

Network Working Group
Request for Comments: 3464
Obsoletes: 1894
Category: Standards Track

K. Moore
University of Tennessee
G. Vaudreuil
Lucent Technologies
January 2003

An Extensible Message Format for Delivery Status Notifications

Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

This memo defines a Multipurpose Internet Mail Extensions (MIME) content-type that may be used by a message transfer agent (MTA) or electronic mail gateway to report the result of an attempt to deliver a message to one or more recipients. This content-type is intended as a machine-processable replacement for the various types of delivery status notifications currently used in Internet electronic mail.

Because many messages are sent between the Internet and other messaging systems (such as X.400 or the so-called "Local Area Network (LAN)-based" systems), the Delivery Status Notification (DSN) protocol is designed to be useful in a multi-protocol messaging environment. To this end, the protocol described in this memo provides for the carriage of "foreign" addresses and error codes, in addition to those normally used in Internet mail. Additional attributes may also be defined to support "tunneling" of foreign notifications through Internet mail.

Table of Contents

1. Introduction	3
1.1 Purposes	3
1.2 Requirements	4
1.3 Terminology	5
2. Format of a Delivery Status Notification	7
2.1 The message/delivery-status content-type	9
2.1.1 General conventions for DSN fields	9
2.1.2 "-type" sub-fields	9
2.1.3 Lexical tokens imported from RFC 822	10
2.2 Per-Message DSN Fields	11
2.2.1 The Original-Envelope-Id field	11
2.2.2 The Reporting-MTA DSN field	12
2.2.3 The DSN-Gateway field	13
2.2.4 The Received-From-MTA DSN field	14
2.2.5 The Arrival-Date DSN field	14
2.3 Per-Recipient DSN fields	14
2.3.1 Original-Recipient field	15
2.3.2 Final-Recipient field	15
2.3.3 Action field	16
2.3.4 Status field	18
2.3.5 Remote-MTA field	19
2.3.6 Diagnostic-Code field	19
2.3.7 Last-Attempt-Date field	20
2.3.8 final-log-id field	20
2.3.9 Will-Retry-Until field	20
2.4 Extension fields	21
3. Conformance and Usage Requirements	22
4. Security Considerations	23
4.1 Forgery	23
4.2 Confidentiality	23
4.3 Non-Repudiation	25
5. References	25
6. Acknowledgments	26
Appendix A - Collected Grammar	27
Appendix B - Guidelines for Gatewaying DSNS	29
Gatewaying from other mail systems to DSNS	29
Gatewaying from DSNS to other mail systems	30
Appendix C - Guidelines for Use of DSNS By Mailing List Exploders	30
Appendix D - IANA Registration Forms for DSN Types	31
IANA registration form for address-type	32
IANA registration form for diagnostic-type	32
IANA registration form for MTA-name-type	32
Appendix E - Examples	33
Simple DSN	34
Multi-Recipient DSN	35
DSN from gateway to foreign system	36

Delayed DSN	37
Appendix F - Changes from RFC 1894	38
Authors' Addresses	39
Full Copyright Statement	40

1. Introduction

This memo defines a Multipurpose Internet Mail Extensions (MIME) [MIME1] content-type for Delivery Status Notifications (DSNs). A DSN can be used to notify the sender of a message of any of several conditions: failed delivery, delayed delivery, successful delivery, or the gatewaying of a message into an environment that may not support DSNs. The "message/delivery-status" content-type defined herein is intended for use within the framework of the "multipart/report" content type defined in [REPORT].

This memo defines only the format of the notifications. An extension to the Simple Message Transfer Protocol (SMTP) [SMTP] to fully support such notifications is the subject of a separate memo [DRPT].

Document Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [RFC2119].

1.1 Purposes

The DSNs defined in this memo are expected to serve several purposes:

- (a) Inform human beings of the status of message delivery processing, as well as the reasons for any delivery problems or outright failures, in a manner that is largely independent of human language and media;
- (b) Allow mail user agents to keep track of the delivery status of messages sent, by associating returned DSNs with earlier message transmissions;
- (c) Allow mailing list exploders to automatically maintain their subscriber lists when delivery attempts repeatedly fail;
- (d) Convey delivery and non-delivery notifications resulting from attempts to deliver messages to "foreign" mail systems via a gateway;

- (e) Allow "foreign" notifications to be tunneled through a MIME-capable message system and back into the original messaging system that issued the original notification, or even to a third messaging system;
- (f) Allow language-independent and medium-independent, yet reasonably precise, indications of the reason for the failure of a message to be delivered; and
- (g) Provide sufficient information to remote MTA maintainers (via "trouble tickets") so that they can understand the nature of reported errors. This feature is used in the case that failure to deliver a message is due to the malfunction of a remote MTA and the sender wants to report the problem to the remote MTA administrator.

1.2 Requirements

These purposes place the following constraints on the notification protocol:

- (a) It must be readable by humans as well as being machine-parsable.
- (b) It must provide enough information to allow message senders (or the user agents) to unambiguously associate a DSN with the message that was sent and the original recipient address for which the DSN is issued (if such information is available), even if the message was forwarded to another recipient address.
- (c) It must be able to preserve the reason for the success or failure of a delivery attempt in a remote messaging system, using the "language" (mailbox addresses and status codes) of that remote system.
- (d) It must also be able to describe the reason for the success or failure of a delivery attempt, independent of any particular human language or of the "language" of any particular mail system.
- (e) It must preserve enough information to allow the maintainer of a remote MTA to understand (and if possible, reproduce) the conditions that caused a delivery failure at that MTA.
- (f) For any notifications issued by foreign mail systems, which are translated by a mail gateway to the DSN format, the DSN must preserve the "type" of the foreign addresses and error codes, so that these may be correctly interpreted by gateways.

A DSN contains a set of per-message fields that identify the message and the transaction during which the message was submitted, along with other fields that apply to all delivery attempts described by the DSN. The DSN also includes a set of per-recipient fields to convey the result of the attempt to deliver the message to each of one or more recipients.

1.3 Terminology

A message may be transmitted through several message transfer agents (MTAs) on its way to a recipient. For a variety of reasons, recipient addresses may be rewritten during this process, so each MTA may potentially see a different recipient address. Depending on the purpose for which a DSN is used, different formats of a particular recipient address will be needed.

Several DSN fields are defined in terms of the view from a particular MTA in the transmission. The MTAs are assigned the following names:

(a) Original MTA

The Original MTA is the one to which the message is submitted for delivery by the sender of the message.

(b) Reporting MTA

For any DSN, the Reporting MTA is the one which is reporting the results of delivery attempts described in the DSN.

If the delivery attempts described occurred in a "foreign" (non-Internet) mail system, and the DSN was produced by translating the foreign notice into DSN format, the Reporting MTA will still identify the "foreign" MTA where the delivery attempts occurred.

(c) Received-From MTA

The Received-From MTA is the MTA from which the Reporting MTA received the message, and accepted responsibility for delivery of the message.

(d) Remote MTA

If an MTA determines that it must relay a message to one or more recipients, but the message cannot be transferred to its "next hop" MTA, or if the "next hop" MTA refuses to accept responsibility for delivery of the message to one or more of its intended recipients, the relaying MTA may need to issue a DSN on behalf of the recipients for whom the message cannot be

delivered. In this case the relaying MTA is the Reporting MTA, and the "next hop" MTA is known as the Remote MTA.

Figure 1 illustrates the relationship between the various MTAs.

