

WEB saugumas

Marius Gžegoževskis

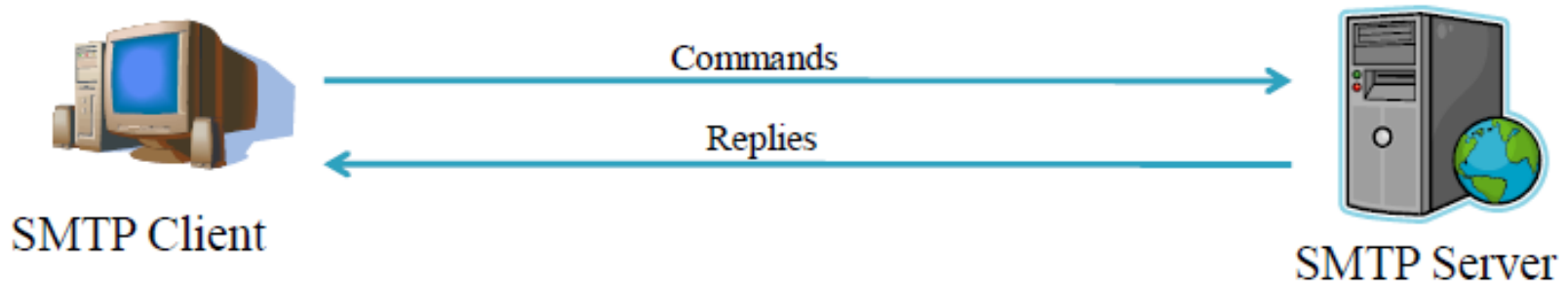


Turinys

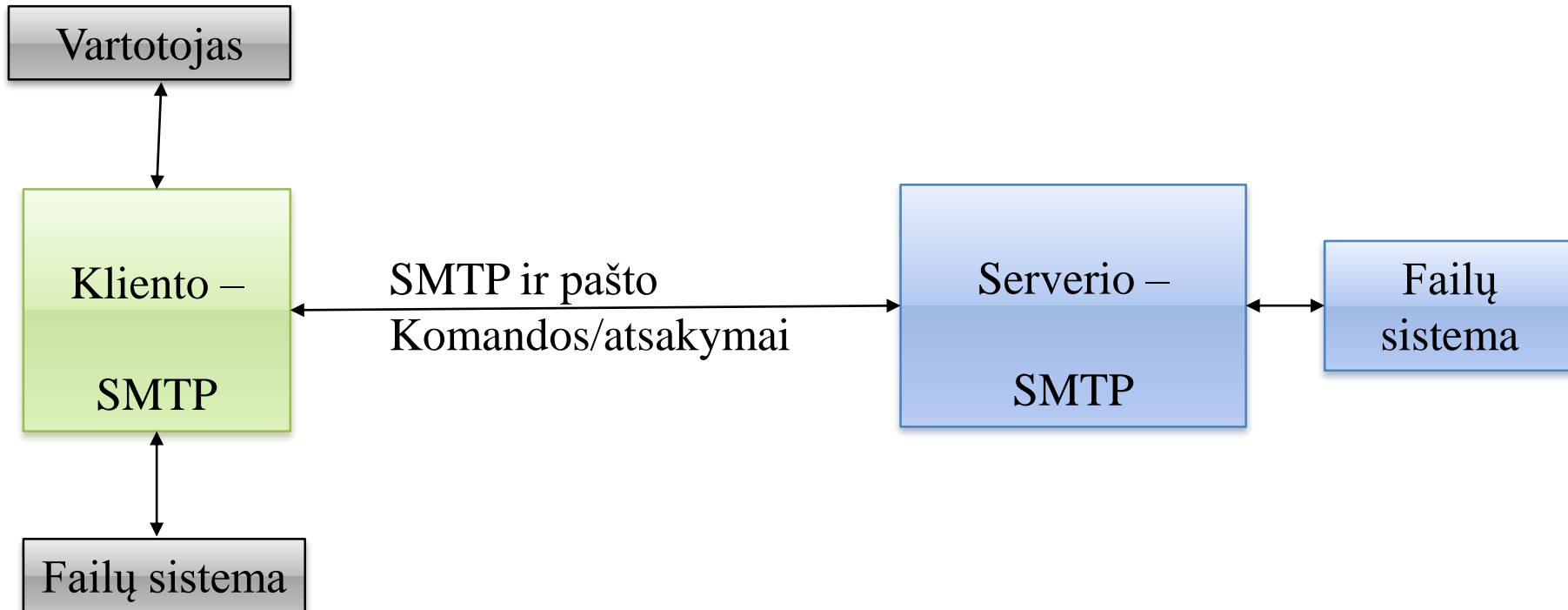
- Elektroninio pašto saugumas:
 - » SMTP (Simple Mail Transfer Protocol) protokolas.
 - » Elektroninio pašto architektūra.
 - » „Anti-spam“ apsisaugojimo metodai.
-

SMTP (angl. Simple Mail Transfer Protocol) protokolas

- Komunikacija tarp vartotojo ir serverio.
- Komunikacijai yra naudojami TCP portai 587 arba 25.



