

Jemný úvod do Postfixu

InstallFest 2010

“The sendmail configuration file is one of those files that looks like someone beat their head on the keyboard. After working with it ... I can see why!”

-- Harry Skelton

Ondřej Čečák <ondrej@cecak.cz>



Email z pohledu uživatele

- email (e-mail, electronic mail)
 - původní koncept sdílení informací na víceuživatelském systému byl představen na MIT v roce 1961
 - “tradičnější” způsob komunikace v roce 1965 (ARPANET začal v roce 1969)



Email z pohledu uživatele

- uživatelé si na email rychle zvykli, především kvůli jeho vlastnostem
 - rychlost a relativně vysoká spolehlivost



Email z pohledu uživatele

- uživatelé si na email rychle zvykli, především kvůli jeho vlastnostem
 - rychlost a relativně vysoká spolehlivost
 - prakticky nulové náklady



Email z pohledu uživatele

- uživatelé si na email rychle zvykli, především kvůli jeho vlastnostem
 - rychlost a relativně vysoká spolehlivost
 - prakticky nulové náklady
 - určitá anonymita



Email z pohledu uživatele

- spam (více než 90 % všech emailů)
 - cca 100.000.000.000 spamů denně
 - těží z oblíbených vlastností emailu
 - funguje (!)
 - při nastavování mailserveru je s tím potřeba vždy počítat