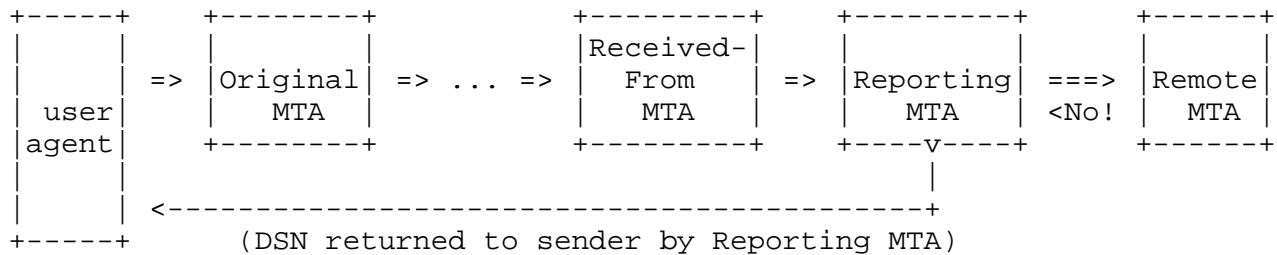


Figure 1. Original, Received-From, Reporting and Remote MTAs

Each of these MTAs may provide information that is useful in a DSN:

- + Ideally, the DSN will contain the address of each recipient as originally specified to the Original MTA by the sender of the message.

This version of the address is needed (rather than a forwarding address or some modified version of the original address) so that the sender may compare the recipient address in the DSN with the address in the sender's records (e.g., an address book for an individual, the list of subscribers for a mailing list) and take appropriate action.

Similarly, the DSN might contain an "envelope identifier" that was known to both the sender's user agent and the Original MTA at the time of message submission, and which, if included in the DSN, can be used by the sender to keep track of which messages were or were not delivered.

- + If a message was (a) forwarded to a different address than that specified by the sender, (b) gatewayed to a different mail system than that used by the sender, or (c) subjected to address rewriting during transmission, the "final" form of the recipient address (i.e., the one seen by the Reporting MTA) will be different than the original (sender-specified) recipient address. Just as the sender's user agent (or the sender) prefers the original recipient address, so the "final" address is needed when reporting a problem to the postmaster of the site where message delivery failed, because only the final recipient address will allow her to reproduce the conditions that caused the failure.

- + A "failed" DSN should contain the most accurate explanation for the delivery failure that is available. For ease of interpretation, this information should be a format that is independent of the mail transport system that issued the DSN. However, if a foreign error code is translated into some transport-independent format, some information may be lost. It is therefore desirable to provide both a transport-independent status code and a mechanism for reporting transport-specific codes. Depending on the circumstances that produced delivery failure, the transport-specific code might be obtained from either the Reporting MTA or the Remote MTA.

Since different values for "recipient address" and "delivery status code" are needed according to the circumstance in which a DSN will be used, and since the MTA that issues the DSN cannot anticipate those circumstances, the DSN format described here may contain both the original and final forms of a recipient address, and both a transport-independent and a transport-specific indication of delivery status.

Extension fields may also be added by the Reporting MTA as needed to provide additional information for use in a trouble ticket or to preserve information for tunneling of foreign delivery reports through Internet DSNs.

The Original, Reporting, and Remote MTAs may exist in very different environments and use dissimilar transport protocols, MTA names, address formats, and delivery status codes. DSNs therefore do not assume any particular format for mailbox addresses, MTA names, or transport-specific status codes. Instead, the various DSN fields that carry such quantities consist of a "type" sub-field followed by a sub-field whose contents are ordinary text characters, and the format of which is indicated by the "type" sub-field. This allows a DSN to convey these quantities regardless of format.

2. Format of a Delivery Status Notification

A DSN is a MIME message with a top-level content-type of multipart/report (defined in [REPORT]). When a multipart/report content is used to transmit a DSN:

- (a) The report-type parameter of the multipart/report content is "delivery-status".
- (b) The first component of the multipart/report contains a human-readable explanation of the DSN, as described in [REPORT].

- (c) The second component of the multipart/report is of content-type message/delivery-status, described in section 2.1 of this document.
- (d) If the original message or a portion of the message is to be returned to the sender, it appears as the third component of the multipart/report.

NOTE: For delivery status notifications gatewayed from foreign systems, the headers of the original message may not be available. In this case the third component of the DSN may be omitted, or it may contain "simulated" RFC 822 headers that contain equivalent information. In particular, it is very desirable to preserve the subject, date, and message-id (or equivalent) fields from the original message.

The DSN MUST be addressed (in both the message header and the transport envelope) to the return address from the transport envelope which accompanied the original message for which the DSN was generated. (For a message that arrived via SMTP, the envelope return address appears in the MAIL FROM command.)

The From field of the message header of the DSN SHOULD contain the address of a human who is responsible for maintaining the mail system at the Reporting MTA site (e.g., Postmaster), so that a reply to the DSN will reach that person. Exception: if a DSN is translated from a foreign delivery report, and the gateway performing the translation cannot determine the appropriate address, the From field of the DSN MAY be the address of a human who is responsible for maintaining the gateway.

The envelope sender address of the DSN SHOULD be chosen to ensure that no delivery status reports will be issued in response to the DSN itself, and MUST be chosen so that DSNs will not generate mail loops. Whenever an SMTP transaction is used to send a DSN, the MAIL FROM command MUST use a NULL return address, i.e., "MAIL FROM:<>".

A particular DSN describes the delivery status for exactly one message. However, an MTA MAY report on the delivery status for several recipients of the same message in a single DSN. Due to the nature of the mail transport system (where responsibility for delivery of a message to its recipients may be split among several MTAs, and delivery to any particular recipient may be delayed), multiple DSNs may still be issued in response to a single message submission.

2.1 The message/delivery-status content-type

The message/delivery-status content-type is defined as follows:

MIME type name:	message
MIME subtype name:	delivery-status
Optional parameters:	none
Encoding considerations:	"7bit" encoding is sufficient and MUST be used to maintain readability when viewed by non-MIME mail readers.
Security considerations:	discussed in section 4 of this memo.

The message/delivery-status report type for use in the multipart/report is "delivery-status".

The body of a message/delivery-status consists of one or more "fields" formatted according to the ABNF of RFC 822 header "fields" (see [RFC822]). The per-message fields appear first, followed by a blank line. Following the per-message fields are one or more groups of per-recipient fields. Each group of per-recipient fields is preceded by a blank line. Using the ABNF of RFC 822, the syntax of the message/delivery-status content is as follows:

```
delivery-status-content = per-message-fields 1*  
                        ( CRLF per-recipient-fields )
```

The per-message fields are described in section 2.2. The per-recipient fields are described in section 2.3.

2.1.1 General conventions for DSN fields

Since these fields are defined according to the rules of RFC 822, the same conventions for continuation lines and comments apply. Notification fields may be continued onto multiple lines by beginning each additional line with a SPACE or HTAB. Text that appears in parentheses is considered a comment and not part of the contents of that notification field. Field names are case-insensitive, so the names of notification fields may be spelled in any combination of upper and lower case letters. Comments in DSN fields may use the "encoded-word" construct defined in [MIME3].

2.1.2 "-type" sub-fields

Several DSN fields consist of a "-type" sub-field, followed by a semicolon, followed by "*text". For these fields, the keyword used in the address-type, diagnostic-type, or MTA-name-type sub-field indicates the expected format of the address, status-code, or MTA-name which follows.