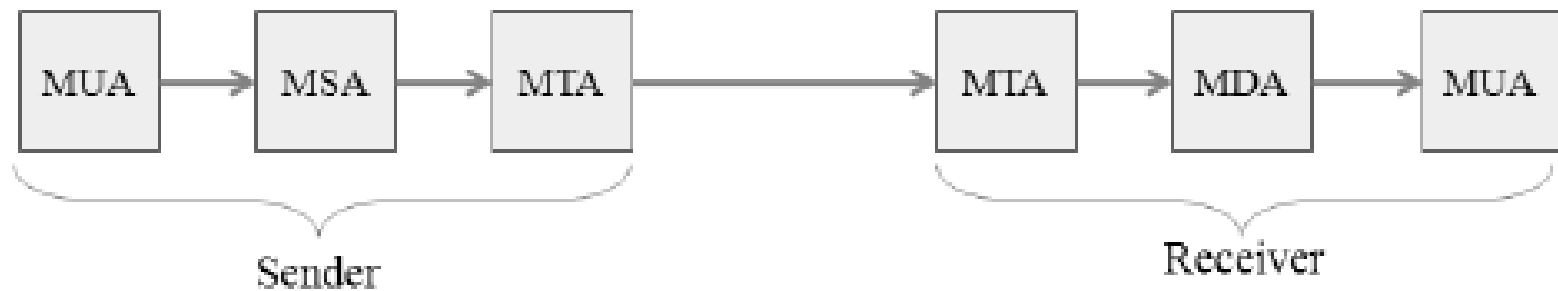
SMTP modelio bazinė struktūra



Elektroninio pašto architektūra

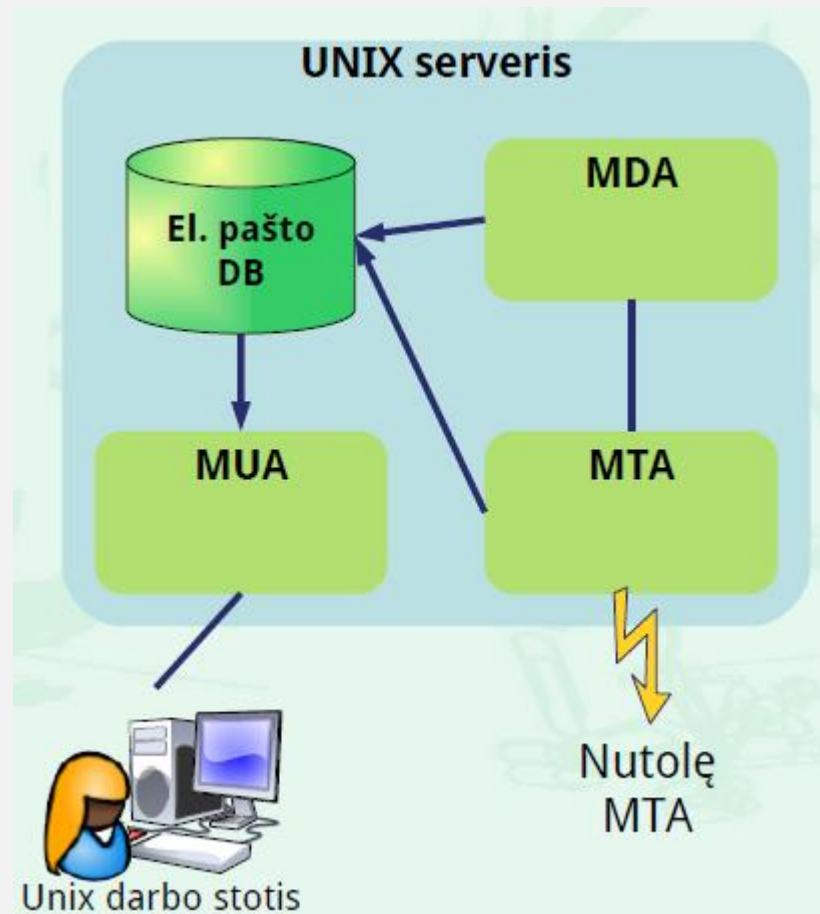
- **MUA** - Mail User Agent. Grafinė vartotojo sąsaja atsakinga už elektroninius laiškus, atsakinga persiųsti žinutę MSA (angl. Mail Submission Agent). Pvz: Eudora, pine, outlook, kmail ir kitos.
 - **MSA** - Mail Submission Agent. Gauna žinutę iš MUA ir perduoda ją MTA. Paprastai yra implementuojama kartu su MTA. MSA gali būti aprašomas saugumo patikrinimas pvz. El. Pašto patikrindama, kad tai nėra nepageidautinas laiškas ar siuntėjas prieš išsiųsdamas tai MTA.
 - **MTA** – Mail Transfer Agent. Sudaro blokus, kurie implementuoja SMTP protokolą. Šis komponentas yra atsakingas už žinučių išsiuntimą ir gavimą. Kai žinutė pasiekia tikslą, MTA išsiunčia žinutę MDA. Pavyzdžiai MTA yra:
 - » Microsoft Exchange Serveris, postfix, sendmail.
 - **MDA** – Mail Delivery Agent. MDA gauna žinutę iš MTA ir perduoda ją į MUA. MDA pavyzdžiai: Procmail ir maildrop.
-

