The Email Marketer's Guide to Bounce Processing

Return Path

The Email Marketer's Guide to Bounce Processing

Author: Cherie Ansari

Bio: Team Lead, Deliverability Consulting

Cherie has been in the email deliverability business since 2004. As a former email marketer and a Return Path client, she understands first-hand what it takes to earn a good sender reputation. Today, she works diligently to reduce ISP blocks, complaints, spam traps, and data hygiene problems for her clients and has proudly achieved 90%+ inbox deliverability rates. Her portfolio of clients includes those in the social networking, retail, travel, insurance, affiliate, and educational industries. Cherie's in-depth knowledge has earned her the privilege to be an email deliverability expert guest speaker at the Direct Marketing Association Conference. Prior to working on email deliverability, Cherie focused her attention on Information Technology. Her technical training as a former Data Network Engineer has proved to be invaluable in helping resolve email authentication and infrastructure related issues. Cherie holds an M.S.B.A with a concentration in eCommerce from San Francisco State University.

Who Should Read This?

Beginner
Beginner content is intended for marketers just starting out or for those who just need a refresher.

Intermediate
Intermediate content is intended for marketers with some experience in the subject matter including strategies and tactics.

Advanced
Advanced content is for marketers who have an advanced level of understanding of email marketing and are looking for advanced strategies and tactics.

This e-book:

About Return Path

Return Path is the worldwide leader in email intelligence. We analyze more data about email than anyone else in the world and use that data to power products that ensure that only emails people want and expect reach the inbox. Our industry-leading email intelligence solutions utilize the world's most comprehensive set of data to maximize the performance and accountability of email, build trust across the entire email ecosystem and protect users from spam and other abuse. We help businesses build better relationships with their customers and improve their email ROI; and we help ISPs and other mailbox providers enhance network performance and drive customer retention. Information about Return Path can be found at: returnpath.com

