M$^3$AAWG | Messaging Malware Mobile
Anti-Abuse Working Group

## Messaging, Malware and Mobile Anti-Abuse Working Group (M$^3$AAWG)

# M$^3$AAWG Recommendations for Configuring Human Readable Delivery Status Notifications (DSN)

**Updated March 2019 (May 2009)**

The reference URL for this document is www.m3aawg.org/ReadableDSN

**Table of Contents**

## Updated in this Version:

This paper has been updated to expand the text related to RFC 3463. Other minor changes were made for clarity or to simplify the text.

## I. Introduction

Email is used by a wide variety of people. The technical abilities of those users are equally diverse. Some users are quite adept at understanding how computer and email systems work. Others simply do not care to understand the inner workings of email and other related technologies; they just want it to work. It is abundantly clear that the latter represents most email users.

Simple Mail Transfer Protocol (SMTP) notification standards have been developed to ensure that servers and users are made aware of any delivery problems, whether temporary or permanent. These existing SMTP reply codes were designed to describe technical problems regarding a single message or addressee.

However, the encoded nature of SMTP reply messages often makes it difficult for end-users to understand why their email had a problem, and what corrective action can be taken. The resulting customer confusion and frustration can end up as extraneousness technical support calls to the operator or service provider.

In addition, concurrent with the rise of email abuse, there has been a significant need to report problems that pertain to behavior or content rather than just transmission errors. Network operators have stated Acceptable Use Policies (AUP) and Terms of Service (TOS) with publicly disclosed requirements and prohibitions. Legitimate and illegitimate mailers alike run aground of these stated AUP and TOS due to negative mailing practices, mailing architecture or prohibited content. When that happens, an automated notice is generated to inform the sender of the problem. In the case of abuse, the notifications have become a growing problem because current SMTP replies were developed to convey transmission issues and do not communicate the scope or duration of policy-related rejections. Users and network operators today are often left without a tangible reason for the rejection or a clear path toward resolution.

## II. SMTP Special Interest Group Disclaimer

The M$^3$AAWG SMTP Reply Special Interest Group (SIG) was established to define this problem, develop common terminology, and present a possible framework for expanding the existing rejection codes to communicate a more robust set of policy violations and technical failures. This document is the first such proposal. It should not be viewed as a formal statement of policy by the Messaging, Malware and Mobile Anti-Abuse Working Group or by any M$^3$AAWG member — not even the authors. It is merely a collection of ideas, presented as a basis for further discussion.

## III. Background

A Delivery Status Notification (DSN) message is created when an email message cannot be delivered. It is important to note DSN messages can also be sent to users when delivery is successful. However, it is beyond the scope of this document to cover all the nuances of DSN messages. To fully understand the capabilities of the DSN service extension please review RFC 3461[1].

RFC 3462[2] is the standard for formatting DSNs. In summary, the standard specifies that a DSN has three parts:

1. The first part should be human readable.
2. The second part of the message is machine parse-able.
3. Optionally, the last part can contain the actual body of the message.

Mail system managers are advised to review their configurations to see how closely they have implemented RFC 3462[2]. They should ensure DSNs generated from their systems have human readable text.

The SMTP reply codes defined in the current standards RFC 5321[3] and the less commonly implemented RFC 3463[4] address only the disposition of an individual message. They leave little room for statements of policy regarding either the message, the SMTP conversation, or the potential future SMTP conversations. Furthermore, RFC 3463[4] states these codes “are not intended for system specific diagnostics.” In the fifteen years since this RFC was published, enterprise cloud email services are now broadly adopted; these semantics need to evolve to match the new landscape.

These currently defined reply codes fall into three broad categories (excluding those not related to this issue):

- **2xx** the message has been accepted

- **4xx** the message was not accepted; the sender may try to deliver that message again later

- **5xx** the message was rejected; the sender must never retry that message

All varieties of mail system managers have attempted to reinterpret these replies to communicate more complex information. This situation has developed primarily, but not exclusively, regarding abuse concerns such as spam and other policy focused violations.