Elektroninio pašto architektūros komponentų sąveika



El. pašto serverio moduliai

- Pašto pristatymo programa
(angl. Mail Delivery Agent – **MDA**)
- Pašto siuntimo programa
(angl. Mail Transfer Agent – **MTA**)
- Pašto vartotojo programa
(angl. Mail User Agent – **MUA**)



Pašto pristatymo programa (MDA)

- Atskira programa, kuri paskirsto laiškus vietiniams sistemos vartotojams.
 - Gali užtikrinti daugybę papildomų funkcijų, kurias tvarkyti dažnai gali administratoriai ir patys vartotojai.
 - Išskviečiama tik tada, kai į el. pašto sistemą patenka laiškas skirtas vietiniam vartotojui.
 - Kai vietinis MTA gauna laišką kuris skirtas vietiniam vartotojui, jis išskviečia MDA ir perduoda jam laišką.
 - MDA nusprendžia ką su laišku toliau daryti, kam ir kaip jį „pristatyti“.
-

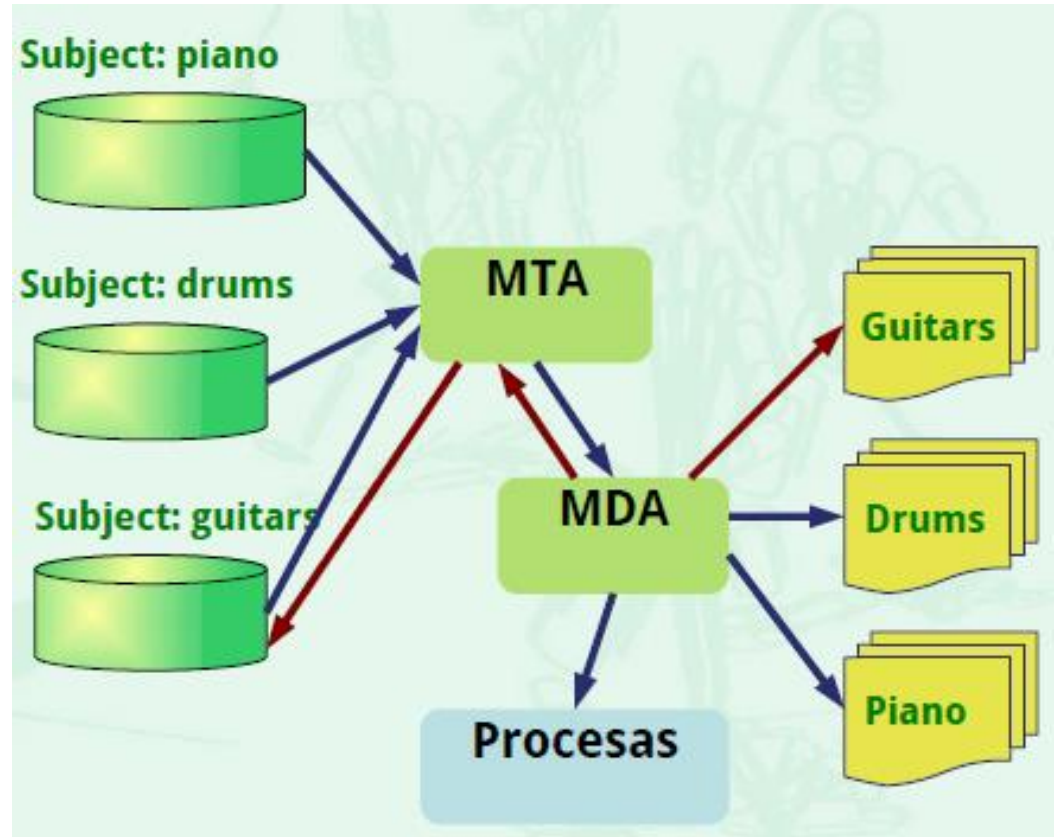
MDA funkcijos

- Patalpina laiškus į atitinkamą DB
 - » /var/spool/mail/xxxx.
 - » \$HOME/mail/xxxx.
 - » Maildir tipo failus ar direktorijas.
 - Kartu gali atlikti papildomą laiškų apdorojimą
 - » Automatinį filtravimą.
 - » Automatinį atsakymą.
 - » Automatinį proceso paleidimą.
-