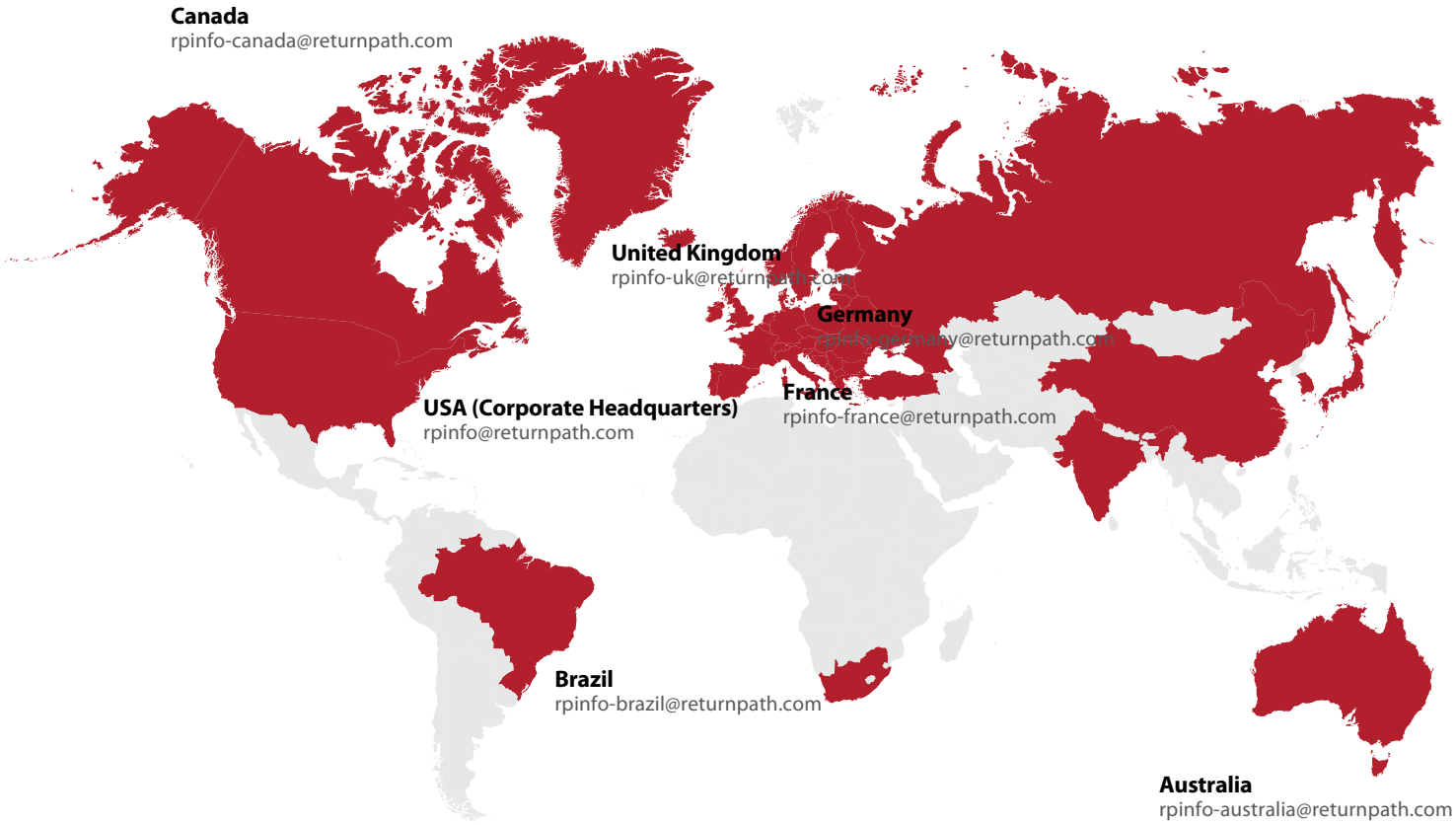


Table of Contents

Statement of Confidentiality & Legal Disclaimer

No part of this document may be disclosed, reproduced or distributed in any form or by any means — electronic, mechanical or otherwise — or stored in a database or retrieval system without the prior written consent of Return Path, Inc.

This document and any information provided herein is intended to be used as a general guideline. Return Path is not responsible for the application or implementation of this information within your business. Information and recommendations about industry best practices and ISP (Internet Service Provider) guidelines are subject to change. Return Path is not responsible for providing updates or amendments to this document unless specifically agreed upon within a work order.

What are Bounce Codes?

Bounce codes are automatic messages sent from a mail system to inform the sender of a deliverability problem. These messages are called non-delivery reports (NDRs). Bounce reports may be returned synchronously in the course of the SMTP conversation, or asynchronously via a separate email conversation.

Bounce codes are typically returned to the sender if there is no such person on the receiving end, or if the receiving server fills up. As a sender, you need to properly identify and act on bounces. Failure to handle bounces correctly can lead to serious reputation and deliverability problems.

What is the SMTP Conversation?

When you send an email, a conversation occurs between the sending and receiving servers. Sending servers are Mail Transfer Agents (MTAs), such as Sendmail or Postfix. Receiving servers are those used by the Internet Service Providers (ISPs).

The most widely used protocol — or, system of rules and formats for exchanging messages — used for sending and receiving emails is the Simple Mail Transfer Protocol (SMTP). So, this conversation between servers is often called the SMTP conversation.

Table 1.0 below shows an example of a typical SMTP conversation. The conversation happening is between ABC and Hotmail if ABC wanted to send mail to joe@hotmail.com.

Table 1.0 – SMTP Conversation

STEP	SERVER	CONVERSATION
1	ABC	Hello
2	Hotmail	Hello. I'm not too busy to talk.
3	ABC	This is abc.com
4	Hotmail	Ah, I know you. Because ABC is a reputable sender, I'll talk to you. (I won't block you.)
5	ABC	I want to send an email from customerservice@abc.com.
6	Hotmail	Ok, I'll accept an email from customerservice@abc.com.
7	ABC	I have an email for joe@hotmail.com.
8	Hotmail	Hmm, let me check. Do I have a joe@hotmail.com account? Yes, I do. Okay, send the email.
9	ABC	Here it comes.
10	Hotmail	Okay, I got it.
11	ABC	Thanks. I'll talk to you later.
12	Hotmail	Bye

In the SMTP conversation above, ABC's MTA talked to Hotmail's MTA. Hotmail's MTA decided that Joe was, in fact, a Hotmail user. Obviously, in this case, no bounce message needed to be sent.

Differences Between Synchronous and Asynchronous Bounces?

As mentioned above, bounce reports may be returned synchronously in the course of the SMTP conversation, or asynchronously via a separate email conversation. Though most mailbox providers send synchronous bounces, it is important to know why a receiver would send an asynchronous bounce — and where that bounce would be stored.

An analogy may help explain the difference between synchronous and asynchronous bounces.

Analogy 1: Synchronous Bounce

Let's say company ABC is an organic farming company that delivers produce to local residents. While signing up for the service, Joe accidentally adds his old address, 10 California Street, San Francisco, as his current address.

When ABC drives to 10 California Street, Mary answers the door. The driver hands her the package and Mary notices it's for Joe. She tells this to the driver who then logs in ABC's delivery system that the package was not delivered.

This is an example of a synchronous bounce: Mary noted the non-delivery while still in the driver's presence.

Analogy 2: Asynchronous Bounce

Continuing with the above scenario, let's say that Mary answers the door but does not notice the package is for Joe. The driver leaves and logs in ABC's system that he delivered the package.

When Mary realizes the mistake, she ships the package back to ABC. Later, ABC checks their mailbox and discovers the package returned. They log it as such.

This is an example of an asynchronous bounce: The rejection occurred after the driver left 10 California Street.