Any effort to overload existing codes with additional semantics is likely to have mixed results because it invites confusion, and the current state of SMTP reply code usage is no exception. Stories abound of SMTP senders unwittingly engaging in abusive behavior due to misunderstanding the intended – and sometimes obscure – meaning of an individually customized SMTP reply.

## IV. Potential for a Solution

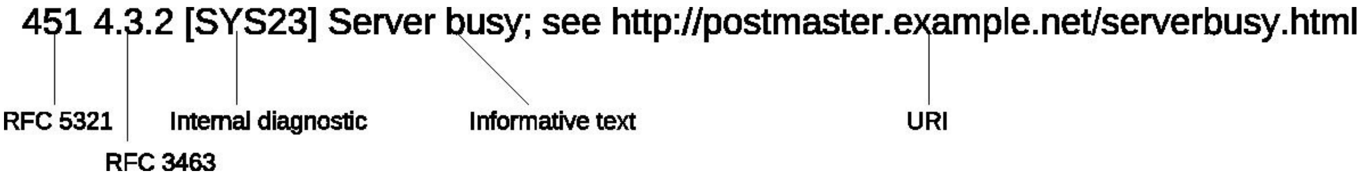
Encoded rejection notices often frustrate end-users and do little to clarify the problem. Average users often have difficulty understanding why a message delivery failure occurred, or what to do about it, because the rejection codes usually are obtuse. However, in most cases the underlying issue is correctly captured somewhere within the response. Yet, that one meaningful line of text can be buried within several other lines of coded information, and to the uninitiated, the notice reads like a cryptic computer language. In addition, network managers would also benefit from more verbose rejection notices when troubleshooting abuse problems.

As mail system managers, we should endeavor to improve this situation. Providing easy to understand messaging to email users is mutually beneficial to both the user and the service provider. One of the main benefits is lowering technical support costs.

Some practices already exist which could be borrowed or expanded upon. Admittedly configuring human digestible responses for all possible delivery failures might not be scalable. However, it is possible to analyze log files for common delivery failures and have human readable responses for the top five or ten delivery problems. Some ISPs include a URI in the text portion of their DSN that points to a page describing the relevant policies in more detail, and often includes a way for the email sender to request assistance. A URI was originally called a URL only now it is simply a unique naming "indicator" instead of always mapping to an internal location,

Many systems also include simple machine-readable strings that augment the standard three-digit SMTP reply and provide additional troubleshooting information, though the particulars of this information may not be public. Hopefully, M$^3$AAWG members support of the adoption of RFC 3463[4] — that is, leading by example — would also eventually result in adoption by non-members and thus facilitation the adoption of the IETF standard.

RFC 3463[4], "Enhanced Mail System Status Codes," expands the SMTP reply string format by adding a second numeric code. We suggest below what elements might be included in this string as an example of implementing this standard.



```
451 4.3.2 [SYS23] Server busy; see http://postmaster.example.net/serverbusy.html
```

RFC 3463[4] status-codes consist of three fields. Each field is separated by a dot "." character. The first field defines the class and uses nomenclature similar to RFC 5321[3] (2XX, 4XX and 5XX). The second field is the subject and the final field provides the detail.

In the example, above, the RFC 3463[4] component of the SMTP reply notice shows a 4.3.2 status code. The first field "4" indicates a temporary error condition. The second field, "3", tells you the status of the mail system. Finally, the "2" provides the detail of the mail system. In this case its status is not accepting messages.