MDA

Binmail

- » Procmail
- » \$HOME/.procmailrc



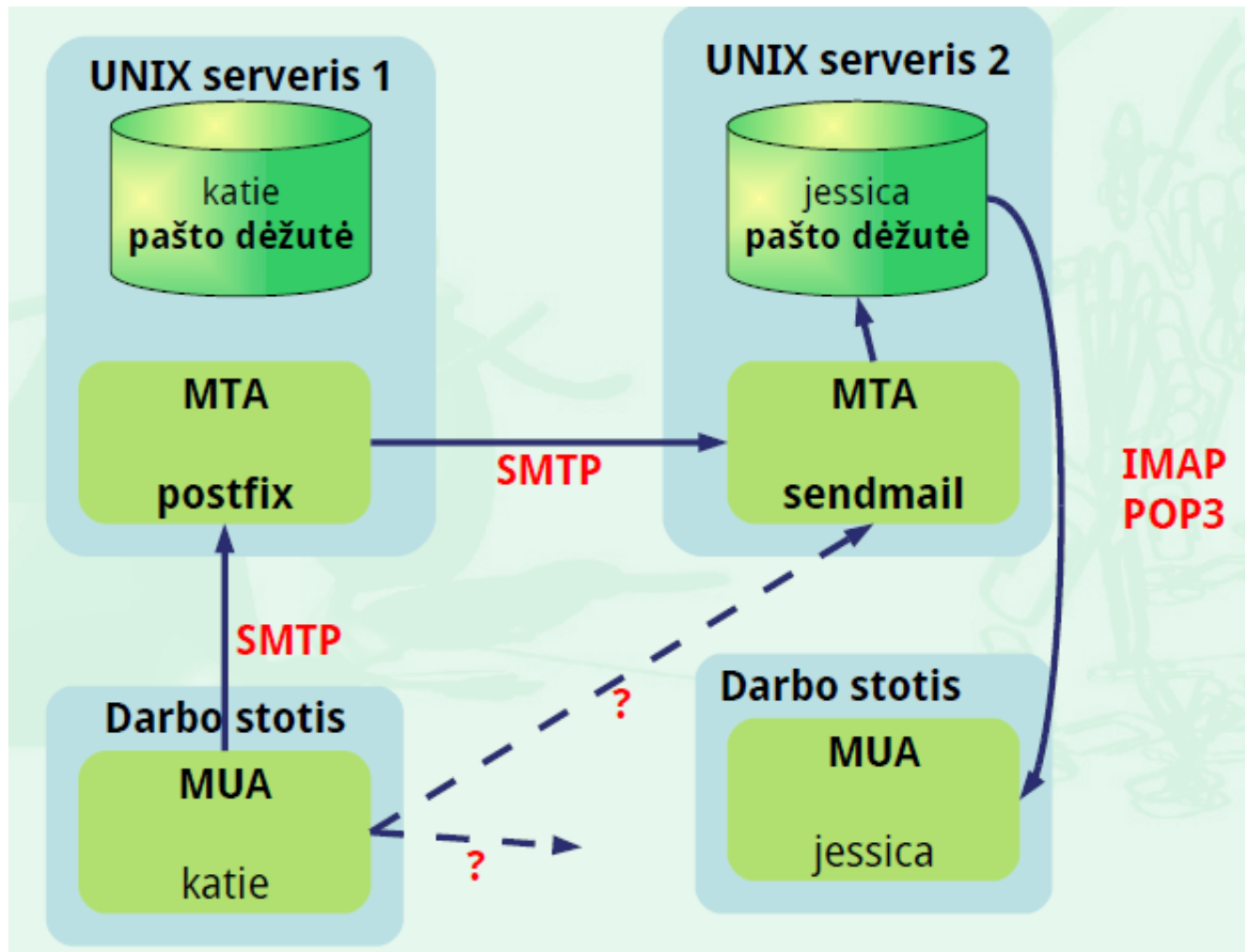
MTA

- Pašto siuntimo programa (MTA) atsakinga už įeinančio ir išeinančio pašto apdorojimą
 - Kiekvienam **išeinančiam** pranešimui ji nustato gavėjo serverio adresą
 - » Jei tai vietinis adresas – laišką perduoda MDA arba iškart įrašo į vartotojo pašto dėžutę (prieš tai gali patikrinti .forward failą)
 - » Jei laiškas skirtas išoriniam vartotojui, jis sužino to vartotojo pašto serverio (SMTP) adresą ir laišką persiunčia jam
 - MTA turi **priimti** pranešimus iš kitų MTA serverių ir po to juos apdoroti taip pat kaip ir išeinančius pranešimus
 - » Bendru atveju nėra ribojimo kokie MTA gali jungtis ir kokius pranešimus jie gali siųsti
 - Tai kritinė laiko ir saugos požiūriu serverio dalis
 - » Sendmail, qmail, postfix, ...
-