Email Scenario 1: Synchronous Bounce

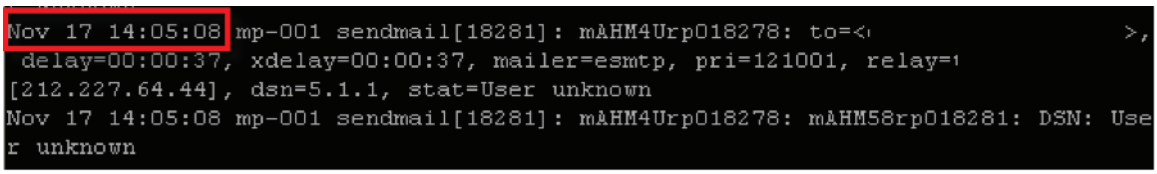
Using the analogies and the SMTP conversation example above, let's examine the difference between a synchronous and asynchronous bounces in terms of email.

We know that synchronous bounces occur during the SMTP conversation.

So, let's say that in step number 8 in the SMTP conversation example above, Outlook.com checks for Joe's email, and discovers it does not exist. In this case, Outlook.com does not let the email through. It also sends ABC an "account closed" bounce message, which ABC stores in their log file. The SMTP conversation is now closed.

Synchronous Bounce Example

Below, find an example of a synchronous bounce found in a Sendmail log. This bounce is stored in the /var/log directory under the maillog file. Notice that the log file records the rejected date and time, along with the bounce reason.



Email Scenario 2: Asynchronous Bounce

We know asynchronous bounces occur after the SMTP conversation.

So, let's say, continuing with the above example, Hotmail accepts the request from ABC without checking to see if Joe's account still exists. ABC marks the email as delivered.

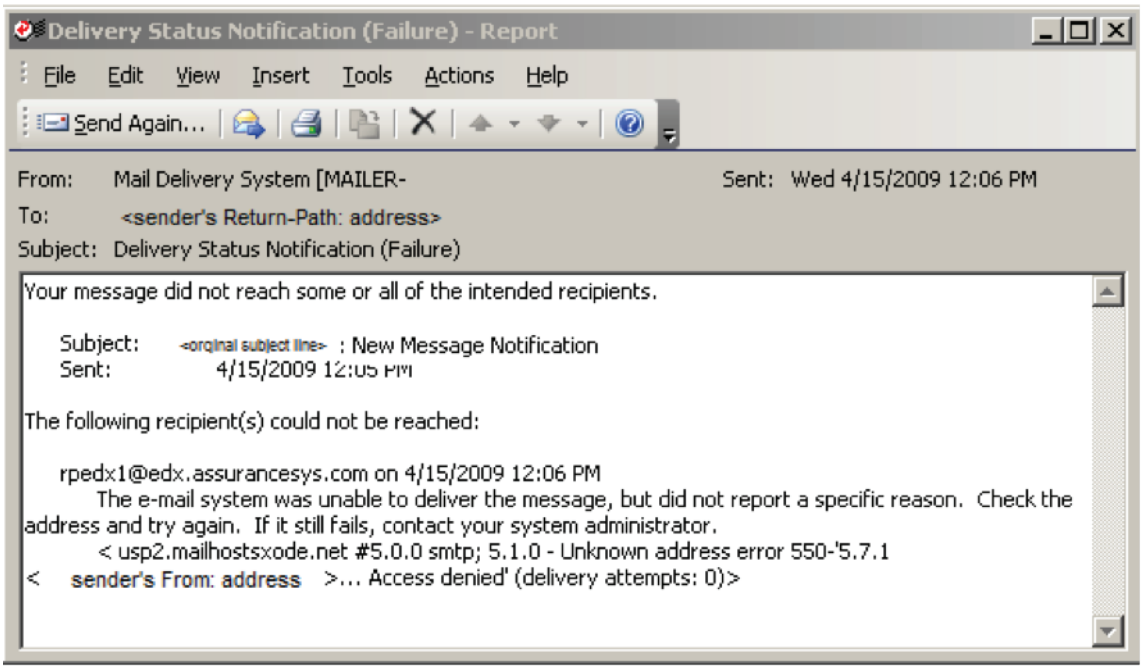
Later, when Hotmail tries to send the email, the account is closed. So, Hotmail sends a bounce message to ABC's envelope sender that the account doesn't exist. (The envelope sender is the email address listed in the Return-Path: email header.)

Because these bounces can trickle in within minutes to days later, ABC needs to check their log files to make sure they are seeing the most up-to-date bounces.

NOTE: Hotmail does not send asynchronous bounces.

Asynchronous Bounce Example

Below, find an example of an asynchronous bounce message. Notice that it's in the form of an email, not a log entry. Some MTA applications will parse this information and record it in the log file. Check your MTA vendor to see how they handle asynchronous bounces.



Section Takeaways:

- Most ISPs use the synchronous bounce approach.
- Synchronous bounces occur during the SMTP conversation. Make sure to check MTA log files for bounce reasons.
- Asynchronous bounces occur after the initial SMTP conversation. Although your MTA log file may show that your email was delivered, make sure you check the email account listed in your Return-Path: email header for asynchronous bounces.

Types of Bounces

Soft Bounces

A soft bounce occurs when an email is sent to an active email address, but is turned away. Often, the problem temporary: the server is down or the recipient's mailbox is over quota.