The "-type" sub-fields are defined as follows:

- (a) An "address-type" specifies the format of a mailbox address. For example, Internet mail addresses use the "rfc822" address-type.

address-type = atom

- (b) A "diagnostic-type" specifies the format of a status code. For example, when a DSN field contains a reply code reported via the Simple Mail Transfer Protocol [SMTP], the "smtp" diagnostic-type is used.

diagnostic-type = atom

- (c) An "MTA-name-type" specifies the format of an MTA name. For example, for an SMTP server on an Internet host, the MTA name is the domain name of that host, and the "dns" MTA-name-type is used.

mta-name-type = atom

Values for address-type, diagnostic-type, and MTA-name-type are case-insensitive. Thus address-type values of "RFC822" and "rfc822" are equivalent.

The Internet Assigned Numbers Authority (IANA) will maintain a registry of address-types, diagnostic-types, and MTA-name-types, along with descriptions of the meanings and acceptable values of each, or a reference to one or more specifications that provide such descriptions. (The "rfc822" address-type, "smtp" diagnostic-type, and "dns" MTA-name-type are defined in [DRPT].) Registration forms for address-type, diagnostic-type, and MTA-name-type appear in Appendix D.

IANA will not accept registrations for any address-type, diagnostic-type, or MTA-name-type name that begins with "X-". These type names are reserved for experimental use.

2.1.3 Lexical tokens imported from RFC 822

The following lexical tokens, defined in [RFC822], are used in the ABNF grammar for DSNs: atom, CHAR, comment, CR, CRLF, DIGIT, LF, linear-white-space, SPACE, text. The date-time lexical token is defined in [HOSTREQ].

2.2 Per-Message DSN Fields

Some fields of a DSN apply to all of the delivery attempts described by that DSN. At most, these fields may appear once in any DSN. These fields are used to correlate the DSN with the original message transaction and to provide additional information which may be useful to gateways.

```
per-message-fields =  
    [ original-envelope-id-field CRLF ]  
    reporting-mta-field CRLF  
    [ dsn-gateway-field CRLF ]  
    [ received-from-mta-field CRLF ]  
    [ arrival-date-field CRLF ]  
    *( extension-field CRLF )
```

2.2.1 The Original-Envelope-Id field

The optional Original-Envelope-Id field contains an "envelope identifier" that uniquely identifies the transaction during which the message was submitted, and was either (a) specified by the sender and supplied to the sender's MTA, or (b) generated by the sender's MTA and made available to the sender when the message was submitted. Its purpose is to allow the sender (or her user agent) to associate the returned DSN with the specific transaction in which the message was sent.

If such an envelope identifier was present in the envelope that accompanied the message when it arrived at the Reporting MTA, it SHOULD be supplied in the Original-Envelope-Id field of any DSNs issued as a result of an attempt to deliver the message. Except when a DSN is issued by the sender's MTA, an MTA MUST NOT supply this field unless there is an envelope-identifier field in the envelope that accompanied this message on its arrival at the Reporting MTA.

The Original-Envelope-Id field is defined as follows:

```
original-envelope-id-field =  
    "Original-Envelope-Id" ":" envelope-id  
  
envelope-id = *text
```

There may be at most one Original-Envelope-Id field per DSN.

The envelope-id is CASE-SENSITIVE. The DSN MUST preserve the original case and spelling of the envelope-id.

NOTE: The Original-Envelope-Id is NOT the same as the Message-Id from the message header. The Message-Id identifies the content of the message, while the Original-Envelope-Id identifies the transaction in which the message is sent.

2.2.2 The Reporting-MTA DSN field

```
reporting-mta-field =  
    "Reporting-MTA" ":" mta-name-type ";" mta-name  
  
mta-name = *text
```

The Reporting-MTA field is defined as follows:

A DSN describes the results of attempts to deliver, relay, or gateway a message to one or more recipients. In all cases, the Reporting-MTA is the MTA that attempted to perform the delivery, relay, or gateway operation described in the DSN. This field is required.

Note that if an SMTP client attempts to relay a message to an SMTP server and receives an error reply to a RCPT command, the client is responsible for generating the DSN, and the client's domain name will appear in the Reporting-MTA field. (The server's domain name will appear in the Remote-MTA field.)

Note that the Reporting-MTA is not necessarily the MTA which actually issued the DSN. For example, if an attempt to deliver a message outside of the Internet resulted in a non-delivery notification which was gatewayed back into Internet mail, the Reporting-MTA field of the resulting DSN would be that of the MTA that originally reported the delivery failure, not that of the gateway which converted the foreign notification into a DSN. See Figure 2.

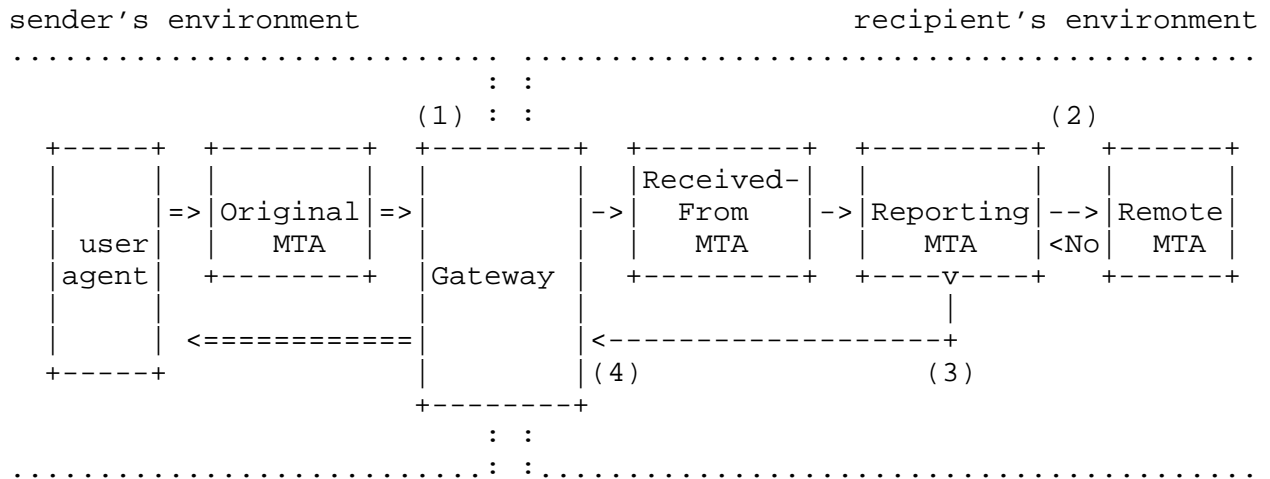


Figure 2. DSNs in the presence of gateways

- (1) message is gatewayed into recipient's environment
- (2) attempt to relay message fails
- (3) reporting-mta (in recipient's environment) returns non-delivery notification
- (4) gateway translates foreign notification into a DSN

The mta-name portion of the Reporting-MTA field is formatted according to the conventions indicated by the mta-name-type sub-field. If an MTA functions as a gateway between dissimilar mail environments and thus is known by multiple names depending on the environment, the mta-name sub-field SHOULD contain the name used by the environment from which the message was accepted by the Reporting-MTA.

Because the exact spelling of an MTA name may be significant in a particular environment, MTA names are CASE-SENSITIVE.

2.2.3 The DSN-Gateway field

The DSN-Gateway field indicates the name of the gateway or MTA that translated a foreign (non-Internet) delivery status notification into this DSN. This field **MUST** appear in any DSN that was translated by a gateway from a foreign system into DSN format, and **MUST NOT** appear otherwise.

```
dsn-gateway-field = "DSN-Gateway" ":" mta-name-type ";" mta-name
```

For gateways into Internet mail, the MTA-name-type will normally be "dns", and the mta-name will be the Internet domain name of the gateway.

