

Network Working Group
Internet-Draft
Updates: [5321](#) (if approved)
Intended status: Standards Track
Expires: May 18, 2014

F. Martin, Ed.
LinkedIn
A. Peterson, Ed.
Message Systems
November 14, 2013

SMTP IPv6 to IPv4 Fallback: An Applicability Statement
draft-martin-smtp-ipv6-to-ipv4-fallback-00

Abstract

This Applicability Statement describes how Mail Transfer Agents (MTAs) can be encouraged to fall back to IPv4 when a message is refused over IPv6.

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 <http://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 May 18, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
1.1.	Moving from IP Reputation to Domain Based Reputation . .	2
2.	Requirements Language	3
3.	Indicating the sender-SMTP server to fall back to IPv4 . . .	3
3.1.	With the service extension IPV6-IPV4-FALLBACK	3
3.2.	Without service extension	4
4.	Acknowledgements	5
5.	IANA Considerations	5
5.1.	SMTP Enhanced Status Codes Registry update	5
5.2.	Simple Mail Transfer Protocol (SMTP) Service Extensions Registry update	6
6.	Security Considerations	6
7.	References	6
7.1.	Normative References	7
7.2.	Informative References	7
Appendix A.	Examples and research	7
A.1.	SMTP fall back from IPv6 to IPv4 without service extension	7
A.2.	SMTP fall back from IPv6 to IPv4 with service extension .	8
A.3.	Common Open Source MTA Design	9
A.3.1.	MX RR configuration	10
A.3.2.	Rejecting Messages for Immediate Retry on IPv4	11
	Authors' Addresses	12

[1.](#) Introduction

The Simple Mail Transfer Protocol (SMTP) is defined in [\[RFC5321\]](#). [Section 5](#) of that document describes the process of host selection. SMTP clients in well known Mail Transfer Agent (MTA) software will retry a message using a different Mail Exchanger (MX) or network address if the message is temporarily rejected. This document describes under which circumstances well known and widely deployed open source MTAs (and others) can be made to retry over IPv4 when an initial connection to IPv6 results in a temporary rejection. Furthermore, the purpose of this document is to record that behaviour and encourage its further adoption while at the same time providing for the future a well defined mechanism via a service extension with cooperating SMTP clients. This behavior could be useful in, for instance, enforcing higher requirements for Simple Mail Transfer Protocol (SMTP) sessions over IPv6 than what exists on IPv4 without simply rejecting the message outright.

[1.1.](#) Moving from IP Reputation to Domain Based Reputation

IPv6 brings more IP addresses, which means building an IP-based reputation system using IPv6 addresses could be difficult to achieve.

Moving from an IP based reputation system to a domain based reputation system is expected to be easier. However, it requires that all SMTP servers participate.

IPv4 address space is well known and many tools have been built to handle unwanted emails from certain IPv4 addresses. There is not yet such expertise on IPv6 nor tools. However, labels, like domain names are more stable, unlike the more dynamic nature of IP address allocation, and provide a relatively better chain to associate an email to its author, provided such labels can be authenticated. Such labels allow better reporting of unwanted emails to the system administrators of mail servers in these domains.

As IPv6 is still relatively nascent, there is a chance to mandate use of the Sender Policy Framework (SPF, [\[RFC4408\]](#)) or DomainKeys Identified Mail (DKIM, [\[RFC6376\]](#)) or similar domain-based authentication mechanisms for messages sent over IPv6 and, if these fail, to do retries over IPv4.

2. Requirements Language

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](#) [\[RFC2119\]](#).

3. Indicating the sender-SMTP server to fall back to IPv4

To move from IP based reputation to a domain based reputation system for email, a receiver-SMTP could, for example, require that messages pass SPF [\[RFC6652\]](#) or DKIM [\[RFC6376\]](#). This section does not discuss the merit of such policy but proposes mechanisms for any policy to get the sender-SMTP to fall back to IPv4 from an IPv6 connection.

