E-mail services over IPv6-only

Ondřej Caletka
Ondrej.Caletka@cesnet.cz

cesnet

August 24, 2018

Neběží.cz / DoesNotWork.eu

- personal contribution to the 2012 World IPv6 launch
- one of approximately 10 .CZ domains publishing only AAAA record
- lightweight static design
- displays information about IPv4 capability and preference

Neběží.cz after launch

- announced during the 2012 IPv6-day conference in Prague
- contact e-mail address with IPv6-only domain
- most people got their e-mail bounced

- added auto-replying mail checker `test@doesnotwork.eu`.
- added reverse DNS record check
- added English version at `http://www.doesnotwork.eu`.

cesnet

IPv6 E-mail checker

- many (mostly) unrelated abilities to test:
  1. deliver mail to v6-only destination
  2. receive mail over IPv6
  3. receive mail from IPv6-only envelope address
  4. receive mail from IPv6-only in-body `From:` address
- my solution:
  1. autoresponder triggered by receiving an e-mail to IPv6-only address
  2. respond from IPv4-only domain via dual-stack transport
  3. respond from IPv6-only domain via IPv6-only transport
  4. in case the IPv6-only bounces, the DSN is forwarded to the origin via dual-stack
- **feel free to try it at `test@doesnotwork.eu`**

cesnet

Used components

- Postfix mail server with two personalities
  - one is dual-stacked
  - other is IPv6-only
  - selected by envelope recipient address
- procmail
- simple custom Python script
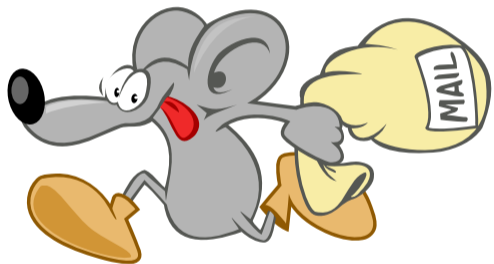
Processed bounce

Od	**DoesNotWork.eu autoreply over IPv4 <test@ipv4.doesnotwork.eu>** ★
Předmět	**DoesNotWork.eu: You are not receiving e-mails over IPv6!**
Komu	
DKIM	Valid (Signed by ipv4.doesnotwork.eu)

Sorry!

Although you were able to send a message to IPv6-only address, there was a problem delivering reply from that address.

The exact description of the problem observed by our server www.doesnotwork.eu is attached. You can inform your e-mail service provider about the issue.

```
--
DoesNotWork.eu
```

```
Final-Recipient: rfc822;                           .org
Action: failed
Status: 5.4.4
Diagnostic-Code: X-Postfix; Host or domain name not found. Name service error
    for name=mxcluster2.one.com type=AAAA: Host found but no data record of
    requested type
```

cesnet

RFC 2821 vs. RFC 5321

RFC 2821

- Proposed standard, 2001
- Defines SMTP over IPv6, IPv6 literals, etc.
- "If no MX records are found, but an A RR is found, the A RR is treated as if it was associated with an implicit MX RR."

RFC 5321

- Draft standard, 2008, obsoletes RFC 2821
- "If an empty list of MXs is returned, the address is treated as if it was associated with an implicit MX RR, with a preference of 0, pointing to that host."

cesnet

Gmail MX handling

- first, only AAAA record for `www.doesnotwork.eu`, no MX
- Gmail bounced immediatelly, saying that there is "No MX record."
- then, self-referring MX record has been added:
  `doesnotwork.eu.  IN  MX 0 www.doesnotwork.eu.`
- with that, Gmail used to hold the message in queue for 3 days, bouncing every 24 hours with following failure:
  `DNS Error: DNS server returned answer with no data`
- this has been fixed around August 2013
  (but Gmail does not accept mail over IPv6 without reverse DNS record)

`http://postfix.1071664.n5.nabble.com/disable-ipv6-when-sending-to-gmail-tp60672p60673.html`

cesnet

Statistics 06/2012 – 10/2012

- no information about delivery attempts
- cca. 100 messages succesfully received from 88 different domains
- no automatic check of the return path by that time
- return path domains lead to 135 different MX destinations, with 113 different IPv4 addresses and 71 different IPv6 addresses
- from 71, only 50 actually accepted TCP connect to port 25!
- all major freemail services, even if webmail was IPv6 ready, could not deliver to IPv6-only network

cesnet

Statistics 05/2014 – 10/2016

- no information about delivery attempts
- 303 test messages received from 217 unique addresses
- 138 unique domain names
- 39 IPv6 bounces from 26 different addresses
  - 34 bounces due to "No AAAA record for MX"
  - 4 bounces due to "Invalid recipient"
  - 1 bounce due to "Protocol error"
- the problem with servers not listening on IPv6 socket is obviously gone

cesnet

Statistics 11/2016 – 08/2018

- no information about delivery attempts
- 282 test messages received from 211 unique addresses
- 137 unique domain names
- 135 IPv6 bounces from 99 different addresses
    - 79 bounces due to "No AAAA record for MX"
    - 18 bounces due to "User Unknown"
    - 31 bounces due to "Unroutable sender's e-mail address"

cesnet

Receiving mail from IPv6-only domain

```
$ telnet smtp2.ms.mff.cuni.cz 25
Connected to smtp2.ms.mff.cuni.cz.
Escape character is '^]'.
220 smtp2.ms.mff.cuni.cz ESMTP Sendmail 8.15.2/8.15.2;
    Tue, 25 Oct 2016 00:07:20 +0200 (CEST)
HELO www.doesnotwork.eu
250 smtp2.ms.mff.cuni.cz Hello www.doesnotwork.eu
    [IPv6:2001:1528:132:70::d0e5], pleased to meet you
MAIL FROM: <ondrej@doesnotwork.eu>
553 5.5.4 <ondrej@doesnotwork.eu>... Sender's best MX
    (www.doesnotwork.eu.) has no IP. Please contact
    your network administrator for futher assistance.
```

cesnet

Securing the IPv6-only website

- how to prove ownership of IPv6-only domain name?
  - StartSSL, WoSign – IPv4-only *(and efficiently dead by now)*
  - only e-mail and HTTP authentication available
  - solved by temporary adding IPv4 MX to the DNS
- Let's Encrypt
  - launched in late 2015 – IPv4-only
  - DNS-based ownership validation since 01/2016
  - full IPv6 validation support since 07/2016
- there is deliberately no redirection to HTTPS
  - you can compare results
  - some HTTP accelerators (like Chrome for Android) **provide IPv6 gateway** as a side effect, but **only for HTTP**

cesnet

Testing various "check your webpage" sites

- `http://isup.me` – tells you that site is down
- `https://dane.sys4.de` – works since inception
- `https://www.ssllabs.com` – support added in 2015
- `https://hstspreload.appspot.com` – software is ready, Google cloud is not. Other domain `https://neběží.xyz` preloaded manually by a Chrome developer.
- HTTPS Everywhere – IPv6-only URLs fail in Travis CI
- `https://observatory.mozilla.org` – launched IPv4-only, partially fixed now

cesnet

Any questions?

Ondřej Caletka
ondrej@doesnotwork.eu
https://Ondrej.Caletka.cz

The slides are already available for download.