2.2.4 The Received-From-MTA DSN field

The optional Received-From-MTA field indicates the name of the MTA from which the message was received.

```
received-from-mta-field =  
    "Received-From-MTA" ":" mta-name-type ";" mta-name
```

If the message was received from an Internet host via SMTP, the contents of the mta-name sub-field SHOULD be the Internet domain name supplied in the HELO or EHLO command, and the network address used by the SMTP client SHOULD be included as a comment enclosed in parentheses. (In this case, the MTA-name-type will be "dns".)

The mta-name portion of the Received-From-MTA field is formatted according to the conventions indicated by the MTA-name-type sub-field.

Since case is significant in some mail systems, the exact spelling, including case, of the MTA name SHOULD be preserved.

2.2.5 The Arrival-Date DSN field

The optional Arrival-Date field indicates the date and time at which the message arrived at the Reporting MTA. If the Last-Attempt-Date field is also provided in a per-recipient field, this can be used to determine the interval between when the message arrived at the Reporting MTA and when the report was issued for that recipient.

```
arrival-date-field = "Arrival-Date" ":" date-time
```

The date and time are expressed in RFC 822 'date-time' format, as modified by [HOSTREQ]. Numeric timezones ([+/-]HHMM format) MUST be used.

2.3 Per-Recipient DSN fields

A DSN contains information about attempts to deliver a message to one or more recipients. The delivery information for any particular recipient is contained in a group of contiguous per-recipient fields. Each group of per-recipient fields is preceded by a blank line.

The syntax for the group of per-recipient fields is as follows:

```
per-recipient-fields =  
  [ original-recipient-field CRLF ]  
  final-recipient-field CRLF  
  action-field CRLF  
  status-field CRLF  
  [ remote-mta-field CRLF ]  
  [ diagnostic-code-field CRLF ]  
  [ last-attempt-date-field CRLF ]  
  [ final-log-id-field CRLF ]  
  [ will-retry-until-field CRLF ]  
  *( extension-field CRLF )
```

2.3.1 Original-Recipient field

The Original-Recipient field indicates the original recipient address as specified by the sender of the message for which the DSN is being issued.

```
original-recipient-field =  
  "Original-Recipient" ":" address-type ";" generic-address  
  
generic-address = *text
```

The address-type field indicates the type of the original recipient address. If the message originated within the Internet, the address-type field will normally be "rfc822", and the address will be according to the syntax specified in [RFC822]. The value "unknown" should be used if the Reporting MTA cannot determine the type of the original recipient address from the message envelope.

This field is optional. It should be included only if the sender-specified recipient address was present in the message envelope, such as by the SMTP extensions defined in [DRPT]. This address is the same as that provided by the sender and can be used to automatically correlate DSN reports and message transactions.

2.3.2 Final-Recipient field

The Final-Recipient field indicates the recipient for which this set of per-recipient fields applies. This field **MUST** be present in each set of per-recipient data.

The syntax of the field is as follows:

```
final-recipient-field =  
    "Final-Recipient" ":" address-type ";" generic-address
```

The generic-address sub-field of the Final-Recipient field MUST contain the mailbox address of the recipient (from the transport envelope), as it was when the Reporting MTA accepted the message for delivery.

The Final-Recipient address may differ from the address originally provided by the sender, because it may have been transformed during forwarding and gatewaying into a totally unrecognizable mess. However, in the absence of the optional Original-Recipient field, the Final-Recipient field and any returned content may be the only information available with which to correlate the DSN with a particular message submission.

The address-type sub-field indicates the type of address expected by the reporting MTA in that context. Recipient addresses obtained via SMTP will normally be of address-type "rfc822".

NOTE: The Reporting MTA is not expected to ensure that the address actually conforms to the syntax conventions of the address-type. Instead, it MUST report exactly the address received in the envelope, unless that address contains characters such as CR or LF which are not allowed in a DSN field.

Since mailbox addresses (including those used in the Internet) may be case sensitive, the case of alphabetic characters in the address MUST be preserved.

2.3.3 Action field

The Action field indicates the action performed by the Reporting-MTA as a result of its attempt to deliver the message to this recipient address. This field MUST be present for each recipient named in the DSN.

The syntax for the action-field is:

```
action-field = "Action" ":" action-value  
  
action-value =  
    "failed" / "delayed" / "delivered" / "relayed" / "expanded"
```

The action-value may be spelled in any combination of upper and lower case characters.

- "failed" indicates that the message could not be delivered to the recipient. The Reporting MTA has abandoned any attempts to deliver the message to this recipient. No further notifications should be expected.
- "delayed" indicates that the Reporting MTA has so far been unable to deliver or relay the message, but it will continue to attempt to do so. Additional notification messages may be issued as the message is further delayed or successfully delivered, or if delivery attempts are later abandoned.
- "delivered" indicates that the message was successfully delivered to the recipient address specified by the sender, which includes "delivery" to a mailing list exploder. It does not indicate that the message has been read. This is a terminal state and no further DSN for this recipient should be expected.
- "relayed" indicates that the message has been relayed or gatewayed into an environment that does not accept responsibility for generating DSNs upon successful delivery. This action-value SHOULD NOT be used unless the sender has requested notification of successful delivery for this recipient.
- "expanded" indicates that the message has been successfully delivered to the recipient address as specified by the sender, and forwarded by the Reporting-MTA beyond that destination to multiple additional recipient addresses. An action-value of "expanded" differs from "delivered" in that "expanded" is not a terminal state. Further "failed" and/or "delayed" notifications may be provided.

Using the terms "mailing list" and "alias" as defined in [DRPT], section 7.2.7: An action-value of "expanded" is only to be used when the message is delivered to a multiple-recipient "alias". An action-value of "expanded" SHOULD NOT be used with a DSN issued on delivery of a message to a "mailing list".

NOTE ON ACTION VS. STATUS CODES: Although the 'action' field might seem to be redundant with the 'status' field, this is not the case. In particular, a "temporary failure" ("4") status code could be used with an action-value of either "delayed" or "failed". For example, assume that an SMTP client repeatedly tries to relay a message to the mail exchanger for a recipient, but fails because a query to a domain name server timed out.

After a few hours, it might issue a "delayed" DSN to inform the sender that the message had not yet been delivered. After a few days, the MTA might abandon its attempt to deliver the message and return a "failed" DSN. The status code (which would begin with a "4" to indicate "temporary failure") would be the same for both DSNs.

Another example for which the action and status codes may appear contradictory: If an MTA or mail gateway cannot deliver a message because doing so would entail conversions resulting in an unacceptable loss of information, it would issue a DSN with the 'action' field of "failure" and a status code of 'XXX'. If the message had instead been relayed, but with some loss of information, it might generate a DSN with the same XXX status-code, but with an action field of "relayed".

2.3.4 Status field

The per-recipient Status field contains a transport-independent status code that indicates the delivery status of the message to that recipient. This field **MUST** be present for each delivery attempt which is described by a DSN.

The syntax of the status field is:

status-field = "Status" ":" status-code

status-code = DIGIT "." 1*3DIGIT "." 1*3DIGIT

- ; White-space characters and comments are NOT allowed within
- ; a status-code, though a comment enclosed in parentheses
- ; MAY follow the last numeric sub-field of the status-code.
- ; Each numeric sub-field within the status-code **MUST** be
- ; expressed without leading zero digits.

Status codes thus consist of three numerical fields separated by ".". The first sub-field indicates whether the delivery attempt was successful (2= success, 4 = persistent temporary failure, 5 = permanent failure). The second sub-field indicates the probable source of any delivery anomalies, and the third sub-field denotes a precise error condition, if known.

The initial set of status-codes is defined in [STATUS].