3.1. With the service extension IPV6-IPV4-FALLBACK

The receiver-SMTP MAY advertise a service extension IPV6-IPV4-FALLBACK, which the sender-SMTP replies by IPV6-IPV4-FALLBACK if capable

In this condition for each message not acceptable due to policy where a retry over IPv4 is requested, the sender-SMTP server MUST reply by the reply code 456, where the sender-SMTP requeues the message for immediate retry by selecting a receiver, according to [Section 5 of \[RFC5321\]](#), that is at an IPv4 address..

If there is no IPv4 address to be tried, the sender-SMTP SHOULD fail the message.

If the receiver-SMTP implements enhanced status codes [[RFC5248](#)], The SMTP enhanced status code SHOULD be 4.4.8.

Example status message

```
456 4.4.8 please retry immediately the message over IPv4
because it fails SPF and DKIM
```

The SMTP status code 456 is introduced in this document, and has a very specific meaning associated to the service extension. The SMTP enhanced status code is also introduced in this document, but like all enhanced status codes, they are usually not interpreted by the SMTP client, but for the bounce processor as to provide more meaningful reports to the mail administrator.

[3.2.](#) Without service extension

The receiver-SMTP server MUST have MX RR pointing to single stack hostnames and for same MX RR preference MUST have a MX RR pointing to an hostname with an A RR and a MX RR pointing to an hostname with an AAAA RR. No hostname pointed by a MX RR have a A RR and an AAAA RR.

For example:

```
example.org.      IN MX    1  mx1-6.example.org.
                  IN MX    1  mx1.example.org
                  IN MX   10  mx10-6.example.org.
                  IN MX   10  mx10.example.org
mx1-6.example.org. IN AAAA 2001:db8:ffff::1
mx1.example.org.  IN A    192.0.2.1
mx10-6.example.org. IN AAAA 2001:db8:ffff::2
mx10.example.org  IN A    192.0.2.2
```

When a receiver-SMTP makes a policy decision not to accept a message over IPv6, it rejects the message with a 451 code if done at connection time and 421 code if done later and terminates the connection so the sender-SMTP requeues the message for immediate retry by selecting a receiver, according to [Section 5 of \[RFC5321\]](#), that is at an IPv4 address..

If the receiver-SMTP implements enhanced status codes [[RFC5248](#)], The SMTP enhanced status code SHOULD be 4.4.8.

The rejection at connection time MAY be issued only when it has been demonstrated that a majority of messages would not pass the policy and that the sender-SMTP is not capable of the service extension IPV6-IPV4-FALLBACK.

The rejection at connection time SHOULD be for a limited time to give a chance for later messages to be re-evaluated against the policy.

456 is not used here, as it is a new SMTP status code introduced for clients that understand the service extension IPV6-IPV4-FALLBACK. It is not sure that sender-SMTP without this service extension would behave as expected with a new SMTP status code.

Research presented in annexes has shown that common MTA exhibit this behavior.

4. Acknowledgements

Thanks to Murray Kucheraway for guidance in getting this draft out.

5. IANA Considerations

This section describes actions requested of IANA.

5.1. SMTP Enhanced Status Codes Registry update

IANA is requested to add the following to the Simple Mail Transfer Protocol (SMTP) Enhanced Status Codes Registry:

- o Enumerated Status Codes
- o Code: X.4.8
- o Summary: retry on IPv4
- o Associated basic status code: 421,451,456
- o Description: the mail system will not accept this message over IPv6 because it lacks some requirements described in the full text of the rejection, however the sending mail system can retry immediately to submit the message over IPv4 only.

5.2. Simple Mail Transfer Protocol (SMTP) Service Extensions Registry update

IANA is requested to add the following to the Simple Mail Transfer Protocol (SMTP) Service Extensions Registry:

- o Textual name: Capable to retry the message over IPv4 from IPv6 if requested
- o EHLO Keyword: IPV6-IPV4-FALLBACK
- o There is no parameters associated with the extension
- o SMTP verb: IPV6-IPV4-FALLBACK
- o Description: When the server indicates the service extension and the client indicates via the SMTP verb that it supports such extension, if the server rejects the message with the status code 456, the client will requeue the message to be delivered over IPv4.
- o This extension does not increase the length of the MAIL and RCPT commands

6. Security Considerations

SMTP clients might not not fall back to IPv4 when requested (by not implementing this proposal) and keep retrying on IPv6. MTA administrators ought to monitor for such servers, and could whitelist them to accept messages over IPv6 or take other action as appropriate.

