

# Improvements in TCP/IP Services anti-spam features

*Source:* <http://unix.derkeiler.com/Newsgroups/comp.os.vms/2003-04/2951.html>

---

*From:* John Johnstone ([jj\\_usenet2\\_at\\_yahoo.com](mailto:jj_usenet2_at_yahoo.com))

*Date:* 04/30/03

Date: Tue, 29 Apr 2003 19:11:58 -0400

There really should be a way to configure the handling of non-existent addresses with HP's TCP/IP Services. Mail to non-existent addresses has reached an intolerable level here. Of all the email addresses that we have, the ones that get the most spam are old addresses that are no longer valid. And it's incredibly ironic that the volume of mail being sent to them is still on the increase. There has even been a big increase to one email address that has never existed. The spam to it started coming from a few consistent IP addresses. Since that's been filtered, all of the mail to this address come from random IPs with random return-paths that are completely unfilterable.

Since 85% of our spam that isn't blocked has an invalid return address, that means all of those messages will be generating a bounce to Postmaster. As Don Sykes noted, the side-effect of clogging up the mail queues with hopeless retries is also quite a drain.

It was great that they added anti-spam features to TCP/IP Services but going just a little bit further would have a huge payoff. How about another field name such as Reject-Rcpt-To?

Reject-Rcpt-To: old-email-address@domain-name

With spam, looking for a signature to match on the mail message (i.e. Mail-From, source IP address, etc.) is always a moving target. If specific non-existent addresses could be configured for a reject, that would block 100% of the spam sent to those addresses. A reject message Reject-Rcpt-To-Text could be tailored as desired if feedback for valid mail was a concern. In my case, if email is sent any of these particular old addresses, there's a 99.999% chance that it's spam.

Since some spammers are thoughtful enough to put the recipient address in as a component of the return-path address, I've found that I can block some spam with:

Reject-Mail-From: \*old-email-address\*domain-name\*

Reject-Mail-From: \*domain-name\*old-email-address\*

## comp.os.vms: Improvements in TCP/IP Services anti-spam features

This regularly catches a small percentage of the spam sent to the old email addresses. You'd think that putting the recipient address in the return-path address would indicate that the sender would be interested in knowing about invalid addresses. That's clearly not the case with many spammers. The bounce or reject does nothing to stop the flow sent from many sources even when the bounces are accepted by the sender.