2.3.5 Remote-MTA field

The value associated with the Remote-MTA DSN field is a printable ASCII representation of the name of the "remote" MTA that reported delivery status to the "reporting" MTA.

```
remote-mta-field = "Remote-MTA" ":" mta-name-type ";" mta-name
```

NOTE: The Remote-MTA field preserves the "while talking to" information that was provided in some pre-existing nondelivery reports.

This field is optional. It MUST NOT be included if no remote MTA was involved in the attempted delivery of the message to that recipient.

2.3.6 Diagnostic-Code field

For a "failed" or "delayed" recipient, the Diagnostic-Code DSN field contains the actual diagnostic code issued by the mail transport. Since such codes vary from one mail transport to another, the diagnostic-type sub-field is needed to specify which type of diagnostic code is represented.

```
diagnostic-code-field =  
    "Diagnostic-Code" ":" diagnostic-type ";" *text
```

NOTE: The information in the Diagnostic-Code field may be somewhat redundant with that from the Status field. The Status field is needed so that any DSN, regardless of origin, may be understood by any user agent or gateway that parses DSNs. Since the Status code will sometimes be less precise than the actual transport diagnostic code, the Diagnostic-Code field is provided to retain the latter information. Such information may be useful in a trouble ticket sent to the administrator of the Reporting MTA, or when tunneling foreign non-delivery reports through DSNs.

If the Diagnostic Code was obtained from a Remote MTA during an attempt to relay the message to that MTA, the Remote-MTA field should be present. When interpreting a DSN, the presence of a Remote-MTA field indicates that the Diagnostic Code was issued by the Remote MTA. The absence of a Remote-MTA indicates that the Diagnostic Code was issued by the Reporting MTA.

In addition to the Diagnostic-Code itself, additional textual description of the diagnostic, MAY appear in a comment enclosed in parentheses.

This field is optional, because some mail systems supply no additional information beyond that which is returned in the 'action' and 'status' fields. However, this field SHOULD be included if transport-specific diagnostic information is available.

2.3.7 Last-Attempt-Date field

The Last-Attempt-Date field gives the date and time of the last attempt to relay, gateway, or deliver the message (whether successful or unsuccessful) by the Reporting MTA. This is not necessarily the same as the value of the Date field from the header of the message used to transmit this delivery status notification: In cases where the DSN was generated by a gateway, the Date field in the message header contains the time the DSN was sent by the gateway and the DSN Last-Attempt-Date field contains the time the last delivery attempt occurred.

last-attempt-date-field = "Last-Attempt-Date" ":" date-time

This field is optional. It MUST NOT be included if the actual date and time of the last delivery attempt are not available (which might be the case if the DSN were being issued by a gateway).

The date and time are expressed in RFC 822 'date-time' format, as modified by [HOSTREQ]. Numeric timezones ([+/-]HHMM format) MUST be used.

2.3.8 final-log-id field

The "final-log-id" field gives the final-log-id of the message that was used by the final-mta. This can be useful as an index to the final-mta's log entry for that delivery attempt.

final-log-id-field = "Final-Log-ID" ":" *text

This field is optional.

2.3.9 Will-Retry-Until field

For DSNs of type "delayed", the Will-Retry-Until field gives the date after which the Reporting MTA expects to abandon all attempts to deliver the message to that recipient. The Will-Retry-Until field is optional for "delay" DSNs, and MUST NOT appear in other DSNs.

will-retry-until-field = "Will-Retry-Until" ":" date-time

The date and time are expressed in RFC 822 'date-time' format, as modified by [HOSTREQ]. Numeric timezones ([+/-]HHMM format) MUST be used.

2.4 Extension fields

Additional per-message or per-recipient DSN fields may be defined in the future by later revisions or extensions to this specification. Extension-field names beginning with "X-" will never be defined as standard fields; such names are reserved for experimental use. DSN field names NOT beginning with "X-" MUST be registered with the Internet Assigned Numbers Authority (IANA) and published in an RFC.

Extension DSN fields may be defined for the following reasons:

- (a) To allow additional information from foreign delivery status reports to be tunneled through Internet DSNS. The names of such DSN fields should begin with an indication of the foreign environment name (e.g., X400-Physical-Forwarding-Address).
- (b) To allow the transmission of diagnostic information which is specific to a particular mail transport protocol. The names of such DSN fields should begin with an indication of the mail transport being used (e.g., SMTP-Remote-Recipient-Address). Such fields should be used for diagnostic purposes only and not by user agents or mail gateways.
- (c) To allow transmission of diagnostic information which is specific to a particular message transfer agent (MTA). The names of such DSN fields should begin with an indication of the MTA implementation that produced the DSN. (e.g., Foomail-Queue-ID).

MTA implementers are encouraged to provide adequate information, via extension fields if necessary, to allow an MTA maintainer to understand the nature of correctable delivery failures and how to fix them. For example, if message delivery attempts are logged, the DSN might include information that allows the MTA maintainer to easily find the log entry for a failed delivery attempt.

If an MTA developer does not wish to register the meanings of such extension fields, "X-" fields may be used for this purpose. To avoid name collisions, the name of the MTA implementation should follow the "X-", (e.g., "X-Foomail-Log-ID").

3. Conformance and Usage Requirements

An MTA or gateway conforms to this specification if it generates DSNs according to the protocol defined in this memo. For MTAs and gateways that do not support requests for positive delivery notification (such as in [DRPT]), it is sufficient that delivery failure reports use this protocol.

A minimal implementation of this specification need generate only the Reporting-MTA per-message field, and the Final-Recipient, Action, and Status fields for each attempt to deliver a message to a recipient described by the DSN. Generation of the other fields, when appropriate, is strongly recommended.

MTAs and gateways MUST NOT generate the Original-Recipient field of a DSN unless the mail transfer protocol provides the address originally specified by the sender at the time of submission. (Ordinary SMTP does not make that guarantee, but the SMTP extension defined in [DRPT] permits such information to be carried in the envelope if it is available.)

Each sender-specified recipient address SHOULD result in at most one "delivered" or "failed" DSN for that recipient. If a positive DSN is requested (e.g., one using NOTIFY=SUCCESS in SMTP) for a recipient that is forwarded to multiple recipients of an "alias" (as defined in [DRPT], section 7.2.7), the forwarding MTA SHOULD normally issue a "expanded" DSN for the originally-specified recipient and not propagate the request for a DSN to the forwarding addresses. Alternatively, the forwarding MTA MAY relay the request for a DSN to exactly one of the forwarding addresses and not propagate the request to the others.

By contrast, successful submission of a message to a mailing list exploder is considered final delivery of the message. Upon delivery of a message to a recipient address corresponding to a mailing list exploder, the Reporting MTA SHOULD issue an appropriate DSN exactly as if the recipient address were that of an ordinary mailbox.

NOTE: This is actually intended to make DSNs usable by mailing lists themselves. Any message sent to a mailing list subscriber should have its envelope return address pointing to the list maintainer [see RFC 1123, section 5.3.7(E)]. Since DSNs are sent to the envelope return address, all DSNs resulting from delivery to the recipients of a mailing list will be sent to the list maintainer. The list maintainer may elect to mechanically process DSNs upon receipt, and thus automatically delete invalid addresses from the list. (See section 7 of this memo.)

This specification places no restrictions on the processing of DSNs received by user agents or distribution lists.

4. Security Considerations

The following security considerations apply when using DSNs:

4.1 Forgery

DSNs may be forged as easily as ordinary Internet electronic mail. User agents and automatic mail handling facilities (such as mail distribution list exploders) that wish to make automatic use of DSNs should take appropriate precautions to minimize the potential damage from denial-of-service attacks.