A bounce code may be displayed as numeric values consisting of three digit numbers. Typically, soft bounce codes can be identified with a 4xx SMTP reply, such as 421 and/or 4.2.1.

NOTE: SMTP reply codes are also known as SMTP error codes, response codes, or status codes.

Table 2.0 – Soft Bounce Examples

SOFT BOUNCE EXAMPLES
Blocked (may appear as 4xx or 5xx error)
Connection Refused
Connection Timed Out
Mail Server Down
Mailbox Full
Message Temporarily Deferred
Network Issues
System Disk Shortage
Temporarily Deferred

Hard Bounces

A hard bounce can occur when an email is sent to an address that was closed or does not exist. This is a permanent failure. Typically, hard bounces include a 5xx series code, such as 551 and/or 5.5.1. Along with the code, you should see a bounce reason.

Table 3.0 – Hard Bounce Examples

SUPPRESS THE EMAIL ADDRESSES FOUND IN THESE HARD BOUNCES FROM FUTURE MAILINGS
Account Closed: account inactivated, archived, closed or expired
Invalid Domain: domain does not exist, domain invalid, hostname invalid or host unknown
Unknown User: addressee unknown, unknown user, user does not exist, unknown or illegal alias, illegal user, no such user on system, no user specified, recipient's address is invalid, address rejected, invalid recipient, not our customer

What to Do about Bounces

When to Remove Hard Bounced Emails

Remove any emails associated with permanent 5xx errors specifying: *account closed, invalid domain, or unknown user.*

Using the examples listed in Table 3.0, audit your bounce logs to identify any hard bounces. Unsubscribe email addresses found in these selective hard bounces after one to two bounces.

When to Retry Soft Bounced Emails

In general, retry messages that bounce with a 4xx SMTP error. These errors are usually temporary; the receiver may be able to accept the message at a later time.

Depending on the number of retry messages you have in your retry queue and how much of a message backlog you're willing to manage, retry a message as many times as you'd like.

Schedule your initial retry for 2-4 hours after the first soft bounce and then employ a backoff retry time strategy that will continue retrying the message for 24–48 hours. (Backoff is the process of increasing the length of time between retries — typically, by double — every time you attempt to deliver it.)

It is unlikely that a major ISP would allow a system or network issue to go undetected or unresolved for longer than 24–48 hours. However, it may take an email user more time to realize that there is a problem with their account such as their mailbox being over quota or suspended.

When *Not* to Retry Soft Bounced Emails

There are some cases when senders should not retry messages with 4xx errors.

For instance, receiving multiple inbox full messages for an email address may indicate that the ISP will soon decommission it. Because these addresses could start hard bouncing or be turned into recycled traps, consider setting a threshold for these bounces to be removed.

Typically, a soft bounce limit should be four soft bounces in 30 days. However, if you send email to subscribers every day, set a threshold to give the subscriber time to fix what may be a temporary problem. Unless you send only periodically — say, once-a-month — remove an address from your list once you receive a fourth soft bounce notification.

Another reason to not retry soft bounced emails is due to transient policy blocks. For more, see the Exceptions section below.

Exception: Policy-Related Blocks

Due to variations in the ways that ISPs implement response codes, some 5xx bounces are not permanent failures, and some 4xx bounces will not automatically resolve on their own.

For instance, ISPs can issue policy-related blocks per host or per recipient. These may be removed once the ISP determines that the sender has fixed the issues causing the block.

The examples below are the most common types of policy blocks. In these cases, the recipient's email address should not be removed from the sender's list. Also, senders should not retry these messages until the policy block at the ISP has been removed.

Table 4.0 – Policy Blocks/Bounces

EXAMPLES OF POLICY BLOCKS/BOUNCES
Access denied: in queue too long
Blacklist
Block
Blocks related to spam-like characteristics or IP/domain reputation problems. Search for “spam” or “abuse” in your bounce logs.
Connection/Throttle problems
Mailbox unavailable

Policy-Related Block Examples

AOL

An example of a 421 SMTP error from AOL:

421 DYN:TI block

This is a temporary block caused by high complaints or low IP reputation.

Hotmail

An example of a 421 error from Hotmail:

Fri Sep 5 08:39:41 2008 Info: Delayed: DCID 1622390592 MID 517359227 to RID 0 - 4.3.2 - Not accepting messages at this time (‘421’, [‘RP-001 The mail server IP connecting to Windows Live Hotmail server has exceeded the rate limit allowed. Reason for rate limitation is related to IP/domain reputation problems. If you are not an email/network admin please contact your E-mail/Internet Service Provider for help. Email/network admins, please visit http://postmaster.live.com for email delivery information and support’]) []

This error is due to rate limiting, and is related to the connection and/or throughput rate the sender has in place for the ISP.

Most ISPs limit connection and throughput rates. The allowed rate may vary with the sender’s reputation. These rates can usually be adjusted according to domain or destination IP by changing configuration settings on the sending MTA.

Blacklist

Examples of blacklisting/policy blocks:

Service unavailable; Client host blocked using 88.blacklist.zap; Mail From IP Banned To request removal from this list please forward this message…

5.7.1, Access denied. IP on internal blacklist.