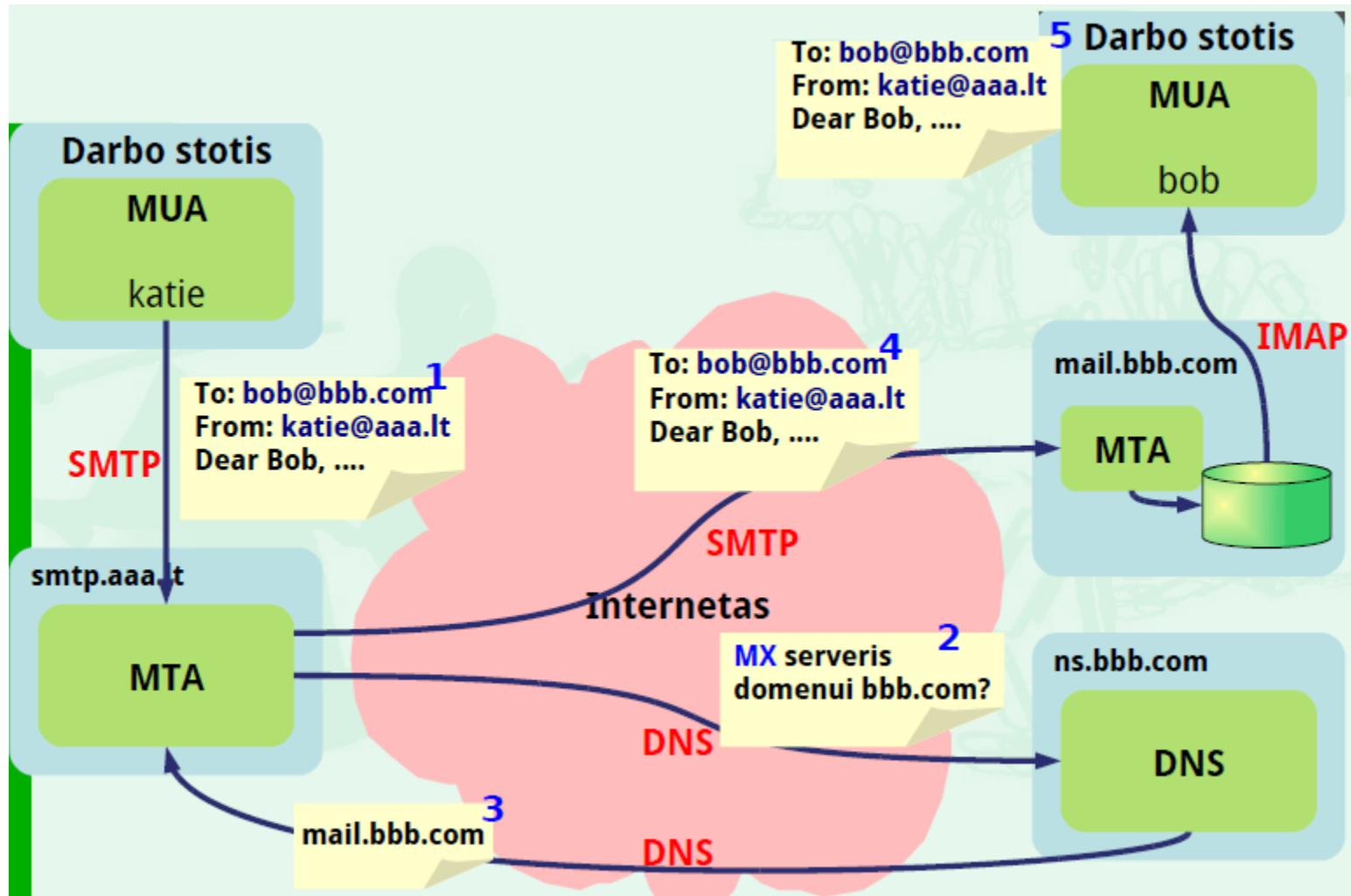
MUA

- UNIX sistemoje kiekvienas vartotojas turi savo asmeninę DB (pašto dėžutę) kurioje saugomi jo laiškai
 - Pašto vartotojo programa (MUA) užtikrina patogią vartotojo sąsają su jo pašto dėžute
 - » MUA tiesiog patogiai parodo kokie laiškai saugomi vartotojo dėžutėje
 - » Kartais leidžia susikurti daugiau DB
 - » Bindmail, pine, Kmail
 - Dabar naudojami nutolę MUA
 - Kur saugoti laiškus?
 - » Serveryje?
 - » Darbo stotyje?
 - » Vieta serveryje prieš darbą iš keleto darbo stočių
-