Security threats related to forged DSNs include the sending of:

- (a) A falsified delivery notification when the message is not delivered to the indicated recipient,
- (b) A falsified non-delivery notification when the message was in fact delivered to the indicated recipient,
- (c) A falsified Final-Recipient address,
- (d) A falsified Remote-MTA identification,
- (e) A falsified relay notification when the message is "dead ended".
- (f) Unsolicited DSNs

4.2 Confidentiality

Another dimension of security is confidentiality. There may be cases in which a message recipient is autoforwarding messages but does not wish to divulge the address to which the messages are autoforwarded. The desire for such confidentiality will probably be heightened as "wireless mailboxes", such as pagers, become more widely used as autoforward addresses.

MTA authors are encouraged to provide a mechanism which enables the end user to preserve the confidentiality of a forwarding address. Depending on the degree of confidentiality required, and the nature of the environment to which a message were being forwarded, this might be accomplished by one or more of:

- (a) issuing a "relayed" DSN (if a positive DSN was requested) when a message is forwarded to a confidential forwarding address, and disabling requests for positive DSNs for the forwarded message,
- (b) declaring the message to be delivered, issuing a "delivered" DSN, re-sending the message to the confidential forwarding address, and arranging for no DSNs to be issued for the re-sent message,
- (c) omitting "Remote-*" or extension fields of a DSN whenever they would otherwise contain confidential information (such as a confidential forwarding address),
- (d) for messages forwarded to a confidential address, setting the envelope return address (e.g., SMTP MAIL FROM address) to the NULL reverse-path ("<>") (so that no DSNs would be sent from a downstream MTA to the original sender),
- (e) for messages forwarded to a confidential address, disabling delivery notifications for the forwarded message (e.g., if the "next-hop" MTA uses ESMTP and supports the DSN extension, by using the NOTIFY=NEVER parameter to the RCPT command), or
- (f) when forwarding mail to a confidential address, having the forwarding MTA rewrite the envelope return address for the forwarded message and attempt delivery of that message as if the forwarding MTA were the originator. On its receipt of final delivery status, the forwarding MTA would issue a DSN to the original sender.

In general, any optional DSN field may be omitted if the Reporting MTA site determines that inclusion of the field would impose too great a compromise of site confidentiality. The need for such confidentiality must be balanced against the utility of the omitted information in trouble reports and DSNs gatewayed to foreign environments.

Implementers are cautioned that many existing MTAs will send non-delivery notifications to a return address in the message header (rather than to the one in the envelope), in violation of SMTP and other protocols. If a message is forwarded through such an MTA, no reasonable action on the part of the forwarding MTA will prevent the downstream MTA from compromising the forwarding address. Likewise, if the recipient's MTA automatically responds to messages based on a request in the message header (such as the nonstandard, but widely used, Return-Receipt-To extension header), it will also compromise the forwarding address.

4.3 Non-Repudiation

Within the framework of today's internet mail, the DSNs defined in this memo provide valuable information to the mail user; however, even a "failed" DSN can not be relied upon as a guarantee that a message was not received by the recipient. Even if DSNs are not actively forged, conditions exist under which a message can be delivered despite the fact that a failure DSN was issued.

For example, a race condition in the SMTP protocol allows for the duplication of messages if the connection is dropped following a completed DATA command, but before a response is seen by the SMTP client.

This will cause the SMTP client to retransmit the message, even though the SMTP server has already accepted it [SMTPDUP]. If one of those delivery attempts succeeds and the other one fails, a "failed" DSN could be issued even though the message actually reached the recipient.

5. Normative References

- [DRPT] Moore, K., "SMTP Service Extension for Delivery Status Notifications", RFC 3461, January 2003.
- [DSN] Moore, K. and G. Vaudreuil, "An Extensible Message Format for Delivery Status Notifications", RFC 1894, January 1996.
- [HOSTREQ] Braden, R. (ed.), "Requirements for Internet Hosts - Application and Support", STD 3, RFC 1123, October 1989.
- [MIME1] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.
- [MIME3] Moore, K., "MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text", RFC 2047, November 1996.
- [REPORT] Vaudreuil, G., "The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages", RFC 3462, January 2003.
- [RFC822] Crocker, D., "Standard for the format of ARPA Internet Text Messages", STD 11, RFC 822, August 1982.
- [SMTP] Postel, J., "Simple Mail Transfer Protocol", STD 10, RFC 821, August 1982.

[SMTPDUP] Partridge, C., "Duplicate Messages and SMTP", RFC 1047, February 1988.

[STATUS] Vaudreuil, G., "Enhanced Mail System Status Codes", RFC 3463, January 2003.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

6. Acknowledgments

The authors wish to thank the following people for their reviews of early drafts of RFC 1894, of which this document is a revision, and their suggestions for improvement: Eric Allman, Harald Alvestrand, Allan Cargille, Jim Conklin, Peter Cowen, Dave Crocker, Roger Fajman, Ned Freed, Marko Kaittola, Steve Kille, John Klensin, John Gardiner Myers, Mark Nahabedian, Julian Onions, Jacob Palme, Jean Charles Roy, and Gregory Sheehan.

Appendix A - collected grammar

NOTE: The following lexical tokens are defined in RFC 822: atom, CHAR, comment, CR, CRLF, DIGIT, LF, linear-white-space, SPACE, text. The date-time lexical token is defined in [HOSTREQ].

```
action-field = "Action" ":" action-value

action-value = "failed" / "delayed" / "delivered"
              / "relayed" / "expanded"

address-type = atom

arrival-date-field = "Arrival-Date" ":" date-time

delivery-status-content = per-message-fields
                          1*( CRLF per-recipient-fields )

diagnostic-code-field = "Diagnostic-Code" ":"
                        diagnostic-type ";" *text

diagnostic-type = atom

dsn-gateway-field = "DSN-Gateway" ":" mta-name-type ";" mta-name

envelope-id = *text

extension-field = extension-field-name ":" *text

extension-field-name = atom

final-recipient-field =
    "Final-Recipient" ":" address-type ";" generic-address

final-log-id-field = "Final-Log-ID" ":" *text

generic-address = *text

last-attempt-date-field = "Last-Attempt-Date" ":" date-time

mta-name = *text

mta-name-type = atom

original-envelope-id-field =
    "Original-Envelope-Id" ":" envelope-id
```

```
original-recipient-field =  
    "Original-Recipient" ":" address-type ";" generic-address
```

```
per-message-fields =  
    [ original-envelope-id-field CRLF ]  
    reporting-mta-field CRLF  
    [ dsn-gateway-field CRLF ]  
    [ received-from-mta-field CRLF ]  
    [ arrival-date-field CRLF ]  
    *( extension-field CRLF )
```

```
per-recipient-fields =  
    [ original-recipient-field CRLF ]  
    final-recipient-field CRLF  
    action-field CRLF  
    status-field CRLF  
    [ remote-mta-field CRLF ]  
    [ diagnostic-code-field CRLF ]  
    [ last-attempt-date-field CRLF ]  
    [ final-log-id-field CRLF ]  
    [ will-retry-until-field CRLF ]  
    *( extension-field CRLF )
```

```
received-from-mta-field =  
    "Received-From-MTA" ":" mta-name-type ";" mta-name
```

```
remote-mta-field =  
    "Remote-MTA" ":" mta-name-type ";" mta-name
```

```
reporting-mta-field =  
    "Reporting-MTA" ":" mta-name-type ";" mta-name
```

```
status-code = DIGIT "." 1*3DIGIT "." 1*3DIGIT
```

```
    ; White-space characters and comments are NOT allowed within a  
    ; a status-code, though a comment enclosed in parentheses  
    ; MAY follow the last numeric sub-field of the status-code.  
    ; Each numeric sub-field within the status-code MUST be  
    ; expressed without leading zero digits.
```

```
status-field = "Status" ":" status-code
```

```
will-retry-until-field = "Will-Retry-Until" ":" date-time
```

Appendix B - Guidelines for gatewaying DSNs

NOTE: This section provides non-binding recommendations for the construction of mail gateways that wish to provide semi-transparent delivery reports between the Internet and another electronic mail system. Specific DSN gateway requirements for a particular pair of mail systems may be defined by other documents.

