RARE-DRAFT
IESG Mail Applicability Design Team
<draft-rare-msg-a-bombs-00.txt>

Jeroen Houttuin
RARE Secretariat
April 1994

Bombs series: Behaviour of Mail Based Servers
Part 2: A-bombs
Answering servers

Abstract

This document defines rules for the behaviour of Mail Based Echo Servers and Vacation Servers in the Internet. It is highly desirable that other e-mail networks connected to the Internet also implement these rules.

Status of this Memo

This document is a RARE Draft. RARE Drafts form a subseries of the Internet Drafts, which 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. For example, RARE Drafts are produced by the RARE Working Groups.

Internet Drafts are draft documents valid for a maximum of six months. Internet Drafts may be updated, replaced, or obsoleted by other documents at any time. It is not appropriate to use Internet Drafts as reference material or to cite them other than as a "working draft" or "work in progress."

Please check the I-D abstract listing contained in each Internet Draft directory to learn the current status of this or any other Internet Draft.

Distribution of this memo is unlimited.

This document builds upon the classification of MBS types, which can be found in the Bombs series, part1: C-bombs [13].

Within the context of the connectivity testing tool 'concord', initial work on the requirements for echo servers was done within SWITCH and XNREN ([7], [8]).

The document was then integrated in the work of the IESG solicited Mail Applicability Design Team, consisting of: Ned Freed (INNOsoft), Jeroen Houttuin (RARE), John Klensin (INfoods, UN), Keith Moore (University of Tennessee).

Depending on the nature of your comments, please respond to one of the following addresses:

The main discussion group:	wg-msg@rare.nl
The design team:	mail-as@infoods.unu.edu
The author:	houttuin@rare.nl

Contents

1. Introduction

Mail Based Servers (MBSs) are defined in C-bombs [13] as follows:

An MBS is a process that automatically generates one or more messages (the output messages) as a result of receiving a message (the input message).

Two main types are identified: repliers and forwarders. This documents deals only with the basic behaviour of a subclass of repliers: echo servers and vacation servers (jointly referred to as 'answering servers').

2. General approach

The overall approach for all MBS header requirements based upon C-bombs [13] is as follows.

If all MBSs would agree to implement a common set of behaviour rules, this set could be fairly small. In practice however, there are some reasons why such a 'minimum approach' will not work:

- The most obvious reason is that one cannot realistically expect all networks and software developers to implement one common strict set of rules. In different mail communities, different MBS conventions have already been used for a long time. Some of these conventions can be unacceptable for other communities to implement.

- MBSs can be built upon different underlying protocols. For instance, it is almost impossible to have a small set of rules that will prevent problems between any combination of MBSs, e.g. between an RFC 822-like MBS running over NJE and a P1 based MBS. More problems can be expected because header fields are crucial for the properly functioning of MBSs, and protocol gateways will not always map header fields bijectively.

- Not all MBSs are controlled by software developers or network operators. Any user can write a simple program that will have the functionality of an MBS.

Because the 'minimum approach' is not feasible, the bombs series follows the 'unilateral safety approach'. This means that any MBS that implements the complete set of rules should be safe from harm, regardless of what other 'dumb' MBSs it is interacting with.

This approach results in quite a large number of recommendations, of which not every single one is strictly necessary to prevent problems, but none of them will 'hurt' the functioning of an MBS.

From the previous paragraphs it follows that MBSs do not operate in a vacuum; they interact with other types of MBSs. As a result, the requirements in this document may sometimes look like an overkill when not seen in the light of the behaviour of other types of MBSs. To get an idea of the requirements for other MBSs, please refer to the H-bombs document [12] (which is the predecessor of the bombs series).

As for the programming overhead caused by the recommendations, there is at least one example of an echo server (Echoput) that implements all a-bombs rules in two pages of (perl) code.

In addition to the rules that protect against loops and explosions, there are also some rules reflecting common sense. For instance, if a user sends a message flagged 'urgent' to an echo server, he would expect not only his request message, but also the reply message to be handled with extra priority.