Nutolę vartotojai



Kaip veikia MTA



SMTP sesija, pvz.

```
telnet smtp.ktu.lt 25

220 aaa.ktu.lt ESMTP Postfix
helo 78-57-171-78.static.zebra.lt
250 aaa.ktu.lt
mail from: aaa@takas.lt
250 Ok
rcpt to: aaa@ktu.lt
250 Ok
data
354 End data with <CR><LF>.<CR><LF>
Labas
Kaip gyvenimas
.
250 Ok: queued as C529011401A5
quit
221 Bye
Connection to host lost.
```

SMTP atsakymo kodai

- Į kiekvieną komandą SMTP serveris atsako triženkliais kodais ir tekstiniu paaiškinimu.
 - Kodų reikšmės:
 - 2: Serveris komandą sėkmingai įvykdė.
 - 3: Serveris komandą suprato, bet laukia daugiau duomenų, kad galėtų ją užbaigti.
 - 4: Laikina serverio klaida (angl. temporary failure). Jei po kurio laiko komanda bus pakartota be jokių pakeitimų ji gali būti sėkmingai įvykdyta.
 - 5: Klaida.
 - Pavyzdžiui:
 - » **451** - Greylisted, please try again in 900 seconds.
 - » **450** - The requested command failed because the user's mailbox was unavailable (for example because it was locked). Try again later.
 - » **452** - The command has been aborted because the server has insufficient system storage.
-

Pavojingos SMTP komandos

- Kartais piktavaliai gali pasinaudoti standartinėmis SMTP protokolo komandomis ir „išgryninti“ savo sąrašus arba „atspėti“ realius vartotojus.

```
telnet smtp.oksl.ktu.lt 25
ehlo as
...
vrfy <postmaster>
502 VRFY command is disabled
expn <postmaster>
502 Error: command not implemented
mail from: aaa@aaa.lt
250 Ok
rcpt to: root
250 Ok
rcpt to: postmaster
250 Ok
rcpt to: alex
550 <alex>: Recipient address rejected: User unknown
```

Pristatymo būsenos pranešimai

- Pristatymo būsenos pranešimas (angl. Delivery Status Notification – DSN) arba „atšokęs“ laiškas (angl. Bounce) – pašto sistemos automatiškai sugeneruotas laiškas, pranešantis laiško siuntėjui, jog jo laiškas nebuvo pristatytas:
 - » Gali būti gautas iš siuntėjo MTA arba iš gavėjo MTA.
 - » Kai MTA priima laišką pristatymui, jis tampa atsakingas ir už tai jog nepristatymo atveju apie tai informuotų siuntėją.
 - » SMTP protokolas vienareikšmiškai reikalauja, kad apie kiekvieną nepristatytą laišką būtų informuojamas jo siuntėjas.
 - » Praktikoje kartais taikomas (ir tai laikoma priimtiniu metodu kovojant su UCE) laiškų „išmetimas“ be siuntėjo informavimo, bet tai yra labai pavojinga ir pažeidžia reikalavimą, kad kiekvienas laiškas yra arba pristatomas arba pranešama apie jo nepristatymą.
-

Saugos problemos

SMTP protokolo problemos

- » Perduodama atviru tekstu naudojant atvirą Internetą.
 - » Bet koks SMTP serveris priima prisijungimus be autentifikacijos ir autorizacijos.
 - » Bendru atveju netikrinamas nei siuntėjo nei gavėjo adresas.
 - Atviri SMTP serveriai (angl. Open Relay).
 - Nepageidaujami komerciniai laiškai (angl. Unsolicited Commercial Email – UCE).
 - Virusai
 - » Patys siunčia laiškus, taip save platindami.
 - » Gali būti persiunčiami vartotojų kaip (kartu su) programinė įranga.
-

Persiuntimas (Relaying)

- Procesas, kurio metu el. pašto serveris (MTA) automatiškai persiunčia laišką gautą iš **nutolusio** kliento į **kitą** serverį (ne save) vadinamas persiuntimu (angl. Relaying)
 - » Atviri SMTP serveriai (angl. Open relay) dominavo paslaugos vystymosi pradžioje
 - » Vartotojas galėjo pasinaudoti bet koku serveriu ir pasiųsti laišką
 - » Dabar jie naudojami nepageidaujamiems komerciniams laiškam (angl. unsolicited commercial e-mail – UCE) siųsti
 - » Dažnai slepia siuntėjo adresą, nes siekia išvengti (įstatyminio) persekiojimo
-