Gatewaying from other mail systems to DSNs

A mail gateway may issue a DSN to convey the contents of a "foreign" delivery or non-delivery notification over Internet mail. When there are appropriate mappings from the foreign notification elements to DSN fields, the information may be transmitted in those DSN fields. Additional information (such as might be useful in a trouble ticket or needed to tunnel the foreign notification through the Internet) may be defined in extension DSN fields. (Such fields should be given names that identify the foreign mail protocol, e.g., X400-* for X.400 NDN or DN protocol elements)

The gateway must attempt to supply reasonable values for the Reporting-MTA, Final-Recipient, Action, and Status fields. These will normally be obtained by translating the values from the remote delivery or non-delivery notification into their Internet-style equivalents. However, some loss of information is to be expected. For example, the set of status-codes defined for DSNs may not be adequate to fully convey the delivery diagnostic code from the foreign system. The gateway should assign the most precise code which describes the failure condition, falling back on "generic" codes such as 2.0.0 (success), 4.0.0 (temporary failure), and 5.0.0 (permanent failure) when necessary. The actual foreign diagnostic code should be retained in the Diagnostic-Code field (with an appropriate diagnostic-type value) for use in trouble tickets or tunneling.

The sender-specified recipient address, and the original envelope-id, if present in the foreign transport envelope, should be preserved in the Original-Recipient and Original-Envelope-ID fields.

The gateway should also attempt to preserve the "final" recipient addresses and MTA names from the foreign system. Whenever possible, foreign protocol elements should be encoded as meaningful printable ASCII strings.

For DSNs produced from foreign delivery or nondelivery notifications, the name of the gateway MUST appear in the DSN-Gateway field of the DSN.

Gatewaying from DSNs to other mail systems

It may be possible to gateway DSNs from the Internet into a foreign mail system. The primary purpose of such gatewaying is to convey delivery status information in a form that is usable by the destination system. A secondary purpose is to allow "tunneling" of DSNs through foreign mail systems, in case the DSN may be gatewayed back into the Internet.

In general, the recipient of the DSN (i.e., the sender of the original message) will want to know, for each recipient: the closest available approximation to the original recipient address, the delivery status (success, failure, or temporary failure), and for failed deliveries, a diagnostic code that describes the reason for the failure.

If possible, the gateway should attempt to preserve the Original-Recipient address and Original-Envelope-ID (if present), in the resulting foreign delivery status report.

When reporting delivery failures, if the diagnostic-type sub-field of the Diagnostic-Code field indicates that the original diagnostic code is understood by the destination environment, the information from the Diagnostic-Code field should be used. Failing that, the information in the Status field should be mapped into the closest available diagnostic code used in the destination environment.

If it is possible to tunnel a DSN through the destination environment, the gateway specification may define a means of preserving the DSN information in the delivery status reports used by that environment.

Appendix C - Guidelines for use of DSNs by mailing list exploders

This section pertains only to the use of DSNs by "mailing lists" as defined in [4], section 7.2.7.

DSNs are designed to be used by mailing list exploders to allow them to detect and automatically delete recipients for whom mail delivery fails repeatedly.

When forwarding a message to list subscribers, the mailing list exploder should always set the envelope return address (e.g., SMTP MAIL FROM address) to point to a special address which is set up to receive non-delivery reports. A "smart" mailing list exploder can therefore intercept such non-delivery reports, and if they are in the DSN format, automatically examine them to determine for which recipients a message delivery failed or was delayed.

The Original-Recipient field should be used if available, since it should exactly match the subscriber address known to the list. If the Original-Recipient field is not available, the recipient field may resemble the list subscriber address. Often, however, the list subscriber will have forwarded his mail to a different address, or the address may be subject to some re-writing, so heuristics may be required to successfully match an address from the recipient field. Care is needed in this case to minimize the possibility of false matches.

The reason for delivery failure can be obtained from the Status and Action fields, and from the Diagnostic-Code field (if the status-type is recognized). Reports for recipients with action values other than "failed" can generally be ignored; in particular, subscribers should not be removed from a list due to "delayed" reports.

In general, almost any failure status code (even a "permanent" one) can result from a temporary condition. It is therefore recommended that a list exploder not delete a subscriber based on any single failure DSN (regardless of the status code), but only on the persistence of delivery failure over a period of time.

However, some kinds of failures are less likely than others to have been caused by temporary conditions, and some kinds of failures are more likely to be noticed and corrected quickly than others. Once more precise status codes are defined, it may be useful to differentiate between the status codes when deciding whether to delete a subscriber. For example, on a list with a high message volume, it might be desirable to temporarily suspend delivery to a recipient address which causes repeated "temporary" failures, rather than simply deleting the recipient. The duration of the suspension might depend on the type of error. On the other hand, a "user unknown" error that persisted for several days could be considered a reliable indication that address were no longer valid.

Appendix D - IANA registration forms for DSN types

The forms below are for use when registering a new address-type, diagnostic-type, or MTA-name-type with the Internet Assigned Numbers Authority (IANA). Each piece of information requested by a registration form may be satisfied either by providing the information on the form itself, or by including a reference to a published, publicly available specification which includes the necessary information. IANA MAY reject DSN type registrations because of incomplete registration forms, imprecise specifications, or inappropriate type names.

To register a DSN type, complete the applicable form below and send it via Internet electronic mail to <IANA@IANA.ORG>.

IANA registration form for address-type

A registration for a DSN address-type MUST include the following information:

- (a) The proposed address-type name.
- (b) The syntax for mailbox addresses of this type, specified using BNF, regular expressions, ASN.1, or other non-ambiguous language.
- (c) If addresses of this type are not composed entirely of graphic characters from the US-ASCII repertoire, a specification for how they are to be encoded as graphic US-ASCII characters in a DSN Original-Recipient or Final-Recipient DSN field.
- (d) [optional] A specification for how addresses of this type are to be translated to and from Internet electronic mail addresses.

IANA registration form for diagnostic-type

A registration for a DSN address-type MUST include the following information:

- (a) The proposed diagnostic-type name.
- (b) A description of the syntax to be used for expressing diagnostic codes of this type as graphic characters from the US-ASCII repertoire.
- (c) A list of valid diagnostic codes of this type and the meaning of each code.
- (d) [optional] A specification for mapping from diagnostic codes of this type to DSN status codes (as defined in [5]).

IANA registration form for MTA-name-type

A registration for a DSN MTA-name-type must include the following information:

- (a) The proposed MTA-name-type name.
- (b) A description of the syntax of MTA names of this type, using BNF, regular expressions, ASN.1, or other non-ambiguous language.

- (c) If MTA names of this type do not consist entirely of graphic characters from the US-ASCII repertoire, a specification for how an MTA name of this type should be expressed as a sequence of graphic US-ASCII characters.

Appendix E - Examples

These examples are provided as illustration only, and are not considered part of the DSN protocol specification. If an example conflicts with the protocol definition above, the example is wrong.