Messages may start to queue on the sender-SMTP side and the mail administrator may not notice it or take appropriate action in time.

If the policy is not explained clearly the mail administrator may not know what is required to pass the policy.

If the policy is too cumbersome and is not based on widely adopted standards and recommendations, the mail administrator may decide not to jump through hoops to get the email delivered.

The fall back mechanism without service extension may create unnecessary burden for the sender as well as the receiver.

7. References

7.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC4408] Wong, M. and W. Schlitt, "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1", [RFC 4408](#), April 2006.
- [RFC5248] Hansen, T. and J. Klensin, "A Registry for SMTP Enhanced Mail System Status Codes", [BCP 138](#), [RFC 5248](#), June 2008.
- [RFC5321] Klensin, J., "Simple Mail Transfer Protocol", [RFC 5321](#), October 2008.
- [RFC6376] Crocker, D., Hansen, T., and M. Kucherawy, "DomainKeys Identified Mail (DKIM) Signatures", STD 76, [RFC 6376](#), September 2011.
- [RFC6652] Kitterman, S., "Sender Policy Framework (SPF) Authentication Failure Reporting Using the Abuse Reporting Format", [RFC 6652](#), June 2012.

7.2. Informative References

- [RFC3974] Nakamura, M. and J. Hagino, "SMTP Operational Experience in Mixed IPv4/v6 Environments", [RFC 3974](#), January 2005.
- [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [BCP 26](#), [RFC 5226](#), May 2008.

Appendix A. Examples and research

A.1. SMTP fall back from IPv6 to IPv4 without service extension

The sender-SMTP server opens a connection to the receiver-SMTP example.org over IPv6, the message is refused because no domain authentication can be performed therefore the sender-SMTP retries immediately using IPv4. "S" indicates text sent by a server, and "C" indicates text sent by a client. Line terminations are omitted in this illustration.


```
S: 220 ipv6.example.com Simple Mail Transfer Service Ready
C: EHLO example.org
S: 250-ipv6.example.com greets example.org over IPv6
S: 250-8BITMIME
S: 250-SIZE
S: 250-DSN
S: 250 HELP
C: MAIL FROM:<Smith@example.org>
S: 250 OK
C: RCPT TO:<Jones@example.com>
S: 250 OK
C: DATA
S: 354 Start mail input; end with <CRLF>.<CRLF>
C: [message body]
C: .
S: 421 4.4.8 message with no SPF or DKIM and over IPv6
S: <disconnect>

S: 220 ipv4.example.com Simple Mail Transfer Service Ready
C: EHLO example.org
S: 250-ipv4.example.com greets example.org over IPv4
S: 250-8BITMIME
S: 250-SIZE
S: 250-DSN
S: 250 HELP
C: MAIL FROM:<Smith@bar.com>
S: 250 OK
C: RCPT TO:<Jones@example.com>
S: 250 OK
C: DATA
S: 354 Start mail input; end with <CRLF>.<CRLF>
C: [message body]
C: .
S: 250 OK
C: QUIT
S: 221 foo.com Service closing transmission channel
```

A.2. SMTP fall back from IPv6 to IPv4 with service extension

The sender-SMTP server opens a connection to example.com over IPv6, the message is refused because no domain authentication can be performed therefore the sender-SMTP retries immediately using IPv4. "S" indicates text sent by a server, and "C" indicates text sent by a client. Line terminations are omitted in this illustration.


```
S: 220 ipv6.example.com Simple Mail Transfer Service Ready
C: EHLO example.org
S: 250-ipv6.example.com greets example.org over IPv6
S: 250-8BITMIME
S: 250-SIZE
S: 250-DSN
S: 250-IPV6-IPV4-FALLBACK
S: 250 HELP
C: IPV6-IPV4-FALLBACK
S: 250 OK
C: MAIL FROM:<Smith@bar.com>
S: 250 OK
C: RCPT TO:<Jones@example.com>
S: 250 OK
C: DATA
S: 354 Start mail input; end with <CRLF>.<CRLF>
C: [message body]
C: .
S: 456 4.4.8 message with no SPF or DKIM and over IPv6
C: QUIT
S: 221 foo.com Service closing transmission channel
```

Message is then retried immediately over IPv4

[A.3.](#) Common Open Source MTA Design

This section discusses current implementations in common open source MTAs.

