on the client’s (mismatching) policy.

A server MUST always accept emails, where no priority is set or where only the non-priority is set.

6.4. Invalid priority levels

If a client provides an invalid value to the PRIORITY argument to the RCPT TO: command, the server MUST reject that recipient with an error code of "558 Invalid priority value" and MAY reject the complete email with the same error code.

An invalid priority level may be a non-numeric value, a negative value or a value not defined in the local policy.

6.5. Default Policy

If the policy identifier of the PRIORITY EHLO keyword is omitted, the default policy set out in this section is applied. Servers MUST NOT use the PRIORITY keyword without an argument if they do not support this policy but support for this policy is OPTIONAL.

6.5.1. Number and names of priorities

- This policy defines the priority levels 1, 2, 3 and 4.

-
The following names are assigned to the different priority levels:

<table>
<thead>
<tr>
<th>Priority</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>NONE</td>
</tr>
<tr>
<td>1</td>
<td>ROUTINE</td>
</tr>
<tr>
<td>2</td>
<td>PRIORITY</td>
</tr>
<tr>
<td>3</td>
<td>IMMEDIATE</td>
</tr>
<tr>
<td>4</td>
<td>FLASH</td>
</tr>
</tbody>
</table>

- The names are case-insensitive.

### 6.5.2. Message size constraints

- The message size for ROUTINE and PRIORITY is unlimited by this policy.

- The message size for the priority level IMMEDIATE MUST NOT exceed 4096 bytes.

- The message size for the FLASH priority is limited to 2048 Bytes.

For calculating the message size the complete email including all control characters and header fields is considered but servers MAY exclude any trace header fields as defined in [RFC 2821][7].

According to section [Section 4.4](#) these size constraints can always be enforced. Servers MUST always determine the size of the email and check against the lowest size constraint introduced by any of the applied priorities prior to finally accepting an email. Servers SHOULD abort a transaction cleanly as soon as possible with the error code defined in section [Section 4.4](#).

If both, the client and server implement the SIZE Extension the SIZE parameter for the MAIL FROM SMTP command MUST be used and its value MUST be set to be greater than or equal to the actual relevant size of the email as defined above. If for any recipient the indicated size of the email exceeds the limit associated with the priority set for this recipient, the recipient MUST be rejected with the appropriate error code for size constraint violations defined in section [Section 4.4](#). Delivery to the remaining recipients is not affected by this.
6.5.3. Delivery time constraints

If the MTA supports the Deliver-By Extension, the following delivery time constraints are associated with the priorities:

- Four hours for ROUTINE,
- one hour for PRIORITY,
- 30 minutes for IMMEDIATE and
- 10 minutes for FLASH.

These constraints MAY be ignored if a client or server does not support the Deliver-By Extension but MUST be applied otherwise. They MUST be retained if emails for recipients with priority levels ROUTINE or PRIORITY are sent to non-compliant or non-priority servers that support the Deliver-By Extension.

6.5.4. Usage of network layer priorities

The default policy doesn’t use network layer priorities. For this reason no mapping of priority levels is defined here.

Administrators of actual installations MAY however define local mappings to network priorities. Routing of emails to other servers implementing SMTP priorities SHOULD NOT be impaired even if the transfer through networks without network priorities is required.

6.5.5. Delivery Failures

If an email can not be delivered to one or more of its (prioritized) recipients, an appropriate error message MUST be presented to the originator of the email. Delivery to the remaining recipients MUST be processed independently.

Error or warning message caused by failures associated with priority handling under this Default Policy MAY be generated individually for each recipient or MAY be aggregated to contain all errors associated with a single email. They MUST NOT contain error messages from more than one email. Additionally, they MAY take the form of an email being sent to the originator or MAY be presented in some other way. An example for an alternative presentation can be a window shown to the originator by his user agent. If the error message has the form of an email it MUST be delivered to the originator with the highest priority of any recipient that caused the error or warning message.
6.5.6. Copy and blind copy recipients

- Copy recipients MUST NOT receive the email at a higher priority than the highest set for any primary recipient.
- The default priority for copy recipients is ROUTINE if the highest priority of the primary recipients is ROUTINE or higher and NONE otherwise.
- The priority for copy recipients may be as high as PRIORITY, if the highest priority set for a primary recipient is PRIORITY or higher.
- The priority for blind copy recipients MUST be set to NONE.