The rules for vacation servers are the same as for echo servers, but due to the lifetime attribute and a vacation server not normally

having a separate administrator, these servers have some additional/exceptional rules.

3. Implementation levels and protocols

Answering servers are normally implemented at UA level. If one wants to test connectivity at a lower level, a message can be sent to a 'nosuchuser' address, which will result in an MTA-generated non-delivery message or report.

To a user, it is often not known beforehand in which protocol world (RFC 822, X.400, others) an MBS is located. Also an MBS doesn't normally 'know' in which world a user lives. In order to come to a consistent echo server behaviour regardless of used protocols, this document describes recommendations for both RFC mail and X.400 echo servers. Note that a one hundred percent transparency cannot be reached (yet), because there exists no one-to-one mapping between all RFC mail and X.400 service elements.

For the reader's convenience, the rules for MBSs in different implementation levels and protocols are explicitly stated in the appropriate terminologies. The rules are labelled as follows:

For Internet mail:

#RFC#	Applies to RFC 822 on top of RFC 821 (SMTP) based MBSs
#1327#	Some the RFC 822 rules deal with non-standard headers as described in RFC 1327

For X.400:

#400#	Applies to X.400 (both 84 and 88) based MBSs
#84#	Applies to X.400(84) based MBSs
#88#	Applies to X.400(88) based MBSs
#P1#	Applies to P1 (MTS) based MBSs
#P2#	Applies to P2 (UA) based MBSs
#P3#	Applies to P3 (MTA) based MBSs

4. Rules

Depending on implementation level and protocol, answering servers follow, as a minimum, the requirements defined in RFC 822, RFC 821, RFC 1123, X.411, X.420, X.435 etc. For those requirements, the MBS must behave as an automated user or UA, depending on whether it is implemented at UA- or MTS-level, respectively. This chapter describes additional rules for answering servers in terms of RFC 821, RFC 822, P1, P3, and P2.

4.1. Input message restrictions

4.1.1. Don't reply to automatically forwarded messages

DISCUSSION: There is no need for a user to automatically forward his incoming messages to an echo server or a vacation server. Note that non-auto-forwarded messages can only be unambiguously identified in P2, Internet mail has no standard headers for this purpose. RFC 1327 gateways map this attribute to a new RFC 822 header "Auto-Forwarded:". In the presence of this header, RFC based MBSs can safely assume that the message was indeed auto-forwarded.

RULE: An auto-forwarded message is not valid as an input message. The result is the generation of an exception output message.

ORIGIN OF RULE: This document.

4.1.2. Don't reply to threads

DISCUSSION: It is very unlikely that a user will send a reply to another message as an input message to an answering server. Such a reply or follow-up should either have gone to the MBS administrator (due to the rules in this document) or to any other address that is not an answering server.

RULE: An exception output message is generated if the input message contains either of the following headers or attributes:

#RFC#	In-Reply-To:	
		References:
#P2#	In-Reply-To	
		crossReferences

ORIGIN OF RULE: This document.

APPLICABILITY: should.

4.1.3. Valid input message types

DISCUSSION #RFC#: An answering server is not to send automatic replies to (automatically generated) non-delivery messages, to avoid loops. In RFC mail, non-delivery messages can be recognised by the empty MAIL FROM: line.

RULE: Only the following types of input messages are valid as input messages. Any other type of input message (report, receipt notification) leads to the generation of an exception message.

#RFC# Any message that does not have an empty MAIL FROM: line.

#84#P1# UserMPDU
#84#P2# IM-UAPDU

#88#P1# Message
#88#P2# IPM

#400# P1.Probes are expected to be handled by the MTS and are thus not interpreted by the MBS.

4.2. Output messages

4.2.1. Relation to the input message

4.2.1.1. User can specify alternate output message recipient

DISCUSSION: The user may decide that the output message should be sent to another address than his own. This is especially useful when the user is an automated process, e.g. a connectivity checker, with a complex distributed configuration.

RULE: If the input message contains the following header or attribute, the output message is sent to that address. If this field contains more than one address, an output message is sent to at least the first address of this field. (Sending to the others is not recommended.)