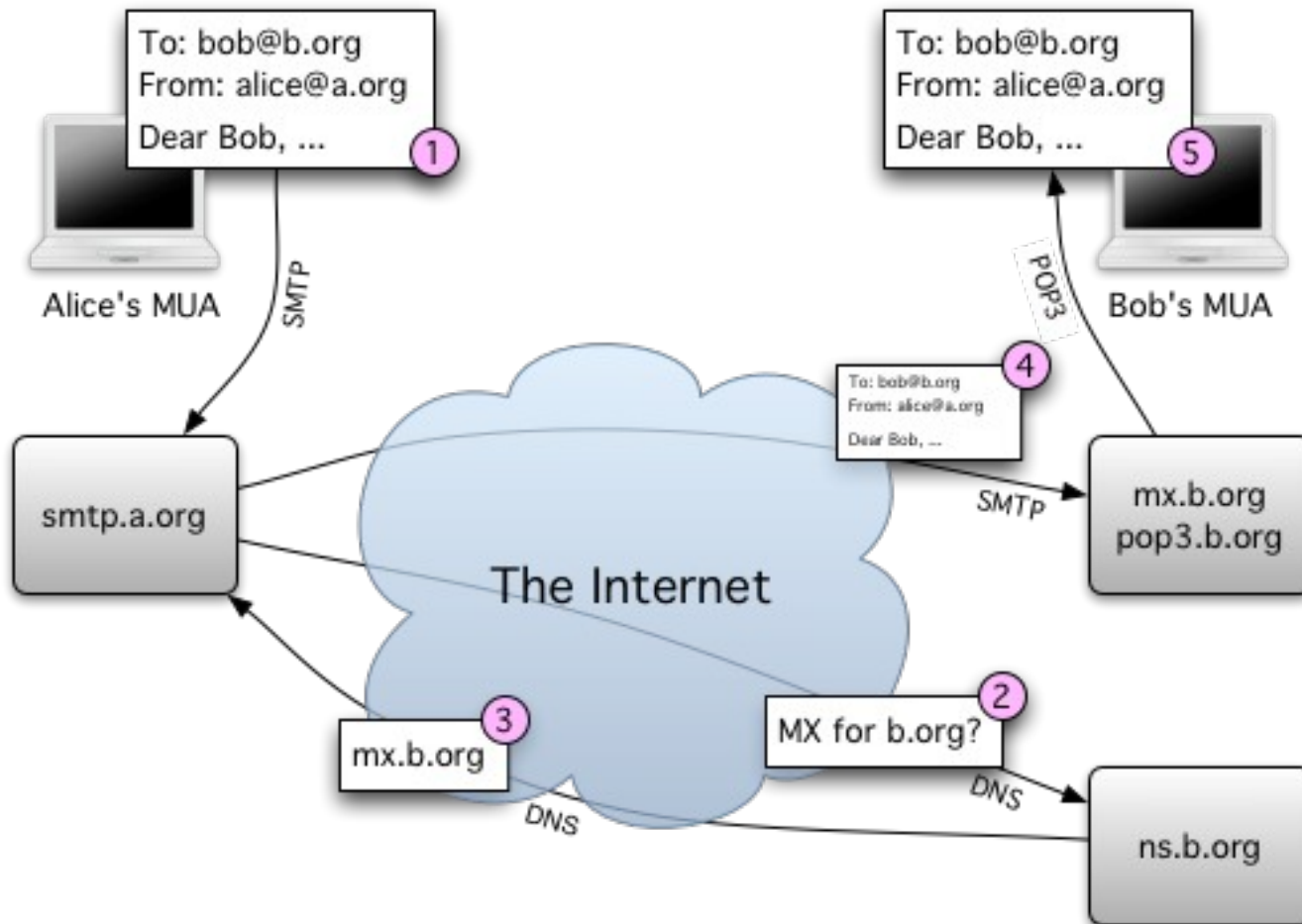
Email z pohledu uživatele

- spam (více než 90 % všech emailů)
 - cca 100.000.000.000 spamů denně
- anti-spam
 - opravdová nutnost
 - analýza obsahu
 - blacklisty
 - formality v DNS, SPF a podobné
 - reputace odesilatele



Email z pohledu správce

- jak to funguje?



Email z pohledu správce

- uživatel napíše email, pomocí SMTP ho pošle mailserveru
 - MUA (Mail User Agent), tedy například Microsoft Outlook, Mozilla Thunderbird
 - uživatel zpravidla považuje po odklepnutí tlačítka “Odeslat” zprávu za doručenou



Email z pohledu správce

- mailserver si přes DNS zjistí, kam email doručit a doručí ho cílovému serveru, tedy i schránce
 - MTA (Mail Transfer Agent), například Postfix, Sendmail
 - doručuje se na MX záznamy, případně na A



Email z pohledu správce

- mailserver si přes DNS zjistí, kam email doručit a doručí ho cílovému serveru, tedy i schránce
 - jedno z kritických míst přenosu (filtry obsahu, formality přenosu)
 - protokolem pro přenos emailů je SMTP



Email z pohledu správce

- protokolem pro přenos emailů je SMTP
 - SMTP potkáte tradičně na portu 25/TCP
 - odchozí komunikace přes port 25 bývá blokována kvůli rozesílání spamů, uživatelé by měli používat jiný port (typicky 587)



Email z pohledu správce

- příklad SMTP komunikace

```
220 service2.sh.cvut.cz ESMTP Postfix (Debian/GNU)
HELO Ondrej
250 service2.sh.cvut.cz
MAIL FROM: <ondrej@cecak.cz>
250 Ok
RCPT TO: <info@installfest.cz>
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: <ondrej@cecak.cz>
To: <info@installfest.cz>
Subject: Email

Ahoj, testovaci email.
-- OC
.
250 Ok: queued as E152A138540
QUIT
221 Bye
```



Email z pohledu správce

- protokolem pro přenos emailů je SMTP
 - pozor na hlavičkového vs. obálkového odesílatele
 - email může být odmítnut až do přijetí druhou stranou (250 Ok ...)
 - pozor na “tichou smrt” emailu (spamové karantény a podobně)



Email z pohledu správce

- mailserver si přes DNS zjistí, kam email doručit a doručí ho cílovému serveru, tedy i schránce
 - umístění do schránky zajistí zpravila mailserver na druhé straně
 - do hry vstupuje ještě MDA (Mail Delivery Agent), například procmail, maildrop



Email z pohledu správce

- uživatel si ho ze schránky možná stáhne, pravděpodobně zobrazí
 - známé a oblíbené protokoly POP3, IMAP4
 - webmaily
 - doručení nemusí znamenat, že si uživatel email přečte (spam, ...)



