                        Forced Redirects in SMTP
                       draft-sam-smtp-redirects-00

Abstract

   This document specifies two new response codes in the SMTP protocol
   that relate to the redirection of emails meant for one email address
   to another mail server/email address.

Status of This Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF). Note that other groups may also distribute
   working documents as Internet-Drafts. The list of current Internet-
   Drafts is at https://datatracker.ietf.org/drafts/current/.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time. It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   This Internet-Draft will expire on 10 January 2021.

Table of Contents

1. Introduction

In todays digital world, email is the primary way of communication
for almost all Internet users. On the internet, there are many
services and accounts that require the use of a email address for
password recovery, etc. Changing a email address while "letting go"
of the old one can be very difficult. For the most part there
already is a solution: People trying to switch from one provider to
another have to "forward" email from their old mailbox to their new
one.

This system presents some problems. First off, the forwarded emails
are still going through the original mail server. w `While some may
like the system of silent fowarding (for example; having a support
email that goes to a random employee in the support department), some
may want to directly give their new address to people sending them
mail. If someone switched their email address to prevent their
emails from being processed or "seen" by the original mail server,
forwarding would be insufficient. In addition, mail server admins
may not want to deal with the extra bandwidth/CPU time required to
forward/relay emails to another server. The 2nd problem is that the
new email address doesn't automatically get updated with all of the
accounts or internet services the owner of the email address may
have, meaning that many entities wouldn't have any record of the new
email and would continue to send emails to the old email. Changing
the email address for each service a person has signed up with is
nearly impossible, and there are bound to be some that a person would
forget to change. To remedy this some opt to send an automated reply
email with their new email address to anyone that emails them; but
this system is not standardized and most automated systems fail to
recognize a email like this. This document aims to fix these
problems by introducing two new reply codes to be used in SMTP
sessions.

1.1. Terminology

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 RFC 2119.

A email is known as "hard-linked" if the mail server is using the
557/558 reply codes to redirect mail to another email address.

The term "sending MTA" or "sending mail server" means any networked
device that tries to send mail to an email address/server, while the
term "receiving MTA" or "receiving mail server" is any networked
device that is receiving mail from a sending MTA.

A "email address" is a valid forward-path as defined in [RFC5321].

A email is known as "hard-linked" if the mail server is using the
557/558 reply codes to redirect mail to another email address.

The email given in the 557/558 response code is defined as the "new"
email address.

2. Problems with using 551 response code

The problem with "reclaiming" the 551 response code is that it is now
being used for anything from incorrect authentication issues to a
response given to when the server is requested to act as an open
relay. This document mandates that any sending MTA that understands
the 557/558 response codes MUST make an attempt to resend the email
to the address given in the 557/558 response. In addition, any
response with a 557/558 code MUST include an additional email
address. Whether or not the forward-path is required to be included
in the 551 response code is unclear in previous RFCs.

3. The 557 and 558 response codes

The 557 and 558 codes are newly created response codes that are used
to "hard-link" email addresses. They both work by responding to a
SMTP request with the new email address.

Think of these response codes as a "forced" 551 response; on
receiving the 557 or 558 response, the sending mail server MUST try
to attempt delivery to the new address. This is what makes it
different from the 551 response code; most mail clients today just
regard 551 as a "failed send". When a email address is "hard-linked"
to a new one, the original email should be treated as if it was a
invalid/inactive/undeliverable email. However, Clients are still not
obligated to update any records as a result of a 557/558.

Servers now have multiple options when it comes to forwarding mail:
acknowledge forwarding with the 251 response code, forward silently
with the 250 code (what most servers do today), mark message as
undeliverable with 550/551, or use the 557/558 response codes. Like
with response code 551, receiving MTAs returning a 557/558 MUST NOT
assume that the client/sending MTA will update any records; but they
can assume that they will deliver it to the email specified in the
response.

3.1. The 557/X.2.7 Response Code

This code should be used when a mailbox has permanently moved to a
different email address. The function of this code is similar to the
HTTP 301 response code. This code is used to indicate that the owner
of the mailbox in question has permanently changed their email
address to one specified in the error response. When a sending mail
client receives this error code, they should send the intended email
to the email address specified in the response if they want the email
to be delivered. Since this is a permanent change, if the sending
MTA (mail transfer agent) is part of a larger system that keeps
tracks of emails (for example: a website/app that keeps emails for
password recovery), then the record SHOULD be updated (but is never
obligated to) hold the new email instead of the old email. If a user
emails another person and the receiving mail server returns a 557
code, then the server SHOULD notify the user about the new email
address.

Here is a sample session between two mail servers to showcase the 557
response code.

```
S: 220 smtp.example.com smtp service ready
C: HELO mail.example.net
S: 250 mail.example.net, I'm happy that you came around today
C: MAIL FROM: <postmaster@example.net>
S: 250 ok
C: RCPT TO:<http@example.com>
S: 250 ok
C: RCPT TO:<gopher@example.com>
S: 557 mailbox has moved to <mccahill@example.org> (X.2.7)
```

Client then connects to mail.example.org.

The server MUST include the new email address for mail to be
redirected to in the 557 response. It MUST NOT include any other
email addresses in the response.

3.2. The 558/X.2.8 Response Code

   This code should be used when a mailbox has TEMPORARILY moved to a
   different email address, which is similar to the 307 response code in
   HTTP. This code should be used to indicate that the owner of the
   mailbox has temporarily moved to a new email address. The reaction
   to this code is similar to the 557 response code; MTAs should attempt
   delivery to the new address. However, this code implies that the
   owner of the email address will remove the "hard-link" at some point,
   so any services keeping track of emails SHOULD NOT update the old
   email in their records.

   Like the 557 reply code, the response MUST include the new email
   address in the response and MUST NOT include any other email address,
   and the sending MTA MUST NOT make any attempt to send the email
   through the old email server.

4. Security Considerations

   A man in the middle/DNS hijack of a email server could return the 557
   return code when an attempt is made to send mail to any email address
   on the hijacked server. Thus, mail clients should be sure that they
   are connecting to the right server. (a DNS/Man in the middle attack
   would still allow emails to be "intercepted" if the servers are using
   plain text and forwarding is in place)

5. IANA Considerations

   IANA should add the following to the "SMTP Enhanced Status Code"
   registry:

   * Add 557/X.2.7 "Permanently Moved" response code

   * Add 558/X.2.8 "Temporarily Moved" response code

6. References

6.1. Normative References

   [RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321,
              October 2008, <https://www.rfc-editor.org/info/rfc5321>.

6.2. Informative References

   [RFC3463] Vaudreuil, G., "Enhanced Mail System Status Codes",
              January 2003, <https://www.rfc-editor.org/info/rfc3463>.

Author's Address

   Ekow Sam

   Email: winshell64@gmail.com