#RFC#	Reply-To:
#84#P2#	replyToUsers
#88#P2#	reply-recipients

ORIGIN OF RULE: Common practice, RFC 821, RFC 822, RFC 1123, X.400.

APPLICABILITY: must.

4.2.1.2. Make output messages traceable

DISCUSSION: This rule allows the user to find know exactly to which message this output message belongs.

ORIGIN OF RULE: RFC 822, X.400, common practice, this document.

4.2.1.2.1. In reply to

RULE: The following header or attribute of the output message has the value:

#RFC#	In-Reply-To: : Message-ID of input message
#84#P2#	inReplyTo : IPMessageID of input message
#88#P2#	replied-to-IPM : this-IPM of input message

APPLICABILITY: must.

4.2.1.2.2. Subject

The following header or attribute of the output message has as value the string 'Re: ', concatenated with the subject of the input message.

#RFC#	Subject:
#P2#	subject

APPLICABILITY: should.

4.2.1.2.3. References

RULE: If the following header or attribute is used in the output message, it has the value:

#RFC#	References: : Message-ID of input message
#84#P2#	crossReferences : IPMessageID of input message
#88#P2#	related-IPMs : this-IPM of input message

APPLICABILITY: may.

4.2.1.2.4. Alternate recipient can trace originator of the input message

DISCUSSION: A user who receives mail from an MBS, without having ordered this information himself, has the right to know who was responsible for having messages sent to his mailbox. The semantics of both RFC 822 and X.400 header fields allow to specify that a message was sent from a certain address, but was authorised by someone else. This matches the semantics needed here. Another reason for using header fields for carrying this information is that the addresses will still be readable for the end-user after the message has crossed a protocol gateway.

RULE:

#RFC# If the output message is not sent to the originator of the input message, its From: field contains the addresses of the From: and the Sender: fields of the input message. In this case the Sender: field of the output message contains the address of the MBS administrator.

#P2# If the output message is not sent to the P2.originator of the input message, its P2.authorizingUsers field contains the addresses of the P2.originator and the P2.authorizingUsers of the input message.

ORIGIN OF RULE: This document, RFC 822, RFC 1327, X.400.

APPLICABILITY: shall.

4.2.1.4. Body contents

DISCUSSION: In order for the user to see what happened to his original input message on its way to the answering server (format, timing etc), the input message is reflected back to the user. Further info- and advertainment about the server can be included as well. See also 4.2.2.

ORIGIN OF RULE: Common practice, this document.

RULE: The input message (all headers and an optionally truncated part of the body) is included in the output message in an end user readable format, preferably as a MIME message body-part, an IPMS.ForwardedIPMessage bodypart, or in plain ASCII text.

APPLICABILITY: must.

4.2.1.5. Conservation

DISCUSSION: There are a number of headers or attributes, set by the originator of the input message, that are to be set to the same value in the output message. For instance, a user will expect a high priority request to be handled with high priority. The output message will in this case have the same priority. Note that an MBS can, as a local decision, choose to spool all requests in order to spread the MBS load. As long as the local processing of high priority request can be guaranteed to be no slower than that of normal requests, and the following rules for the output messages are followed, these local processing delays will be transparent for the MBS users.

4.2.1.5.1. Retain privacy requests

DISCUSSION: The server is to respect the originator's request for privacy.

RULE: The following headers or attributes have the same value in the output message as in the input message:

#1327#	Sensitivity:
#1327#	Importance:
#1327#	Priority:
#P2#	P2.sensitivity
#P2#	Importance
#P1#P3#	Priority

ORIGIN OF RULE: this document.

APPLICABILITY: must.

4.2.1.5.2. Answer in same type of content

DISCUSSION: To minimise the chance of UAs not being able to handle a certain message content type, the content type of the output message is the same as that of the input message.

RULE: The following headers or attributes have the same value in the output message as in the input message

#RFC#	MIME-Version:

#RFC#	Content-Transfer-Encoding:
#84#P1#P3#	ContentType

ORIGIN OF RULE: this document.

APPLICABILITY: should.

