SMTP Service Extension for Priority Message Handling
draft-schmeing-smtp-priorities-05.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 February 24, 2007.

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 ............................................. 3
2. Terminology ........................................... 4
3. Terminology & background ................................ 5
4. Framework for the Priority Extension .................... 6
5. The Priority Service Extension ............................. 8
   5.1. Expedited Transfer .................................. 8
      5.1.1. Probability ................................... 9
      5.1.2. Preemption of sessions or transactions .......... 9
      5.1.3. Handling of emails with multiple recipients .... 10
   5.2. Timely Delivery .................................... 10
   5.3. Resolving conflicts for the sending order of messages
        with the same priority ............................... 10
   5.4. Size Limitation .................................... 11
   5.5. Further Constraints ................................ 12
6. Recipient Dependent Priority .............................. 13
   6.1. Maillists, Aliases and Forwarding .................... 13
7. NameSpaces ................................................. 14
   7.1. Conflicts with external constraints .................. 15
   7.2. Handling Non-priority Servers and Mismatching Policies .. 16
   7.3. Recipients without priorities ........................ 17
   7.4. Invalid priority levels .............................. 17
   7.5. Mappings to other NameSpaces ........................ 17
8. Example .................................................... 19
9. Security Considerations .................................. 20
10. IANA Considerations ..................................... 21
11. List of abbreviations ................................... 22
12. References ............................................... 23
    12.1. Informative Reference .............................. 23
    12.2. Normative References .............................. 23
Authors’ Addresses ......................................... 25
Intellectual Property and Copyright Statements ............ 26
1. Introduction

Prioritization is an issue that gains attention when resources are scarce and sets of users (and their data) are considered more important than others. Military Message Handling Systems (MMHS) such as AUTODIN and the Defense Messaging System (DMS), have requirements to prioritize their traffic to help ensure that important data is given preferential treatment over what would normally be viewed as best effort.

Deployments of MMHS typically include the ability to preempt or displace less important data traffic. This displacement can be in the form of dropped packets, removal of reservations or termination of end-to-end sessions. Outside MMHS systems such as GETS rely on increasing the probability of obtaining resources or successfully forwarding downstream packets instead of preempting resources. In either case, the critical feature incumbent in both systems is an ability to prioritize data in anticipation of resource contention.

The Simple Mail Transfer Protocol [7] (SMTP) is one of the most popular applications used over the Internet by today’s general public. The examinations documented in [1] show that SMTP, including some SMTP extensions, also provides most of the features requested by the military (a user community whose requirements are more stringent than the general public). But one of the most important requirements of MMHS not provided by SMTP is priority or precedence in handling between Message Transfer Agents (MTA).

This document defines an SMTP Service Extension offering such a service allowing Mail Transfers Agents 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" [4].

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.

The policy defining the use of priorities within a given NameSpace is called "NameSpace Policy". A NameSpace is a name (or label) for a finite and ordered set of priorities. In some instances, this memo or a NameSpace Policy may allow additions to the definitions of the NameSpace Policy. These additions are called "local policy".
3. Terminology & background

RFC 3487 [15] articulates a set of requirements for prioritizing access to services and resources using the Session Initiation Protocol (SIP). As in the case of SMTP, SIP has a priority field used to convey the importance of a session (or message, in the case of SMTP) to the end-user. However, the value within the field was not meant for intermediate nodes. From these requirements, the SIP working group defined a new optional Resource Priority field in RFC 4412 [16] for the SIP protocol. The new field was divided into two distinct parts. The first is Value subfield, which contains the priority associated with the SIP message. The second subfield is the NameSpace, which identifies a set or family of 1 or more priorities. The strength in this approach is that support for the prioritization feature is not bound to a one-size-fits-all design. As an example, the DoD/NATO community has an existing set of 5 priorities used for its messaging system. Other communities of interest may have sets that are smaller or larger than that currently used by DoD/NATO.

Underneath the SIP layer, and its Resource Priority extension, ongoing work is being done by the NSIS working group to define a QSPEC that includes fields correlating to SIP’s NameSpace/Value tuple. In addition, the TSV Working Group is in the process of defining an extension to RSVP that defines a priority policy element correlating to the NameSpace/Value tuple. Both of these efforts are aimed at facilitating underlying signaling of network elements to obtain resources based on the priority set at the application layer.
4. Framework for the Priority Extension

- The textual name of this extension is "Priority Message Handling".
- The EHLO-Keyword is PRIORITY.
- One mandatory parameter is used with this keyword. This parameter is a list of NameSpaces supported by the server. The syntax for this value is described below. The "token-nodot" production is copied from RFC 3265 [10].

```
namespace-list = namespace * (COMMA namespace)
namespace = token-nodot
```

A NameSpace is a name of an ordered set of priorities with attached policy.

