Network Working Group
Request for Comments: 1892
Category: Standards Track

G. Vaudreuil
Octel Network Services

January 1996

The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages

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.

1. The Multipart/Report MIME content-type

The Multipart/Report MIME content-type is a general "family" or "container" type for electronic mail reports of any kind. Although this memo defines only the use of the Multipart/Report content-type with respect to delivery status reports, mail processing programs will benefit if a single content-type is used to for all kinds of reports.

The Multipart/Report content-type is defined as follows:

MIME type name: multipart
MIME subtype name: report
Required parameters: boundary, report-type
Optional parameters: none
Encoding considerations: 7bit should always be adequate
Security considerations: see section 4 of this memo.

The syntax of Multipart/Report is identical to the Multipart/Mixed content type defined in [MIME]. When used to send a report, the Multipart/Report content-type must be the top-level MIME content type for any report message. The report-type parameter identifies the type of report. The parameter is the MIME content sub-type of the second body part of the Multipart/Report.

User agents and gateways must be able to automatically determine that a message is a mail system report and should be processed as such. Placing the Multipart/Report as the outermost content provides a mechanism whereby an auto-processor may detect through parsing the RFC 822 headers that the message is a report.

The Multipart/Report content-type contains either two or three sub-parts, in the following order:

(1) [required] The first body part contains human readable message. The purpose of this message is to provide an easily-understood description of the condition(s) that caused the report to be generated, for a human reader who may not have an user agent capable of interpreting the second section of the Multipart/Report.

The text in the first section may be in any MIME standards-track content-type, charset, or language. Where a description of the error is desired in several languages or several media, a Multipart/Alternative construct may be used.

This body part may also be used to send detailed information that cannot be easily formatted into a Message/Report body part.

(2) [required] A machine parsable body part containing an account of the reported message handling event. The purpose of this body part is to provide a machine-readable description of the condition(s) which caused the report to be generated, along with details not present in the first body part that may be useful to human experts. An initial body part, Message/delivery-status is defined in [DSN]

(3) [optional] A body part containing the returned message or a portion thereof. This information may be useful to aid human experts in diagnosing problems. (Although it may also be useful to allow the sender to identify the message which the report was issued, it is hoped that the envelope-id and original-recipient-address returned in the Message/Report body part will replace the traditional use of the returned content for this purpose.)

Return of content may be wasteful of network bandwidth and a variety of implementation strategies can be used. Generally the sender should choose the appropriate strategy and inform the recipient of the required level of returned content required. In the absence of an explicit request for level of return of content such as that provided in [DRPT], the agent which generated the delivery service report should return the full message content.

When data not encoded in 7 bits is to be returned, and the return path is not guaranteed to be 8-bit capable, two options are available. The origional message MAY be reencoded into a legal 7 bit MIME message or the Text/RFC822-Headers content-type MAY be used to return only the origional message headers.

2. The Text/RFC822-Headers MIME content-type

The Text/RFC822-Headers MIME content-type provides a mechanism to label and return only the RFC 822 headers of a failed message. These headers are not the complete message and should not be returned as a Message/RFC822. The returned headers are useful for identifying the failed message and for diagnostics based on the received: lines.

The Text/RFC822-Headers content-type is defined as follows:

```
MIME type name: Text
MIME subtype name: RFC822-Headers
Required parameters: None
Optional parameters: none
Encoding considerations: 7 bit is sufficient for normal RFC822
       headers, however, if the headers are broken and require
       encoding, they may be encoded in quoted-printable.
Security considerations: see section 4 of this memo.
```

The Text/RFC822-headers body part should contain all the RFC822 header lines from the message which caused the report. The RFC822 headers include all lines prior to the blank line in the message. They include the MIME-Version and MIME Content- headers.

3. References

[DSN] Moore, K., and G. Vaudreuil, "An Extensible Message Format for Delivery Status Notifications", RFC 1894, University of Tennessee, Octel Network Services, January 1996.

[RFC822] Crocker, D., "Standard for the format of ARPA Internet Text Messages", STD 11, RFC 822, UDEL, August 1982.

[MIME] Borenstein, N., and N. Freed, "Multipurpose Internet Mail Extensions", RFC 1521, Bellcore, Innosoft, June 1992.

[DRPT] Moore, K., "SMTP Service Extension for Delivery Status Notifications", RFC 1891, University of Tennessee, January 1996.

4. Security Considerations

Automated use of report types without authentication presents several security issues. Forging negative reports presents the opportunity for denial-of-service attacks when the reports are used for automated maintenance of directories or mailing lists. Forging positive reports may cause the sender to incorrectly believe a message was delivered when it was not.

5. Author's Address

Gregory M. Vaudreuil
Octel Network Services
17060 Dallas Parkway
Dallas, TX 75248-1905

Phone: +1-214-733-2722
EMail: Greg.Vaudreuil@Octel.com