4.2.2. Restrictions

4.2.2.1. Don't ask for replies

DISCUSSION: If an MBS would request some form of reply or report for an output message, other MBSs might as a result automatically send a message, report or (non)delivery message back to the MBS, which is to be avoided at all cost, or to the MBS administrator, which is highly undesirable.

ORIGIN OF RULE: This document.

4.2.2.1.1. Don't give incentive to reply to output message

DISCUSSION: Replies to the output message should be avoided, especially because they might be generated automatically.

RULE: The following headers or attributes are not used in the output message:

#RFC#1327#	Reply-By:
#RFC#1327#	Expiry-Date:
#P2#	Recipient.replyRequest (defaults to FALSE)
#84#P2#	replyBy
#84#P2#	expiryDate
#88#P2#	reply-time
#88#P2#	Expiry Time
#88#P1#P3#	Proof-of-delivery-request (defaults to proof-of-delivery-not-requested)

APPLICABILITY: shall

4.2.2.1.2. Use of Reply-To functionality

DISCUSSION: It is redundant to explicitly attract replies to the output message to the MBS administrator, as the other rules in this document will ensure such behaviour. If an MBS decides to explicitly attract replies to the output message to a certain address, that address is not to be the server's address, but preferably the administrators. Since this rule contains three different applicability levels, it is subdivided into 3 rules.

A. Don't use Reply-To functionality

DISCUSSION: Other rules in this document will ensure that replies to the output message will automatically be sent to the right address (the administrator's).

RULE: The following headers or attributes are not used in the output message:

#RFC#	Reply-To:
#84#P2#	replyToUsers
#88#P2#	reply-recipients

ORIGIN OF RULE: This document.

APPLICABILITY: shall

B. Don't attract replies towards the server itself

DISCUSSION: If the MBS decides, despite rule A, to attract replies to a certain address, that address is not this (or any other) answering server's.

RULE: If the following field is used in the output message, it does not contain the address of the answering server.

#RFC#	Reply-To:
#84#P2#	replyToUsers
#88#P2#	reply-recipients

ORIGIN OF RULE: This document.

APPLICABILITY: must.

C. Attract replies towards the administrator

DISCUSSION: If the MBS decides, despite rule A, to attract replies to a certain address, that address is the MBS administrator's.

RULE: If the following field is used in the output message, it contains the address of the answering server's administrator.

#RFC#	Reply-To:
#84#P2#	replyToUsers
#88#P2#	reply-recipients

ORIGIN OF RULE: This document.

APPLICABILITY: should.

4.2.2.2. Avoid non deliverable output messages to cause loops

DISCUSSION: If the output message has an MTS-level originator with the address of the answering server itself, a loop can occur if the output message is undeliverable. Note that for X.400 answering servers, this rule affects a P1 attribute, but only when the output message is P2. For instance, consider a P1 distribution list that distributes another content type than P2, say Pc. Since Pc can be completely unstructured, changing the P1.originator would make it impossible to reply to the originator of the input message. Changing the P1.originator will also make sense for content types that have P2 like header fields, e.g. for P35 messages.

RULE: The following line or attribute of the output message has the value:

#RFC#	MAIL FROM: : address of the MBS administrator
#P2#	P1.originator : address of the MBS administrator

ORIGIN OF RULE: Common practice, this document.

APPLICABILITY: must.

4.2.2.3. Avoid replies to the output message to go back to the server

RULE: The following line or attribute of the output message has the value:

#RFC#	From: : address of the MBS administrator
#P2#	P2.originator : address of the MBS administrator

ORIGIN OF RULE: This document.

APPLICABILITY: must.

4.2.2.4. Avoid reports about the output message

DISCUSSION: We don't want anything automatically generated in reply to the output message, to avoid loops.

A. PerRececipientFlags

RULE: #84#P1#P3# Every PerRececipientFlag in the output message has the following bits set:

Report Request:	01
User Report Request:	00

(I.e. the Non-delivery Notification service will be prevented)

ORIGIN OF RULE: this document.

APPLICABILITY: must.