- 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 in alpha-numeric form. The syntax of the value is:

```
priority-arg = "PRIORITY" EQUAL value
value = namespace "." priority
priority = token-nodot
```

- Two examples of PRIORITY parameters are shown below:

```
PRIORITY=Example.1
PRIORITY=AnotherExample.Flash
```

- The ‘value’ parameter in the ‘PRIORITY’ extension indicates the concatenated tuple of the ‘namespace’, the ‘priority’ within that NameSpace and the "." character separating the two. An entry in a ‘namespace’ must be unique from all other NameSpaces. Entries in a ‘priority’ must be unique within a NameSpace, but they may be the same as those in other NameSpaces.

- The maximum length of a RCPT TO command line is increased by 9 characters plus the length of the ‘value-list’ 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].
5. 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 [8] and Delivery Status Notification [11][14][13][12] 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.

5.1. 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 a default policy, emails with higher priority waiting to be sent by 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. Policy associated with a specific NameSpace may override this default policy; an example being the use of a weighted round robin initiation of transactions in order to prevent a starving of resources from lower priorities.

The handling of messages with the same priority level is described in Section 5.3.

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 would be the use of RSVP and the work-in-progress effort extension to RSVP that prioritizes reservations. If such services are available, it is a matter of NameSpace 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 NameSpace Policy. If the NameSpace Policy does not regulate the use of network priorities, their use can be defined by local policy.

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. The manner in which expedited transfer can be accomplished is divided into two approaches. One is probability, the other involves preemption, both of which are described in more detail below.

5.1.1. Probability

As the name suggests, probability involves increasing the chances of obtaining resources without adversely affecting previously established connections. One example would involve requesting resources set aside for specific priority levels. If these additional resources are exhausted, then the desired connection is denied. Queues, new timers, or combinations thereof can be used to facilitate the higher priority requests, but the key is that mechanisms focus on increasing the probability of message transfer.

5.1.2. Preemption of sessions or transactions

Preemption is binary type of action and focusses only on a comparison of priorities to determine if previously established transactions must be displaced in favor of higher priority requests. 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. NameSpace Policies and 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. Regulations from local policy MUST NOT be applied before NameSpace Policy and MUST NOT conflict with NameSpace policy settings. If
after applying the priority test and all criteria defined by applicable NameSpace Policy and 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 [2]

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.

5.1.3. 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.

5.2. 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. In some cases, higher priorities mean shorter maximum allowed time of delivery.

As 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 NameSpace 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 applicable NameSpace Policy does not specify time constraints for a given priority, no such constraints are applied.

5.3. 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. NameSpace Policy and local policy 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. Definitions from NameSpace Policy always take precedence over definitions from local policy. NameSpace Policy MAY disallow local policy to define additional criteria to determine sending order.

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

5.4. 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, NameSpace Policy MAY define size constraints for any or all of its priority levels.

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 [3].

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. Unless NameSpace Policy defines another course of action, if the size provided with the SIZE argument of the MAIL FROM: command is too large for the priority set for any of the recipients, the recipient MUST be rejected with an error code of "556 Priority defined size limit exceeded". Processing for the remaining recipients is to continue normally.

If the NameSpace 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.

5.5. 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, NameSpace 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.
6. 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 set, is called a prioritized recipient (address).

6.1. 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. NameSpace Policy however MAY deviate from this behavior for good reason.
7. NameSpaces

A NameSpace identifies a set of one or more alpha-numeric priorities. These NameSpaces are registered with IANA and are unique for the registry associated with the SMTP priority extension. Ideally a given NameSpace satisfies the needs for groups of organizations and user sets. As an example, a NameSpace that correlates to the Q.735.3 protocol in support of Multi-Level Precedence and Preemption (MLPP) would be applicable to all messaging systems that support Q.735.3.

New NameSpaces MUST be defined as an Informational RFC after Expert Review in accordance with the policy set forth in RFC 2434 [5]. The Expert Reviewer will consult with the Application Area Directors and the IEPREP mailing list. The following elements MUST be addressed when registering a new NameSpace:

- Priority level(s) must be enumerated as a finite ordered list
- A priority algorithm must be defined and described. This algorithm defines the schema of how messages are handled based on their labeled priority. For example, one algorithm may describe the use of preemption of resources of a lower priority message (i.e., dropped message) to satisfy a higher priority message. Another algorithm may involve queuing of messages based on availability of extra resources set aside for specific priorities. A third algorithm may be a hybrid of preemption and queuing.
- Any new new response codes (warning or Error) unique to the NameSpace must be listed and explained.
- The document needs to specify a new row for the following table that summarizes the features of the NameSpace. For the tabel below, there is ONE NameSpace label and ONE Algorithm. There N-number of levels, each having a corresponding Warning-Code OR Error-Code. It is expected that the warning/error codes are the same for each NameSpace.Priority tuple. Finally, an RFC is used as the reference for the table of information.