To help determine a sender’s reputation, ISPs reference various blacklists. If a sender’s IP is present on a blacklist, they typically block it until it is removed. To figure out more information about the blacklist, including how to apply for removal, review the status text.

Section Takeaways

- Remove recipients from your list only when you receive a valid hard bounce (5xx), i.e. unknown users.
- Verify that hard bounces are permanent and not policy blocks.
- Do not retry email addresses that are blocked for policy reasons until the cause is determined and the block is removed.
- Some MTAs and email management software packages are more flexible than others in the ways they handle bounces. Talk to your system administrator or vendor about what bounce configuration options are available for your infrastructure.

How to Read Bounce Codes

SMTP reply codes contain three numbers with each digit having special significance.

The SMTP reply codes (5xx) are referenced in RFC 5321 (originally RFC 2821). Due to limitations in the original codes, extended bounce codes (5.x.x) were developed and referenced in RFC 3463.

The following sections originated from RFC 5321 or the TCP/IP Guide at http://www.tcpipguide.com/free/t_SMTPRepliesandReplyCodes-2.htm.

First Reply Code: Digit X

The first digit denotes whether the response is good, bad, or incomplete.

An unsophisticated SMTP client, or one that receives an unexpected code, will be able to determine its next action (proceed as planned, redo, retrench, etc.) by examining this first digit.

Table 5.0 – SMTP Reply Code Format: First Digit Interpretation

REPLY CODE FORMAT	MEANING	DESCRIPTION
1yz	Positive Preliminary Reply	An initial response indicating that the command has been accepted and in process. The SMTP sender should expect another reply before a new command may be sent. Though this first digit type is formally defined in the SMTP specification for completeness, it is not currently used by any of the SMTP commands. (That is to say, there are no SMTP reply codes between 100 and 199.)
2yz	Positive Completion Reply	The command has been successfully processed and completed.
3yz	Positive Intermediate Reply	The command was accepted, but processing has been delayed, pending receipt of additional information. This type of reply is often made is after receipt of a DATA command to prompt the SMTP sender to then send the actual email message.
4yz	Transient Negative Completion Reply	The command was not accepted and no action was taken, but the error is temporary and the command may be tried again. This is used for errors that may be a result of temporary glitches or conditions that may change.
5yz	Permanent Negative Completion Reply	The command was not accepted and no action was taken. Trying the same command again is likely to result in another error. An example would be sending an invalid command.

Second Reply Code: Digit Y

The middle digit categorizes messages into functional groups.

An SMTP client can discover approximately what kind of error occurred (mail system error, command syntax error, etc.) by examining the second digit.

Table 6.0: Reply Code Format: Second Digit Interpretation

REPLY CODE FORMAT	MEANING	DESCRIPTION
x0z	Syntax	These replies refer to syntax errors, syntactically-correct commands that do not fit any functional category, and unimplemented or superfluous commands
x1z	Information	Replies to requests for information, such as status requests
x2z	Connections	Replies related to the connection between the SMTP sender and SMTP receiver
x3z	Unspecified	Not defined
x4z	Unspecified	Not defined
x5z	Mail System	Replies related to the SMTP mail service itself

Second Reply Code: Digit Z

This digit presents the finest gradation of information by indicating a specific type of message within each of the groups described by the second digit.

This digit allows each functional group to have 10 different reply codes for each reply type given by the first code digit.

Table 7.0: Reply codes in Numeric Order

REPLY CODE	REASON
211	system status or system help reply
214	help message (information on how to use the receiver or the meaning of a particular non-standard command; this reply is useful only to the human user)
220	<domain> service ready
221	<domain> service closing transmission channel
250	requested mail action okay, completed
251	user not local; will forward to <forward-path>
252	cannot VRFY user, but will accept message and attempt delivery
354	start mail input; end with <CRLF>.<CRLF>
421	<domain> service not available, closing transmission channel (this may be a reply to any command if the service knows it must shut down)
450	requested mail action not taken: mailbox unavailable (e.g., mailbox busy or temporarily blocked for policy reasons)
451	requested action aborted: local error in processing
452	requested action not taken: insufficient system storage
455	server unable to accommodate parameters
500	syntax error, command unrecognized (this may include errors such as an overlong command line)
501	syntax error in parameters or arguments
502	command not implemented
503	bad sequence of commands
504	command parameter not implemented
550	requested action not taken: mailbox unavailable (e.g., mailbox not found, no access, or command rejected for policy reasons)
551	user not local; please try <forward-path> (See Section 3.4)
552	requested mail action aborted: exceeded storage allocation
553	requested action not taken: mailbox name not allowed (e.g., mailbox syntax incorrect)
554	transaction failed (or, in the case of a connection-opening response, “no SMTP service here”)
555	MAIL FROM/RCPT TO parameters not recognized or not implemented

Enhanced Mail System Status Codes (RFC 3463)

When the ENHANCED STATUS CODES SMTP extension is enabled, the SMTP receiver issues supplemental reply codes in response to each command. These enhanced codes provide more information about the results of operations, especially errors.