B. Don't request Reports or Notifications to the output message

RULE: The following attribute is empty in the output message:

#84#P2#	Recipient.reportRequest
#88#P2#	NotificationRequests

ORIGIN OF RULE: this document.

APPLICABILITY: must.

4.2.2.5. Extension Identifiers

DISCUSSION: There is at least one case where not all P1.ExtensionIdentifiers being different has caused a mailing loop. Although this was due to a software bug, there is no good reason for not using different P1.ExtensionIdentifiers.

RULE #P1#: All P1.ExtensionIdentifiers in the output message are distinct.

ORIGIN OF RULE: Common practice, common sense, this document.

APPLICABILITY: shall.

4.2.2.6. Body contents

DISCUSSION: In order for the user to see what happened to his original input message on its way to the answering server (format, timing etc), the input message is reflected back to the user. Further info- and advertainment about the server can be included as well. See also under 4.2.1.

ORIGIN OF RULE: Common practice, this document.

RULE: Additional information is included in separate bodyparts of the output message.

APPLICABILITY: may.

4.3. Logging

4.3.1. Logging for the administrator

DISCUSSION: This rule allows the MBS administrator to track down malicious behaviour.

RULE: The MBS logs the originator of the input message and all recipient(s) of the output/exception message(s).

ORIGIN OF RULE: this document.

APPLICABILITY: shall.

4.3.2. Log output message IDs

DISCUSSION: This will prevent all routing and MTS-redirection loops amongst MBSs. UA level MBSs, which create a new output message for each input message, will at least be safeguarded against mail storms from other MTS based MBSs.

RULE: The MBS logs the message ID of every input message and every output message. It generates an exception message if the same message ID is encountered in the input message more than once.

ORIGIN OF RULE: This document. Similar techniques are already being used in Netnews.

APPLICABILITY: should.

4.3.3. Vacation logging

DISCUSSION: Users of vacation servers don't normally want to use a server, but to reach another person. One output message stating that this person is on vacation will be enough.

RULE: Vacation servers at least log the originator of the input message. During the lifetime of an vacation server, only one output message per input message originator is generated.

ORIGIN OF RULE: This document. Similar techniques are already being used in Netnews.

APPLICABILITY: must.

4.3.4. Black list

DISCUSSION: Repliers are not to send output messages to addresses which are likely to be repliers themselves, to avoid loops.

RULE: Repliers keep a list of loop-suspicious addresses, containing at least the following values for the local address designator (localpart, Surname, CommonName):

```
autoanswer
echo
listserv
mailerdaemon
mirror
netserv
server
```

In this respect, also echo servers can be thought to have a limited lifetime, during which a normal output message (with an extra

bodypart containing a warning) will be sent to loop-suspicious addresses only once. This can be implemented by automatically adding the exact suspicious address to a negative access control list. Whenever this list is cleared, the replier can be thought to start a new lifetime.

The loop suspicious addresses are matched in any combination of upper and lower case.

ORIGIN OF RULE: Tradition, this document.

APPLICABILITY: shall.

4.4. Access permissions

DISCUSSION: The user is is to be informed whether and why he has not been granted access to the server.

ORIGIN OF RULE: Tradition, this document.

DISCUSSION #RFC#: Note that in this case the not granted access is to be reported from MTS level, i.e. by the MBS administrator, owner or operator - and not by the MBS itself.

RULE: #RFC# In case of an Access Permission violation an exception message is generated with the following text in the message body:

"Originator not allowed to send to this address"

APPLICABILITY: shall.

DISCUSSION #84#: Note that also here the not granted access is to be reported from MTS level, i.e. by the MBS administrator, owner or operator - and not by the MBS itself. This holds for both options:

RULE option 1: #84#: In case of an Access Permission violation a P1.DeliveryReportMPDU is generated with the following values:

ReasonCode: unableToTransfer(1)
DiagnosticCode:uaUnavailable(4)
SupplementaryInformation:
"Originator not allowed to send to this address"

APPLICABILITY: shall.

DISCUSSION: This option is preferred, but a P2 server may choose to respond more in line with RFC servers as follows:

RULE option 2: #84#P2# In case of an Access Permission violation an exception message is generated with the following text in the message body:

"Originator not allowed to send to this address"

APPLICABILITY: may.