These constraints MUST be enforced by the submitting UA or MTA and MUST be ignored by any other MTA or the receiving UA(s).

6.5.7. Handling of non-priority servers

If emails must be transferred to non-priority servers to be delivered to any or all recipients the following rules apply:

- Emails MUST be sent to non-priority servers for recipients with priorities NONE, ROUTINE or PRIORITY. If the server and client both support the Deliver-By Extension the client MUST deploy it to ensure timely delivery of the email.
- It is strongly believed that this email will reach its destination in time. A deliver-by-time from one or even four hours is certainly no problem for today's Internet.
- The sending client SHOULD write a log message to record loss of priority handling for those recipients and MAY as well inform the originator of this fact.
- Emails MUST NOT be sent to non-priority servers for any recipients with priorities of IMMEDIATE or FLASH. For these recipients a reply code of "558 Priority level violation" MUST be generated.
- If an email must be sent to a non-priority server for both, recipients with priorities not higher than PRIORITY and those with priorities of IMMEDIATE or FLASH, it must be transferred for the recipients with priorities not higher than PRIORITY and error messages must be created for the other recipients.
6.5.8. Handling servers with different policies

Mismatching servers are considered to be non-priority servers when deciding whether to send emails to them or not. If emails are sent to them, all priorities MUST be set to NONE, but otherwise the handling is exactly as if the servers were non-priority servers.
7. Example

This example shows an SMTP session with one transaction using the priority extension. Lines starting with C are sent by the client, lines starting with S by the server.

S: 220 foo.com Simple Mail Transfer Service Ready
C: EHLO bar.com
S: 250-foo.com greets bar.com
S: 250-SIZE
S: 250-DSN
S: 250-PRIORITY
S: 250 HELP
C: MAIL FROM:<Smith@bar.com>
S: 250 OK
C: RCPT TO:<Jones@foo.com> PRIORITY=2
S: 250 OK
C: RCPT TO:<Brown@foo.com> PRIORITY=4
S: 250 OK
C: DATA
S: 354 Start mail input; end with <CRLF>.<CRLF>
C: Blah blah blah...
C: ...etc. etc. etc.
C: .
S: 250 OK
C: QUIT
S: 221 foo.com Service closing transmission channel
8. Security Considerations

This memo does not discuss security issues and is not believed to raise any security issues not already endemic in electronic mail and present in fully conforming implementation of RFC 2821 [7].

Possible Denial-of-Service (DoS) attacks through extensive use of high priorities are outside the scope of this memo. It is believed that they are best dealt with by access control and careful design of local policies.
9. IANA Considerations

The IANA Mail Parameters registry documents SMTP service extensions. The "PRIORITY" service extension has to be added to this registry in accordance with the specifications of section Section 3.
10. List of abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCC</td>
<td>Blind Carbon Copy</td>
</tr>
<tr>
<td>CC</td>
<td>Carbon Copy</td>
</tr>
<tr>
<td>DSN</td>
<td>Delivery Status Notification</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>MMHS</td>
<td>Military Message Handling System</td>
</tr>
<tr>
<td>MTA</td>
<td>Message Transfer Agent</td>
</tr>
<tr>
<td>MTS</td>
<td>Message Transfer System</td>
</tr>
<tr>
<td>NATO</td>
<td>North Atlantic Treaty Organization</td>
</tr>
<tr>
<td>RFC</td>
<td>Request For Comment</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>TTY</td>
<td>Teletypewriter</td>
</tr>
<tr>
<td>UA</td>
<td>User Agent</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
</tbody>
</table>
11. References

11.2. Informative Reference


11.3. Normative References


11. References
Authors’ Addresses

Michael Schmeing
Forschungsgesellschaft fuer Angewandte Naturwissenschaften e.V.
Neuenahrer Strasse 20
Wachtberg  53343
DE

Phone: +49 228 9435 593
Email: schmeing@fgan.de
URI: http://www.fgan.de

Jan-Wilhelm Brendecke
Forschungsgesellschaft fuer Angewandte Naturwissenschaften e.V.
Flerzheimer Strasse 36
Rheinbach  53359
DE

Phone: +49 2226 913760
Email: brendecke@gmx.de
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights 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; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat 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 on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

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, 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.

Copyright Statement

Copyright (C) The Internet Society (2006). 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.

Acknowledgment

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