Table 1 below describes the status codes at a high level:

**Table 1**

| | |
|---|---|
| X.0.0 | Other undefined status |
| X.1.X | Address status |
| X.2.X | Mailbox status |
| X.3.X | Mail system status |
| X.4.X | Network and routing status |
| X.5.X | Mail delivery protocol status |
| X.6.X | Message content or message media status |
| X.7.X | Security or policy status |

### A. Extending SMTP Codes (RFC 3463 and Related RFCs) with Accompanying Text

We encourage the use of existing codes defined in RFC 3463[4] and RFC 5248[5]. Some of the especially relevant existing codes are listed below:

- x.0.0 Other undefined status (rely on text and URI for more information).
- 5.1.1 Bad destination mailbox address (user does not exist).
- 5.1.6 Destination mailbox has moved; no forwarding address.
- x.3.0 Other or undefined mail system status (rely on text and URI for more information).
- x.3.2 System not accepting network messages.
- 4.4.4 Mail system congestion.
- x.5.3 Too many recipients.
- x.7.0 Other or undefined security status (rely on text and URI for more information)
- x.7.1 Delivery not authorized; message refused (for any policy violation) — RFC 3463[4] says "this is useful only as a permanent error," but it can easily be expanded to cover transient policy refusals as well.
- x.7.5 Cryptographic failure — can be used for DK/DKIM failures.
- 5.7.13 User account disabled — defined in RFC 5248[5], not quite the same meaning as 5.1.1 above. Some privacy policies may prohibit this differentiation.

Because the current RFCs only cover a small fraction of what mail servers issue for SMTP errors, many new reasons to use them have been created in the work arena. This is especially noticeable with abuse and antispam policies. For many of these, the extended SMTP code of 5.7.1, or 4.7.1 are used. If there is not a specific extended SMTP code for the anti-abuse policy being used, it is highly recommended that the code 5.7.1, or 4.7.1 for transient errors, be used until a more specific code becomes available. Further work is required to properly define new unique identifiers that are unambiguous and more expansive than 5.7.1 and 4.7.1.

The text portion after the extended SMTP should be composed of at least two parts:

- **Informative or Explanatory Text**
This text may vary widely, just as in RFCs 5321[3] and RFC 3463[4]. There will be no attempt here to standardize this portion, but the text should clearly explain whether the rejection is related to the message, the sender, or another characteristic. For example, "too many recipients" could become "maximum message recipients of XYZ exceeded, please send to fewer recipients".

  The key point is to be unambiguous about necessary actions for resolution. For example, this text should, where appropriate, identify the sending IP address, and when an IP-based block has been set against an .IP address, the text should identify that IP address.

- **URI for Additional Information**
To assist the SMTP sender, include a URI for additional information. This information may be as detailed or as general as the SMTP receiver feels is necessary, but M$^3$AAWG would encourage the inclusion of appropriate contact information for resolution of any issues, at a minimum.

  Any other additional information can be included in the text. This includes encoded information that may be useful only to the issuer of the text.

## V. Conclusion

Augmenting delivery status notifications with human readable text, and using SMTP reply codes in a typical manner to reflect behavioral or content issues associated with abuse, will both improve users' experience and avoid unnecessary technical support calls. At the same time, the improved communications would increase operational efficiencies for most network operators. However, because of the dynamic nature of the protocols that make up SMTP, it is recommended that network operators watch for updates to RFC 5248[5] and apply them whenever an extended SMTP code of 5.7.1 is being used.

This paper was produced as the first step in this process. It identifies the problem and provides a foundation to support a productive dialogue on improving SMTP reply codes.

## VI. References

1. RFC 3461, Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs), https://tools.ietf.org/html/rfc3461.

2. RFC 3462, The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages, https://tools.ietf.org/html/rfc3462.

3. RFC 5321, Simple Mail Transfer Protocol, https://tools.ietf.org/html/rfc5321.

4. RFC 3463, Enhanced Mail System Status Codes, https://tools.ietf.org/html/rfc3463.

5. RFC 5248, A Registry for SMTP Enhanced Mail System Status Codes, https://tools.ietf.org/html/rfc5248.

As with all documents that we publish, please check the M$^3$AAWG website (www.m3aawg.org) for updates.