How to Read Enhanced Mail System Status Codes (RFC 3463)

Enhanced Mail System Status Codes also use three digits, but these digits are separated by periods.

The first digit reflects the class status code, which classifies the delivery attempt. The second digit reflects the subject status code, which includes the source of the delivery anomaly. The third digit reflects the detail status code, which provides the precise error condition.

The explanation for the detail sub-code is dependent upon the subject sub-code. Table 8.0 illustrates this below.

Table 8.0: Subject and Detail Sub-Code (Second and Third Digits) Relationship

SUB-CODE	DEFINITION
Other or Undefined	
X.0.X	no additional subject information available
X.0.0	other undefined status is the only undefined error code; other identified status should be used for all errors for which only the class of the error is known
Addressing	
X.1.X	address status reports on the originator or destination address; it may include address syntax or validity
X.1.0	other address status
X.1.1	bad destination mailbox address
X.1.2	bad destination system address
X.1.3	bad destination mailbox address syntax
X.1.4	destination mailbox address ambiguous
X.1.5	destination mailbox address valid
X.1.6	mailbox has moved
X.1.7	bad sender's mailbox address syntax
X.1.8	bad sender's system address
Mailbox	
X.2.X	general mailbox issues
X.2.0	other or undefined mailbox status
X.2.1	mailbox disabled, not accepting messages
X.2.2	mailbox full
X.2.3	message length exceeds administrative limit
X.2.4	mailing list expansion problem
Mail System	
X.3.X	general destination system issues
X.3.0	other or undefined mail system status
X.3.1	mail system full
X.3.2	system not accepting network messages

X.3.3	system not capable of selected features
X.3.4	message too big for system
Network and Routing	
X.4.X	networking or routing codes that report status about the delivery system itself; these system components include any necessary infrastructure such as directory and routing services
X.4.0	other or undefined network or routing status
X.4.1	no answer from host
X.4.2	bad connection
X.4.3	routing server failure
X.4.4	unable to route
X.4.5	network congestion
X.4.6	routing loop detected
X.4.7	delivery time expired
Mail Delivery Protocol	
X.5.X	failures involving the message delivery protocol—including the full range of problems resulting from implementation errors or unreliable connections
X.5.0	other or undefined protocol status
X.5.1	invalid command
X.5.2	syntax error
X.5.3	too many recipients
X.5.4	invalid command arguments
X.5.5	wrong protocol version
Message Content or Media	
X.6.X	failures involving the content of the message including translation, transcoding, or otherwise unsupported message media
X.6.0	other or undefined media error
X.6.1	media not supported
X.6.2	conversion required and prohibited
X.6.3	conversion required but not supported
X.6.4	conversion with loss performed
X.6.5	conversion failed
Security or Policy	
X.7.X	failures involving policies such as per-recipient or per-host filtering and cryptographic operations; because security and policy status issues are assumed to be under the control of either or both the sender and recipient, both the sender and recipient must permit the exchange of messages and arrange the exchange of necessary keys and certificates for cryptographic operations
X.7.0	other or undefined security status
X.7.1	delivery not authorized, message refused
X.7.2	mailing list expansion prohibited
X.7.3	security conversion required but not possible
X.7.4	security features not supported
X.7.5	cryptographic failure
X.7.6	cryptographic algorithm not supported
X.7.7	message integrity failure

Why Bounce Messages Are Confusing

ISPs continue to evolve the set of bounce codes in use as email abusers come up with new ways to evade their safeguards.

Some ISPs only return a basic SMTP (4xx), enhanced mail system status code (4.x.x), or both. The status text for any given return code is usually different for each ISP and can vary from message to message for the same ISP.

For instance, if an AOL user no longer has an email address, AOL returns the 500 error status text as MAILBOX NOT FOUND. However, if the user has never logged into their mailbox at AOL, they return the status text for a 500 error as: "We would love to have gotten this email to recipient@aim.com. But, your recipient never logged onto their free AIM Mail account … ."

The differences in the ways ISPs return status text can be significant or not, depending on how you process each return code or status. Some MTAs may allow the administrator to process individual return codes differently, while others may not.

Table 9.0 – Examples of Confusing Bounce Messages

ISP	Bounce Reason	Why It's Confusing
Bluetie	421 4.7.0 mx024.roc2.bluetie.com Error: too many errors	bounce reason is unclear
Comcast	BLY004	doesn't use standard SMTP bounce codes
Verizon	550 4.2.1 'Mailbox Temporarily Unavailable'	both permanent and temporary bounce codes are included
Yahoo!	yahoo.com 554 delivery error: dd This account has been temporarily suspended. Please try again later.	listed as a permanent failure (554), but is really a temporary problem

Section Takeaways

- The format for the original SMTP reply code displays three digits (xxx). Each digit has a specific meaning, which is shown in Tables 5.0–8.0.
- Hard bounces can easily be identified because they start with a 5xx or 5.x.x reply code.
- Soft bounces start with 4xx or 4.x.x.
- The enhanced version (x.x.x.) was introduced to provide greater details about the bounce.
- The MTA log files may show the traditional SMTP reply codes (5xx) and/or the enhanced reply code (5.x.x).
- Interpreting the bounce messages can be quite confusing and frustrating because the ISPs can report anything they want to and not follow the standard recommendations.