5. Reference implementations

There are a number of MBS implementations that follow most of the recommendations listed in this document. They include the following, all operating at UA level:

Name	Protocols	Contact
Concord	RFC, X.400(84)	klarenberg@netconsult.ch
EAN echo server	X.400	martinez@fundesco.es
Echoput	RFC, MIME	klarenberg@netconsult.ch
PP echo server	X.400(84 and 88)	onions@xtel.co.uk

6. Acknowledgements

Thanks for ideas, comments, flames and corrections: Harald Alvestrand (SINTEF), Allan Cargille (XNREN), Urs Eppenberger (SWITCH), Paul Klarenberg (NetConsult AG), Ignacio Martinez (Fundesco), Juan Pizzorno (DFN), Eric Thomas (SUNET), Johan Vromans (Multihouse), Jan van der Weele (Du Pont).

7. Security considerations

Security issues are not discussed in this memo.

8. Bibliography

[1] Jonathan B. Postel, "Simple Mail Transfer Protocol", RFC 821, University of Southern California, August 1982

[2] Crocker, D., "Standard of the Format of ARPA Internet Text Messages", RFC 822, UDEL, August 1982.

[3] R. Braden, Editor, "Requirements for Internet Hosts -- Application and Support", RFC 1123, USC/Information Sciences Institute, October 1989.

[4] Kille, S., "Mapping between X.400(1988) / ISO 10021 and RFC 822", RFC 1327, UCL, May 1992.

[5] Kille, S., "X.400 1988 to 1984 downgrading", RFC 1328, UCL, May 1992

[6] N. Borenstein, N. Freed, MIME (Multipurpose Internet Mail Extensions), RFC 1341, June 1992

[7] J. Houttuin, "Concord functional specification", COSINE MHS server, Mail: cosine-mhs-server@nic.switch.ch, FTP: nic.switch.ch, Username: cosine , File: tools/operational/concord/xxxxxxxx

[8] J. Houttuin, Allan Cargille, "Requirements for concord echo servers and distribution lists", COSINE MHS server, Mail: cosine-mhs-server@nic.switch.ch, FTP: nic.switch.ch, Username: cosine, File: procedures/echo-server-reqs

[9] "list of surnames/usernames not to automatically reply to", RARE server, Mail: server@rare.nl, FTP: ftp.rare.nl, File: working-groups/wg-msg/div/dontreply

[10] CCITT Recommendations X.400 - X.430. Data Communication Networks: Message Handling Systems. CCITT Red Book, Vol. VIII - Fasc. VIII.7, Malaga-Torremolinos 1984

[11] CCITT Recommendations X.400 - X.420. Data Communication Networks: Message Handling Systems. CCITT Blue Book, Vol. VIII - Fasc. VIII.7, Melbourne 1988

[12] Houttuin, J., "H-bombs: Header Behaviour of MBSs", work in progress, November 1993.

[13] Houttuin, J., "C-bombs: Classification of Breeds of MBSs", work in progress, April 1994.

9. Abbreviations

ASCII	American Standard Code for Information Exchange
CCITT	Comite Consultatif International de Telegraphique et Telephonique
COSINE	Co-operation for OSI networking in Europe
EAN	MHS software (not an abbreviation)
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IPM	Inter-Personal Message
IPN	Inter-Personal Notification
MHS	Message Handling System
MBS	Mail based server
MTA	Message Transfer Agent
MTL	Message Transfer Layer
MTS	Message Transfer System
NJE	Network Job Entry
PP	MHS software (not an abbreviation)
RARE	Reseaux Associes pour la Recherche Europeenne
SMTP	simple mail transfer protocol
UA	User Agent

10. Author's Address

Jeroen Houttuin

RARE Secretariat
Singel 466-468
NL-1017 AW Amsterdam
Europe

Tel +31 20 6391131
Fax +31 20 6393289

RFC 822 houttuin@rare.nl
X.400 /S=houttuin/O=rare/PRMD=surf/ADMD=400net/C=nl/