Email z pohledu správce

- uživatelé si na email rychle zvykli, především kvůli jeho vlastnostem => obvykle od vás pak tyto vlastnosti emailů očekávají a možná ještě něco navíc
 - 100% doručitelnost
 - filtry a automatické odpovědi
 - groupware (?)



Postfix



- vznikl v roce 1999 jako “alternativa” k běžně používaným MTA (například populární Sendmail)
- licencován pod IBM Public License (free, open source software; licenčně nekompatibilní s GNU GPL)



Postfix

- původním autorem Wietse Wenema (Nizozemí)
- spolupracoval také na SATAN, TCP Wrapper



Postfix



- výborná dokumentace na webu www.postfix.org
- rychlý
- mocný
- průhledný a bezpečný
- poměrně snadný na správu



Postfix, konfigurace

- `/etc/mailname`
 - jméno mailového systému



Postfix, konfigurace

- `/etc/postfix/master.cf`
 - konfigurační soubory jednotlivých daemonů
 - ladění výkonu
 - integrace filtrů
 - ovlivňování některých mechanismů ovlivňující procházející emaily



Postfix, konfigurace

- `/etc/postfix/main.cf`
- obecné volby:
 - `myhostname`
 - `mydestination`
 - `inet_interfaces`



Postfix, konfigurace

- `/etc/postfix/main.cf`
- obecné volby:
 - `myhostname`
 - jméno poštovního systému
 - `mydestination`
 - lokálně doručované domény
 - `inet_interfaces`



Postfix, konfigurace

- `/etc/postfix/main.cf`
- obecné volby:
 - `myhostname`
 - jméno poštovního systému
 - `mydestination`
 - lokálně doručované domény
 - `inet_interfaces`
 - použitá síťová rozhraní, adresy



Postfix, konfigurace

- `/etc/postfix/main.cf`
- odesílání emailů přes SMTP smarthost
 - předáme email serveru, on si s ním už nějak poradí
 - pozor, možná chceme lokálně doručované emaily
 - `relayhost`
 - smarthost (jméno nebo IP adresa)
 - `mynetworks`
 - sítě, kterým důvěřujeme



Postfix, konfigurace

- `/etc/postfix/main.cf`
- doplnění na kompletní mailový systém
 - vypustíme smarthost
 - přidáme virtuální aliasy



Postfix, konfigurace

- `/etc/postfix/main.cf`
- doplnění na kompletní mailový systém
 - vypustíme smarthost
 - přidáme virtuální aliasy

```
virtual_transport = virtual
virtual_alias_domains = example.com
virtual_alias_maps =
hash:/etc/postfix/virtual
```



Postfix, konfigurace

- `hash:/etc/postfix/virtual`
 - říkáme Postfixu, že použijeme BerkeleyDB
 - po editaci textového souboru databázi vytvoříme pomocí nástroje `postmap`

```
postmastmaster@example.com      postmaster
jana@exaple.com                  jana
info@example.com                 jana,petr@example2.com
@example.com                      kos
```



Postfix, konfigurace

- pár dalších doporučení ke konfiguraci
 - `delay_warning_time = 4h`
 - informace o emailech, které jsou stále ve frontě
 - `unknown_local_recipient_reject_code=550`
 - permanentně odmítat neznámé příjemce
 - `smtpd_helo_required = yes`
 - `strict_rfc821_envelopes = yes`
 - vyžadovat “správnější” SMTP komunikaci



Čemu se vyhnout?

- nebud'te open relay (obecně pozor na spam)



Čemu se vyhnout?

- nebud'te open relay (obecně pozor na spam)
- počítejte s tím, že některé programy maily používají jako komunikační prostředek s uživatelem/správce (například používaná implementace `cronu`)
- pozor na zpětnou doručitelnost (přepisování, lokální pošta z webových skriptů)