Bounce Message Troubleshooting

Deciphering bounce messages can be confusing and frustrating. Use the URLs below to give you background information about the ISPs' bounce process and/or the bounce code explanation.

Table 10.0 – Helpful ISP Hyperlinks

AOL
http://postmaster.aol.com/Postmaster.Errors.php
ATT (and Bellsouth)
http://www.att.com/esupport/postmaster/email-errors/
Bluetie
http://postmaster.bluetie.com/subcontent/smtpCodes.php
Comcast
http://postmaster.comcast.net/mail-error-codes.html
Cox
http://postmaster.cox.net/confluence/display/postmaster/Error+Codes
http://getsatisfaction.com/deliverability/tags/bounce_codes
Facebook
http://postmaster.facebook.com/response_codes
Gmail
http://www.google.com/support/appsecurity/bin/answer.py?hl=en&answer=134416
Road Runner
http://postmaster.rr.com/rejected_connections
http://postmaster.rr.com/error_messages
Windows Live Hotmail
SMTP Error Codes http://mail.live.com/mail/troubleshooting.aspx
Yahoo
http://help.yahoo.com/l/us/yahoo/mail/postmaster/errors/;_ylt=AIndj61uSAyZH806UrDnRWVvMiV4
http://help.yahoo.com/l/us/yahoo/mail/postmaster/basics/postmaster-01.html;_ylt=AmFFAdxRv4haeus4UGAjdQEIJHdG
Also, try entering the bounce code in the search field.

Frequent Types of ISP Bounces

The table below shows the most frequent types of ISP bounces. Use this information to help you decipher the reason for the bounce, and the action to take next.

Table 11.0 – Top ISP Bounces

SMTP/ Extended Return Code	Domain	Status Text	Recommended Action
550	aol.com	MAILBOX NOT FOUND	hard bounce; suppress associated email address
550	aol.com	We would love to have gotten this email to recipient@aim.com. But, your recipient never logged onto their free AIM Mail account. Please contact them and let them know that they're missing out on all the super features offered by AIM Mail.	hard bounce; suppress associated email address
554	aol.com	HVU:B1 http://postmaster.info.aol.com/errors/554hvub1.html TRANSACTION FAILED	policy block; resolve complaint problem, then retry; do not unsubscribe.
5.1.1	gmail.com	5.1.1 The email account that you tried to reach does not exist. Please try double-checking the recipient's email address for typos or unnecessary spaces. Learn more at http://mail.google.com/support/bin/answer.py?answer=6596	hard bounce; suppress associated email address
5.2.2	gmail.com	5.2.2 The email account that you tried to reach is over quota. Please direct the recipient to http://mail.google.com/support/bin/answer.py?answer=6558	policy block; retry
550	hotmail.com	Requested action not taken: mailbox unavailable	treat as a soft bounce; the account was deactivated because the user hasn't logged into his/her account for more than 10 days; however, the address is still reserved for 365 days
535	msn.com	Virtual MTA invite does not exist	client MTA error; fix configuration and retry

421 451	yahoo.com	Message temporarily deferred	policy block; resolve complaint problem, then retry; do not unsubscribe
5.1.1	yahoo.com	VS10-RT Possible forgery or deactivated due to abuse (#5.1.1)	investigate spoof or infrastructure-related problem, then retry; do not unsubscribe
553	yahoo.com	Mail from <IP> not allowed	policy block; retry
554	yahoo.com	delivery error: dd Sorry your message to cannot be delivered. This account has been disabled or discontinued.	hard bounce; suppress associated email address
554	yahoo.com	delivery error: dd This account has been temporarily suspended. Please try again later.	retry
554	yahoo.com	delivery error: dd This user doesn't have a yahoo.com account	hard bounce; suppress associated email address

Manual Telnet SMTP Connection

Sometimes your log file may cut off part of the bounce message due to character size limitations. If this happens, increase the field size for the bounce reason or connect with your sending MTA to the ISP to obtain the entire bounce message. To do so, you must have a manual telnet SMTP connection. See Appendix A for instructions.

Delivery Log Analysis

Some MTAs only provide log files with no reports. This makes it difficult to see the most frequent ISP failures by hard and soft bounce. If you don't have an internal reporting tool, contact Return Path to generate a report for you that includes the following:

- Reports of subscriber domain distribution
- Reports of delivery performance at ISPs
- Identification of non-delivery (bounce) reasons for at ISPs
- Identification of ISP messages that indicate blocking or filtering
- Identification of unknown user rates to determine if they're a contributor to blocking or filtering
- Identification of whether Inbox Monitor missing seeds are a result of delivery issues at ISPs

Section Takeaways

- If you need additional support: use Table 10.0 to identify the ISP bounce code explanation or use Table 11.0 for recommended action items of the top ISP bounces.
- Need an aggregate report of your log files? Return Path can generate a delivery log analysis for you.
- Need a customized solution? Contact Return Path.