Likewise, the use of *-type sub-field names or extension fields in these examples is not to be construed as a definition for those type names or extension fields.

These examples were manually translated from bounced messages using whatever information was available.

Simple DSN

This is a simple DSN issued after repeated attempts to deliver a message failed. In this case, the DSN is issued by the same MTA from which the message was originated.

Date: Thu, 7 Jul 1994 17:16:05 -0400 From: Mail Delivery Subsystem
<MAILER-DAEMON@CS.UTK.EDU> Message-Id:
<199407072116.RAA14128@CS.UTK.EDU> Subject: Returned mail: Cannot
send message for 5 days To: <owner-info-mime@cs.utk.edu> MIME-
Version: 1.0 Content-Type: multipart/report; report-type=delivery-
status;

boundary="RAA14128.773615765/CS.UTK.EDU"

--RAA14128.773615765/CS.UTK.EDU

The original message was received at Sat, 2 Jul 1994 17:10:28 -0400
from root@localhost

----- The following addresses had delivery problems -----
<louisl@larry.slip.umd.edu> (unrecoverable error)

----- Transcript of session follows -----
<louisl@larry.slip.umd.edu>... Deferred: Connection timed out
with larry.slip.umd.edu.
Message could not be delivered for 5 days
Message will be deleted from queue

--RAA14128.773615765/CS.UTK.EDU
content-type: message/delivery-status

Reporting-MTA: dns; cs.utk.edu

Original-Recipient: rfc822;louisl@larry.slip.umd.edu
Final-Recipient: rfc822;louisl@larry.slip.umd.edu
Action: failed
Status: 4.0.0
Diagnostic-Code: smtp; 426 connection timed out
Last-Attempt-Date: Thu, 7 Jul 1994 17:15:49 -0400

--RAA14128.773615765/CS.UTK.EDU
content-type: message/rfc822

[original message goes here]

--RAA14128.773615765/CS.UTK.EDU--

Multi-Recipient DSN

This is another DSN issued by the sender's MTA, which contains details of multiple delivery attempts. Some of these were detected locally, and others by a remote MTA.

Date: Fri, 8 Jul 1994 09:21:47 -0400
From: Mail Delivery Subsystem <MAILER-DAEMON@CS.UTK.EDU>
Subject: Returned mail: User unknown
To: <owner-ups-mib@CS.UTK.EDU>
MIME-Version: 1.0
Content-Type: multipart/report; report-type=delivery-status;
boundary="JAA13167.773673707/CS.UTK.EDU"

--JAA13167.773673707/CS.UTK.EDU
content-type: text/plain; charset=us-ascii

----- The following addresses had delivery problems -----
<arathib@vnet.ibm.com> (unrecoverable error)
<wsnell@sdcc13.ucsd.edu> (unrecoverable error)

--JAA13167.773673707/CS.UTK.EDU
content-type: message/delivery-status

Reporting-MTA: dns; cs.utk.edu

Original-Recipient: rfc822;arathib@vnet.ibm.com
Final-Recipient: rfc822;arathib@vnet.ibm.com
Action: failed
Status: 5.0.0 (permanent failure)
Diagnostic-Code: smtp; 550 'arathib@vnet.IBM.COM' is not a
registered gateway user
Remote-MTA: dns; vnet.ibm.com

Original-Recipient: rfc822;johnh@hpnjld.njd.hp.com
Final-Recipient: rfc822;johnh@hpnjld.njd.hp.com
Action: delayed
Status: 4.0.0 (hpnjld.njd.jp.com: host name lookup failure)

Original-Recipient: rfc822;wsnell@sdcc13.ucsd.edu
Final-Recipient: rfc822;wsnell@sdcc13.ucsd.edu
Action: failed
Status: 5.0.0
Diagnostic-Code: smtp; 550 user unknown
Remote-MTA: dns; sdcc13.ucsd.edu

--JAA13167.773673707/CS.UTK.EDU
content-type: message/rfc822

[original message goes here]

--JAA13167.773673707/CS.UTK.EDU--

DSN from gateway to foreign system

A delivery report generated by Message Router (MAILBUS) and gatewayed by PMDF_MR to a DSN. In this case the gateway did not have sufficient information to supply an original-recipient address.

Disclose-recipients: prohibited
Date: Fri, 08 Jul 1994 09:21:25 -0400 (EDT)
From: Message Router Submission Agent <AMMGR@corp.timeplex.com>
Subject: Status of: Re: Battery current sense
To: owner-ups-mib@CS.UTK.EDU
Message-id: <01HEGJ0WNB28Y95LN@mr.timeplex.com>
MIME-version: 1.0
content-type: multipart/report;
 report-type=delivery-status;
 boundary="84229080704991.122306.SYS30"

--84229080704991.122306.SYS30
content-type: text/plain

Invalid address - nair_s
%DIR-E-NODIRMTCH, No matching Directory Entry
Entry found

--84229080704991.122306.SYS30
content-type: message/delivery-status

Reporting-MTA: mailbus; SYS30

Final-Recipient: unknown; nair_s
Status: 5.0.0 (unknown permanent failure)
Action: failed

--84229080704991.122306.SYS30--

Delayed DSN

A delay report from a multiprotocol MTA. Note that there is no returned content, so no third body part appears in the DSN.

MIME-Version: 1.0
From: <postmaster@nsfnet-relay.ac.uk>
Message-Id: <199407092338.TAA23293@CS.UTK.EDU>
Received: from nsfnet-relay.ac.uk by sun2.nsfnet-relay.ac.uk
id <g.12954-0@sun2.nsfnet-relay.ac.uk>;
Sun, 10 Jul 1994 00:36:51 +0100
To: owner-info-mime@cs.utk.edu
Date: Sun, 10 Jul 1994 00:36:51 +0100
Subject: WARNING: message delayed at "nsfnet-relay.ac.uk"
content-type: multipart/report; report-type=delivery-status;
boundary=foobar

--foobar
content-type: text/plain

The following message:

UA-ID: Reliable PC (...
Q-ID: sun2.nsf:77/msg.11820-0

has not been delivered to the intended recipient:

thomas@de-montfort.ac.uk

despite repeated delivery attempts over the past 24 hours.

The usual cause of this problem is that the remote system is temporarily unavailable.

Delivery will continue to be attempted up to a total elapsed time of 168 hours, i.e., 7 days.

You will be informed if delivery proves to be impossible within this time.

Please quote the Q-ID in any queries regarding this mail.

--foobar
content-type: message/delivery-status

Reporting-MTA: dns; sun2.nsfnet-relay.ac.uk

Final-Recipient: rfc822;thomas@de-montfort.ac.uk

Status: 4.0.0 (unknown temporary failure)

Action: delayed

--foobar--

Appendix F - Changes from RFC 1894

Changed Authors contact information

Updated required standards boilerplate

Edited the text to make it spell-checker and grammar checker compliant

Updated references to point to later, more mature documents, changed reference enumeration scheme.

Fixed paragraph numbering on page 20

Fixed Delayed DSN example

Added Table of Contents

Moved Appendices to the end of the document

Changed the MTA-name-Type for gateways into Internet mail, the MTA-name-type from "SMTP" to "dns".

Authors' Addresses

Keith Moore
University of Tennessee
1122 Volunteer Blvd, Suite 203
Knoxville TN 37996-3450
USA

Phone: +1-865-974-3126
Fax: +1-865-974-8296
EMail: moore@cs.utk.edu

Gregory M. Vaudreuil
Lucent Technologies
7291 Williamson Rd
Dallas, Tx. 75214
USA

Phone: +1 214 823 9325
EMail: GregV@ieee.org

Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS 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.

Acknowledgement

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