<table>
<thead>
<tr>
<th>NameSpace</th>
<th>Algo</th>
<th>Priority(s)</th>
<th>Warn-Code</th>
<th>Error-Code</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;label&gt;</td>
<td>&lt;preempt, queue, hybrid&gt;</td>
<td>&lt;new code, new code, none&gt;</td>
<td>new code, new code, none</td>
<td>&lt;RFC&gt;</td>
<td></td>
</tr>
</tbody>
</table>

NameSpace labels are case-insensitive, priority labels are case-
insensitive unless defined case-sensitive by the NameSpace policy.

In addition to the requirements described above, the following constraints apply to all NameSpaces:

- 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.

- If additional constraints such as size limitations or maximum delivery times are associated with any or all priorities of a NameSpace, the RFC must define which constraints apply to which priority.

- In some cases it is possible to determine that an individual recipient can not be accepted because of a violation of the NameSpace Policy directly when the respective RCPT TO SMTP command is issued. A NameSpace 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.

- 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.

7.1. 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 NameSpace Policy, the error message MUST NOT indicate a NameSpace Policy violation.

To illustrate this, consider the following example:

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

- The NameSpace is recognized and accepted

- The highest priority of the NameSpace set for any of the recipients is n.
o The maximum size for emails with priority n is 3 M-Byte.

o At the server to which the email should be transferred, 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 NameSpace 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 NameSpace 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 [3] and send the appropriate error code for overly large messages.

If on the other hand the NameSpace 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 NameSpace Policy violation that would be indicated with the error code defined in section Section 5.4 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 NameSpace 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.

7.2. 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 recipients without a priority 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 NameSpace".

Namespace Policy MAY however define certain priorities 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.

7.3. Recipients without priorities

A server MUST always accept recipients, where no priority is set,
independend of whether other recipients of the email have priorities
assigned or not. Such recipients MUST be treated as best-effort
delivery. Other reasons such as invalid addresses or syntactical
errors in the RCPT TO: command nevertheless may still prevent
acceptance of the recipient.

A client MAY use RCPT TO: commands with and without the PRIORITY
parameter for the same email transaction.

7.4. Invalid priority levels

As a default course of action, 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.

Namespace Policy MAY override the default action upon detection of an
invalid PRIORITY argument. For example, the server may replace the
value with a "NULL" argument, indicating that there is no priority
associated with recipient.

7.5. Mappings to other Namespaces

A Namespace A MAY define a mapping to another Namespace B. Namespace
A in this case MUST define to which priority level of NameSpace B each of its priority levels is mapped.

While more than one priority level of NameSpace A may be mapped to a given priority level of NameSpace B, a priority level of A MUST NOT be mapped to zero or more than one priority levels of B.

For all priority levels a1 and a2 of NameSpace A where a1 is greater than a2 and all priority levels b1 and b2 of NameSpace B, the following condition MUST be fulfilled: If a1 is mapped to b1 and a2 is mapped to b2, then b1 MUST be greater than or equal to b2.

An MTA MUST NOT change the priority assigned to a recipient, unless

- the next server to which the email must be sent for the recipient does not support the original NameSpace; and

- the NameSpace originally used for the recipient defines a mapping to at least one of the NameSpaces announced by the server to which the email is to be sent.
8. 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 Example,AnotherExample
S: 250 HELP
C: MAIL FROM:<Smith@bar.com>
S: 250 OK
C: RCPT TO:<Jones@foo.com> PRIORITY=Example.2
S: 250 OK
C: RCPT TO:<Brown@foo.com> PRIORITY=AnotherExample.Flash
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
9. 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.
10. 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 4.
11. List of abbreviations

BCC     Blind Carbon Copy
CC      Carbon Copy
DSN     Delivery Status Notification
IETF    Internet Engineering Task Force
IP      Internet Protocol
MMHS    Military Message Handling System
MTA     Message Transfer Agent
MTS     Message Transfer System
NATO    North Atlantic Treaty Organization
RFC     Request For Comment
SMTP    Simple Mail Transfer Protocol
TTY     Teletypewriter
UA      User Agent
URL     Uniform Resource Locator
12. References

12.1. Informative Reference


12.2. Normative 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  
Flerzheimer Strasse 36  
Rheinbach  53359  
DE  
Phone: +49 2226 913760  
Email: brendecke@gmx.de

Ken Carlberg  
G11  
123a Versailles Circle  
Towson, MD  
USA  
Email: carlberg@g11.org.uk
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.