Laiškų antraštės

- Administratorius turi atsakyti, kaip ir kodėl laiškas pateko pas vartotoją, kodėl pavėlavo, kodėl neatėjo išvis, ...
 - RFC 5322 numato laiškų antraščių naudojimą
 - » <lauko_pav>:<kūnas>CRLF
 - » Sintaksiškai privalomi laukai tik du:
Data (Date:) ir siuntėjas (From:, Sender:, Reply-To:)
 - Nebūtini laukai
 - » To: Cc: Bcc: From: Subject:
 - » Received: Delivered-To: Return-Path:
-

Laiškų antraštės

Received:


from host_name
by host_name
via physical_path
with protocol
id message-id
for final_e-mail_dest

Laiško kelias iki adresato

- RFC numato jog kiekvienas MTA persiunčiantis laišką privalo pridėti Received: lauką. Be to jis negali keisti kitų Received: laukų jau esančių laiške
- MTA kuris pristato laišką savo vartotojui prideda Delivered-To: lauką

Return-Path: <nerijus@takas.lt>
Delivered-To: nerijus@vil.ktu.lt
Received: from diedas.soften.ktu.lt (diedas.soften.ktu.lt [193.219.33.197])
by pegasas.vil.ktu.lt (Postfix) with ESMTP id AA17D11401AC
for <nerijus@vil.ktu.lt>; Fri, 17 Sep 2010 11:29:44 +0300 (EEST)
Received: from localhost (localhost [127.0.0.1])
by diedas.soften.ktu.lt (Postfix) with SMTP id 9D35EBF99FC
for <nerijus@vil.ktu.lt>; Fri, 17 Sep 2010 11:29:07 +0300 (EEST)
Message-Id: <20100917082907.9D35EBF99FC@diedas.soften.ktu.lt>
Date: Fri, 17 Sep 2010 11:29:07 +0300 (EEST)
From: nerijus@takas.lt

Ką pasakė HELO sakinyje



Laiško tekstas

Antraščių klastojimas

- Piktavaliai klastoja From: lauką
- Galima suklastoti net ir To: lauką!

```
220 aaa.ktu.lt ESMTF Postfix
helo zebra.lt
250 aaa.ktu.lt
mail from: piktavalis@spam.org
250 Ok
rcpt to: nermork@ktu.lt
250 Ok
data
354 End data with <CR><LF>.<CR><LF>
From: jonaitis@ktu.lt
To: petraitis@zebra.lt
Subject: Suklastotas laishkas
Labas
Kaip gyvenimas
.
250 Ok: queued as C529011401A5
quit
221 Bye
```

```
HELO mta.cloud7.ex
MAIL FROM: <bob@cloud7.ex>
RCPT TO: <alice@wonderland.ex>
```

MAIL FROM | Return-Path

Prarandamas
pristačius

SMTP envelope

```
From: bob@cloud7.ex
To: alice@wonderland.ex
Subject: Let's go out tonight
```

message header

Hi Alice!

message body

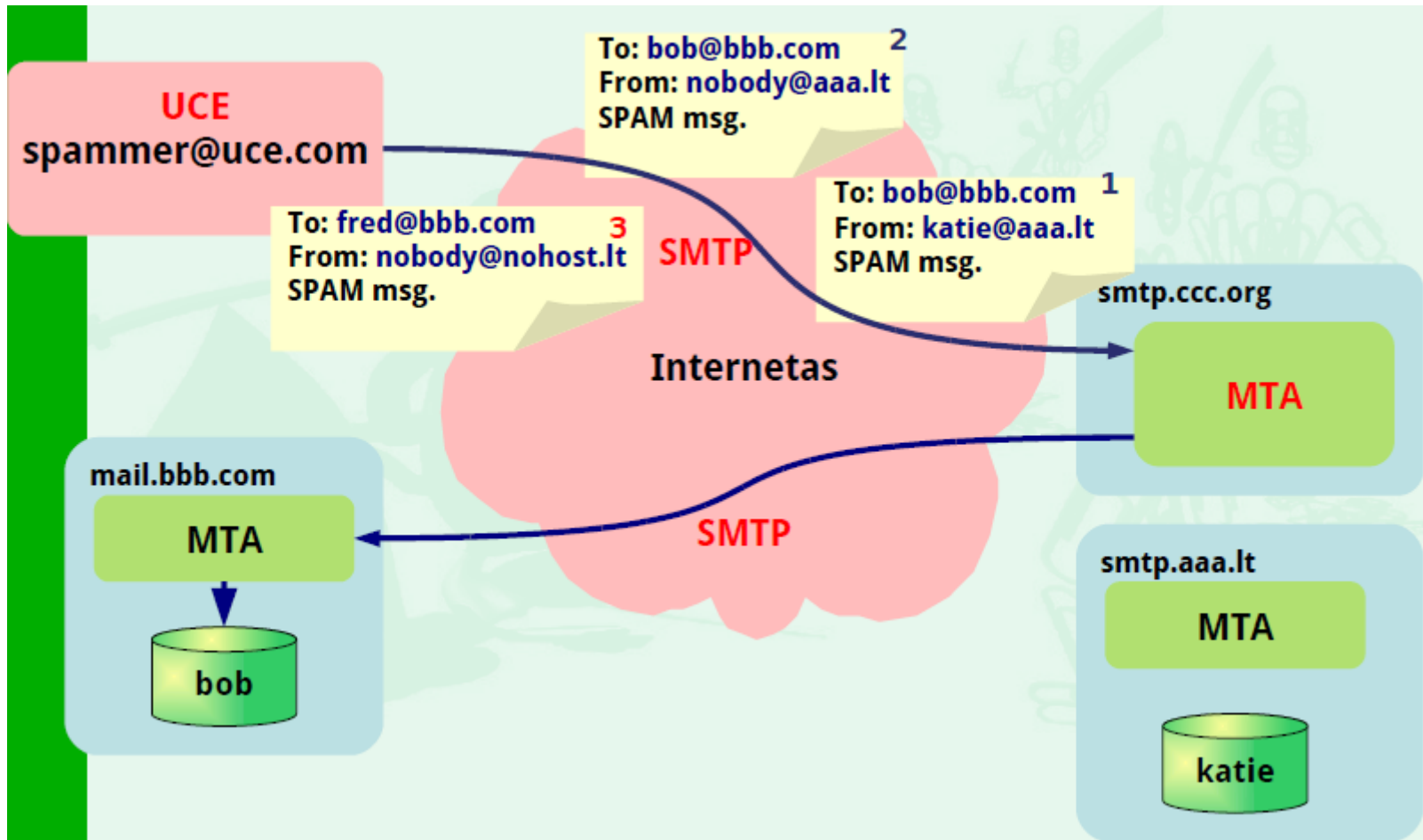
Do you want to go out tonight?
Let's meet at Charlie's at 6pm.