Appendix A: Manual Telnet SMTP Connection Test

It is possible to perform a manual SMTP connection test from the system that the client uses to send mail. This can be a good way to see the raw SMTP error message for an IP address block by an ISP, or find an issue with a specific email address.

An example SMTP telnet session is shown below. This session was performed in a Linux terminal window by connecting to port 25 on the destination server.

```
[dbrooks@datools dladb]$ telnet smtp.returnpath.net 25
Trying 216.183.97.124...
Connected to smtp.returnpath.net (216.183.97.124).
Escape character is '^]'.
220 smtp.returnpath.net ESMTP Postfix
helo bobo.net
250 smtp.returnpath.net
mail from: <someguy@bobo.net>
250 2.1.0 Ok
rcpt to: <dbrooks@returnpath.net>
250 2.1.5 Ok
rcpt to: <anotherguy@dumbdomain.net>
554 5.7.1 <anotherguy@dumbdomain.net>: Relay access denied
data
354 End data with <CR><LF>.<CR><LF>
test
.
250 2.0.0 Ok: queued as 6C64A7405C
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

The sender issues the telnet, EHLO, MAIL FROM, RCPT TO, and QUIT commands. The lines that begin with 220, 250, 354 and 221 are the destination email server responses that indicate success.

NOTE: The line that says “554 5.7.1 <anotherguy@dumbdomain.net>: Relay access denied” is a hard bounce due to the invalid domain name in the recipient address.

Manual SMTP Telnet Test from a Windows PC

Before you start the Telnet session, you must have the full SMTP email address of the destination user to whom you want to send this test message. This destination email address must be in this format: user@site.domain.com.

You must also have the fully qualified domain name (FQDN) or the IP address of the server running the SMTP services (for example, 10.120.159.1). If you do not have this information, find it by using nslookup.exe to find the DNS record.

Make sure that SMTP has started on the server that runs the SMTP service. To test if SMTP has started, run the basic tests listed below and verify that you receive the 220 response from the remote server. This also verifies that SMTP is running.

Basic Testing

Follow these steps to make sure that the host computer and the remote SMTP server can communicate.

If you receive the error message – 500 command not recognized – after you type any one of the following commands, the SMTP server does not recognize it because of a syntax error or an erroneous command. If this happens, check the command and type it again or verify that you are communicating directly to an SMTP server.

NOTE: Telnet does not permit you to use the Backspace key. If you make a mistake when you type a command, press Enter then start a new command.

How to Test by Running Telnet from the Command Line

1. Click Start
2. Click Run
3. Type cmd in the Open box
4. Click OK
5. Start a Telnet session by using the Telnet command in the following format: telnet smtp.servername. portnumber (for example, smtp.returnpath.net 25)

NOTE: Press Enter after each line.

NOTE: You can replace servername with the IP address or the FQDN of the SMTP server to which you want to connect.

6. Receive a response from the SMTP server that is similar to the following: 220 smtp.returnpath.net ESMTP Postfix.

NOTE: There are different versions of SMTP servers, and you may receive different responses from the receiving server. It is most important that you receive the 220 response with the FQDN of the server and the version of SMTP.

7. Start communication by typing the following command: EHLO test.com

NOTE: You can use the HELO command, but EHLO is a verb that exists in the Extended SMTP verb set that is supported in most current implementations of SMTP.

8. If the command is successful, you receive the following response: 250 OK
9. Type the following command to tell the receiving SMTP server who the message is from: MAIL FROM: admin@test.com. Make sure this is a valid email address.

NOTE: Some SMTP mail systems filter messages based on the MAIL FROM: address and may not permit certain IP addresses to connect or may not permit the IP address to send e-mail to the SMTP mail system if the connecting IP address does not match the domain where the SMTP mail system resides. In this example, that domain is test.com.

10. Receive the following response from the SMTP server: 250 OK - MAIL FROM admin@test.com.
11. Type the following command to tell the receiving SMTP server whom the message is to: RCPT TO: user@domain.com. Use a valid recipient SMTP address.
12. Receive the following response: 250 OK - recipient user@domain.com.
13. Type the following command to tell the SMTP server that you are ready to send data: DATA.
14. Receive the following response: 354 Send data
15. End with CRLF.CRLF
16. Type the following command to add a subject line: Subject: test message.
17. Press Enter two times (you will not receive a response from this command).

NOTE: The two ENTER commands comply with Request for Comments (RFC) 822 and 2822. 822 commands must be followed by a blank line.

18. Type the following command to add message body text: This is a test message you will not see a response from this command.
19. Type a period (.) at the next blank line then press Enter.
20. Receive the following response: 250 OK.
21. Close the connection by typing the following command: QUIT.
22. Receive the following response: 221 closing connection.
23. Verify that the recipient received the message. If any error event messages appear in the event log, or if the recipient did not receive the message, check the configuration or the communication to the host.