

E-mailové služby na IPv6-only

Ondřej Caletka
Ondrej.Caletka@cesnet.cz



5. června 2019



- osobní příspěvek ke světovému spuštění IPv6 v roce 2012
- jedna z přibližně deseti .CZ domén s IPv6-only adresou
- statický web
- informuje o funkčnosti IPv4 a preferenci



NEBĚŽÍ.CZ
Server, který na protokolu IPv4 neběží...

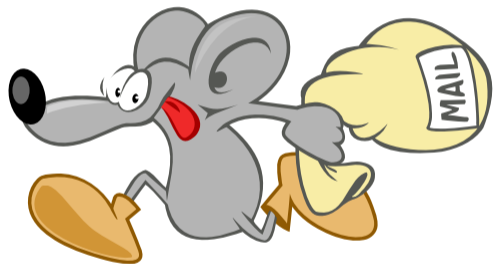
- ✓** Fokud se vám tato webová stránka načela, znamená to, že máte k dispozici připojení pomocí moderního protokolu IPv6. Gratulujeme!
- Info** Vaše IPv6 adresa je: 2001:c7c:64:42::1c:bfff:fe94:9543
Máte nastánu (nebo ručně nakonfigurovanou) IPv6 konektivitu!
- ✓** Vypadá to, že máte počítač připojený do sítě, která podporuje jak moderní protokol IPv6, tak i starší protokol IPv4.
- IPv6** V případě stránek, které jsou dostupné oběma protokoly, dává váš počítač přednost modernímu protokolu IPv6.
- ✉** Vyzkoušejte si ještě, zda váš e-mail umí IPv6. Zkuste nám napsat na test@nebezi.cz a počkejte na automatickou odpověď.

- oznámeno během konference IPv6-day v Praze
- kontaktní e-mailová adresa na IPv6-only doméně
- mnoho reakcí nebylo doručeno

- přidán automatický tester `test@doesnotwork.eu`.
- přidána kontrola reverzních záznamů
- přidána anglická verze na `http://www.doesnotwork.eu`.

- mnoho ne zcela souvisejících problémů:
 - ① doručit zprávu na IPv6-only adresu
 - ② přijímat zprávy po IPv6
 - ③ přijímat zprávy s IPv6-only obálkovou adresou
 - ④ přijímat zprávy s IPv6-only adresou odesílatele
- moje řešení:
 - ① automatický odpovídač je spuštěn doručením na IPv6-only
 - ② odpoví z IPv4-only adresy pomocí dual-stack přenosu
 - ③ odpoví z IPv6-only adresy pomocí IPv6-only přenosu
 - ④ nedoručenky jsou automaticky zpracovány a předány pomocí dual-stacku
- **vyzkoušejte na test@nebezi.cz**

- Postfix se dvěma osobnostmi
 - první je dual-stack
 - druhá je IPv6-only
 - výběr se provádí podle obáلكové adresy odesílatele
- procmail
- jednoduchý skript v Pythonu



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; [redacted].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

RFC 2821 vs. RFC 5321

RFC 2821

- Proposed standard, 2001
- Definuje SMTP přes IPv6, IPv6 literály, atd.
- “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, nahrazuje 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.”

- nejprve měl nebezi.cz jen AAAA záznam, žádné MX
- Gmail zprávy okamžitě odmítal s chybou “No MX record.”
- poté byl přidán MX záznam:
nebezi.cz. IN MX 0 www.nebezi.cz.
- od té doby Gmail držel zprávu 3 dny ve frontě, každých 24 upozorňoval na chybu:
DNS Error: DNS server returned answer with no data
- zhruba od srpna 2013 lze doručovat na IPv6-only bez problému
(ale při příjmu pošty po IPv6 je striktně vyžadován reverzní DNS záznam)

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

- bez informace o pokusech doručení
- cca. 100 zpráv přijatých z 88 různých domén
- bez automatické kontroly zpáteční adresy
- zpáteční adresa vedla na 135 různých MX serverů, 113 různých IPv4 adres a 71 různých IPv6 adres
- pouze 50 IPv6 adres přijalo TCP spojení na port 25
- žádný freemail nedokázal na IPv6-only doručit

- bez informace o pokusech doručení
- 303 zpráv z 217 různých adres
- 138 různých domén
- 39 nedoručenek pro IPv6 odpovědi od 26 různých adres
 - 34 nedoručenek kvůli “No AAAA record for MX”
 - 4 nedoručenky kvůli “Invalid recipient”
 - 1 nedoručenka kvůli “Protocol error”
- problém s nepřijímáním TCP spojení po IPv6 zmizel

- bez informace o pokusech doručení
- 395 zpráv z 280 různých adres
- 189 různých domén
- 149 nedoručenek pro IPv6 odpovědi od 118 různých adres
 - 93 nedoručenek kvůli “Host or domain name not found”
 - 34 nedoručenek kvůli “Unroutable sender’s e-mail address”
 - 19 nedoručenek kvůli “User Unknown”

Příjem pošty z IPv6-only domény

```
$ 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.nebezi.cz
250 smtp2.ms.mff.cuni.cz Hello www.nebezi.cz
    [IPv6:2001:1528:132:70::ebe2], pleased to meet you
MAIL FROM: <ondrej@nebezi.cz>
553 5.5.4 <ondrej@nebezi.cz>... Sender's best MX
    (www.nebezi.cz.) has no IP. Please contact
    your network administrator for futher assistance.
```

Zabezpečení IPv6-only webu

- jak prokázat držení IPv6-only domény
 - StartSSL, WoSign – IPv4-only (*a dnes už neexistují*)
 - vyřešeno dočasným IPv4 MX záznamem pro příjem ověřovací zprávy
- Let's Encrypt
 - spuštěno koncem roku 2015 – IPv4-only
 - validace pomocí DNS od ledna 2016
 - plná podpora validace po IPv4 od července 2016
- nepoužívám přesměrování na HTTPS
 - lze porovnat výsledky
 - některé HTTP akcelerátory (šetřič dat pro Chrome v Androidu) **fungují jako brána do IPv6, ale jen pro HTTP**

Testování webových testerů

- <http://isup.me> – dříve down, teď up
- <https://dane.sys4.de> – funguje od prvního dne
- <https://www.ssllabs.com> – podpora od roku 2015
- <https://hstspreload.appspot.com> – Google cloud stále IPv6 nepodporuje
- HTTPS Everywhere – IPv6-only URLs IPv6 nefunguje na Travis CI
- <https://observatory.mozilla.org> – spuštěno jako IPv4-only, částečně opraveno

Děkuji za pozornost

Ondřej Caletka
ondrej@nebezi.cz
[https://Ondřej.Caletka.cz](https://Ondrej.Caletka.cz)

