Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 21, 2014

J. Levine
Taughannock Networks
M. Delany
Apple Inc.

May 20, 2014

A NULL MX Resource Record for Domains that Accept No Mail
draft-ietf-appsawg-nullmx-01

Abstract

Internet mail determines the address of a receiving server through the DNS, first by looking for an MX record and then by looking for an A/AAAA record as a fallback. Unfortunately this means that the A/AAAA record is taken to be mail server address even when that address does not accept mail. The NULL MX RR formalizes the existing mechanism by which a domain announces that it accepts no mail, which permits significant operational efficiencies.

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 November 21, 2014.

Table of Contents

1. Conventions Used in This Document

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 [RFC2119].

2. Introduction

This document formally defines the "NULL MX" as a simple mechanism by which a domain can indicate that it will never accept email.

SMTP clients have a prescribed sequence for identifying aserver that accepts email for a domain. Section 5 of [RFC5321] covers this in detail, but in essence the SMTP client first looks up a DNS MX RR and if that is not found it falls back to looking up a DNS A or AAAA RR. Hence this overloads an email service semantic onto a DNS record with a different primary mission.

If a domain has no MX records, senders will attempt to deliver mail to the hosts at the domain's A or AAAA record's addresses. However many domains do not accept email.

If there is no SMTP listener at the A/AAAA address, the message will be attempted repeatedly for a long period, typically a week, before the sending MTA gives up. This will delay notification to the sender in the case of misdirected mail, and will consume resources at the sender.

A domain could set up an SMTP listener at that address that rejects all connections (for instance with a 554 response as a connection-opening response) or have an MX record pointing to such a listener, to notify senders in a timely fashion. But resources (generating a bounce) will still be consumed by the sender and it requires additional services to be provided which provide little benefit to the domain.

These resource usage problems are exacerbated when large volumes of email are sent using forged email addresses from a domain which does not accept email as its envelope sender, causing large numbers of bounces to be generated and to consume large amounts of resources at the sender of the bounces.

This document defines a NULL MX that will cause all mail delivery attempts to a domain to fail immediately.

3. SMTP server benefits

The ability to detect domains that never accept email offers many resource savings to an SMTP server. It can choose to reject email during the SMTP conversation that presents an undeliverable 5321.MailFrom domain.

Also, if an SMTP server accepts a message, it can be more confident that an attempt to send a Delivery Status Notification or other response will reach a recipient SMTP server. This helps to reduce non-delivery queues. Currently, a DSN for, e.g., www.example.net, will sit in the queue for a full queue lifetime until the server's attempts to deliver to www.example.net time out.

4. Parallel Considerations

Senders of abusive email often use return addresses with domain names that do not accept mail. the perpetrators of such mail can adapt such that the "vast class of email" that this mechanism helps identify, simply move over to using 5321.MailFrom domains that have valid MX RRs.

While this is true, the direct benefits to the SMTP server still apply. When an SMTP server queues a non-delivery email, the target domain will accept the email or give a definitive rejection so the queue entry will be removed promptly, thus keeping the queues short.

There is also a fair amount of mail that is just misaddressed by people who mistranscribed or misunderstood an e-mail address, for example, alice@www.example.com or alice@examp1e.com rather than alice@example.com. NULL MX allows a mail system to report the

delivery failure when the user sends the message, rather than hours or days later.

5. The NULL MX Resource Record

To indicate that a domain never accepts email, it advertises a single MX RR with a RDATA section consisting of preference number 0, and a dot, i.e., the DNS root, as the mail exchanger domain, to denote that there exists no mail exchanger for a domain. (The DNS root is not a valid host name, which avoids any possibility that a NULL MX record could be confused with an ordinary MX record.)

The interpretation of a NULL MX RR only applies when the domain has a single MX RR. If a domain advertises multiple MX RRs including a NULL MX, the interpretation is as described in RFC5321.

6. Domains that do not send mail

The operator of an SMTP server might prefer to reject mail sent from domains that publish NULL MX, since a response or non-delivery notice will never be accepted, and legitimate mail rarely comes from domains that do not accept replies.

SMTP servers that reject mail because a MAIL FROM domain has a NULL MX record SHOULD use a 550 reply code.

A domain that does not accept mail, as declared by NULL MX, often will also not send mail. Operators can publish SPF [RFC4408] -ALL policies to make an explicit declaration that the domain is not valid in the rfc5321.mailfrom command.

7. Security Considerations

SMTP mail is inherently insecure in that it is feasible for even fairly casual users to negotiate directly with SMTP servers. This specification is about eliminating one small section of SMTP insecurity.

In the unlikely event that a domain legitimately sends email but never wants to receive email, SMTP servers that reject mail from domains that advertise a NULL MX risk losing email from those domains. Note that the normal way to send mail for which a sender wants no responses remains unchanged, by using an empty 5321.MailFrom address.

Within the DNS, a NULL MX RR is an ordinary MX record and presents no new security issues.

8. References

8.1. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, October 2008.

8.2. Inforrmative References

[RFC4408] Wong, M. and W. Schlitt, "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1", RFC 4408, April 2006.

Appendix A. Change Log

NOTE TO RFC EDITOR: This section may be removed upon publication of this document as an RFC.

A.1. Change to appsawg-nullmx-1

Editorial improvements per D. Crocker's review.

A.2. Change to appsawg-nullmx-0

Fix typos.

Authors' Addresses

John Levine
Taughannock Networks
PO Box 727
Trumansburg, NY 14886

Phone: +1 831 480 2300
Email: standards@taugh.com
URI: http://jl.ly

Mark Delany
Apple Inc.
1 Infinite Loop
Cupertino, CA 95014

Email: mx0dot@yahoo.com