SMTP clients only interpret SMTP status codes, but the use of SMTP enhanced status codes can be used to better monitor and act on the reason of the temporary failure.

For instance, at the end of DATA, if the message was sent over IPv6, the SMTP server can evaluate whether the message passes SPF or DKIM and reject the message using 421 if neither pass. If one passes, then an authenticated domain name is available and domain reputation rules can be applied. The IPv6 address of the SMTP client can be noted, and further connections over IPv6 can be temporarily failed using the 451 status code for some period of time period so as to minimize resources to evaluate each message after the end of DATA. On the other hand, if a message coming from an IPv6 address does not pass SPF or DKIM, it is unlikely that this state would quickly change for the next message coming from the same network address.

For proprietary mail systems or large mailbox providers, they all do a form of domain authentication, either SPF or DKIM, so the above may not apply to them. Not all are yet enabled to send email over IPv6.

Some observations:

- o When presented with a permanent failure code (5yz) during connection establishment, MTA clients will declare the message non deliverable and will not retry it on a different MX. Some clients do retry however.
- o When an SMTP server rejects during the connection phase using the code 451 and disconnects, the SMTP client will typically retry the message immediately on a different MX.
- o When an SMTP server rejects after the DATA phase using a 421 SMTP reply code followed by a disconnect, the SMTP client will retry the message immediately on a different MX.

MX RR configuration and the proper rejection need both to be properly defined.

A.3.1. MX RR configuration

When a message is temporarily refused, using a 400-series SMTP error code, the strategy for the SMTP client is sometimes to retry immediately to a different MTA, as defined by the target selection process defined in [[RFC5321](#)].

When the new MX refers to a dual-stacked machine (see [[RFC3974](#)]), some MTA software will not pick up all of the A or AAAA RRs (Resource Records), but will instead select only the RRs matching the address family preferred by the local TCP/IP implementation. Thus, MX RRs MUST NOT refer to dual-stacked machines.

For instance, the following configuration is desired:

```
example.org.      IN MX    10  mx1.example.org.
                  IN MX    10  mx1-6.example.org.
mx1.example.org.  IN A      192.0.2.1
mx1-6.example.org. IN AAAA   2001:db8:ffff::1
```


In this configuration, the SMTP client see two MXes at the same preference, and will automatically pick one and try the other one if the message is properly temp-failed. Therefore, in the above example, if the first connection was over IPv6 and the message temporarily refused and the session disconnected, the next connection will be over IPv4.

[A.3.2.](#) **Rejecting Messages for Immediate Retry on IPv4**

Here is an example of an initial message sent over IPv6. The SMTP client then retries immediately on the next MX record, here an IPv4 address. "S" indicates text sent by a server, and "C" indicates text sent by a client. Line terminations are omitted in this illustration.

```
C: <connection establishment>
S: 220 example.net Simple Mail Transfer Service Ready
C: EHLO example.com
S: 250-example.net greets example.com over IPv6
S: 250-8BITMIME
S: 250-SIZE
S: 250-DSN
S: 250 HELP
C: MAIL FROM:<Smith@example.com>
S: 250 OK
C: RCPT TO:<Jones@example.net>
S: 250 OK
C: DATA
S: 354 Start mail input; end with <CRLF>.<CRLF>
C: <message content>
C: .
S: 421 4.4.8 SPF and/or DKIM required on IPv6; try elsewhere
C: QUIT
S: 221 foo.com Service closing transmission channel
```

Where the client is known to not use DKIM and/or SPF, the server may terminate the connection immediately:

```
C: <connection establishment>
S: 451 4.4.8 Come back on IPv4 as I told you before
```


Authors' Addresses

Franck Martin (editor)
LinkedIn
Mountain View, CA
US

Email: fmartin@linkedin.com

Alec Peterson (editor)
Message Systems
Columbia, MD
US

Email: alec@messagesystems.com