Love, Bob.

Kaip atrodo KTU pašto sistemoje:

```
Data:    Fri, 17 Sep 2010 11:57:47 +0300
Nuo:     jonaitis@ktu.lt Lithuania
Kam:     petraitis@zebra.lt
Tema:    Suklastotas laishkas
```


Atviras SMTP serveris (Open Relay)



POP3 protokolas

- **POP3** (angl. **Post Office Protocol Version 3**) – trečios versijos protokolas, naudojamas elektroninių laiškų gavimui iš serverio. Paprastai yra naudojamas kartu su SMTP protokolu.
 - Ankstesnės protokolo versijos (POP, POP2) paseno.
 - POP3 protokolo standartas yra apibrėžtas RFC 1939. Išplėtimai ir autorizacijos metodai apibrėžti RFC 2195, RFC 2449, RFC 1734, RFC 2222, RFC 3206, RFC 2595.
 - Egzistuoja POP3-serverių versijos palaikančios TLS ir SSL.
 - Alternatyviu elektroninių laiškų surinkimo protokolu gali būti IMAP.
-

POP3 seanso būsenos

POP3 protokole yra numatytos 3 seanso būsenos:

1. Autorizacija

» Klientas atlieka autorizacijos procedūrą.

2. Tranzakcija

» Klientas gauna informacija apie elektroninės pašto dėžutės būseną, priima ir pašalina paštą.

3. Atnaujinimas

» Serveris ištrina pasirinktus laiškus ir nutraukia susijungimą.

IMAP protokolas

- IMAP (angl. *Internet Message Access Protocol*) – elektroninio pašto serverio protokolas. Šis protokolas reglamentuoja elektroninių laiškų laikymą ir tvarkymą serverio kompiuteryje, neatsiunčiant jų į gavėjo kompiuterį.
 - Naudojant IMAP protokolą vietoj POP protokolo, nereikia vietos laiškam gavėjo kompiuterio diske ir galima iš bet kurios vietos tvarkyti savą paštą – sukurti aplankus ir laikyti juose laiškus, dirbti su laiškų juodraščiais ir atlikti kitus veiksmus. Pakanka turėti tik prieigą prie interneto. Darbas su IMAP serveriu per modemą gali būti spartesnis negu su POP serveriu dėl to, kad peržiūrėjimui galima parsisiųsdinti tik laiškų antraštes. Galima paieška žinučių tekstuose jų neatsiunčiant (serverio pusėje). Saugumui padidinti perduodami slaptažodžiai gali būti šifruojami.
-

IMAP protokolas

- IMAP yra naujesnis ir didesnes galimybes turintis protokolas, tačiau IMAP serverius turi ne visi elektroninio pašto paslaugų teikėjai.
 - IMAP protokolas nenaudojamas laiškams išsiųsti. Laiškai dažniausiai išsiunčiami naudojant SMTP protokolą ar kitokį metodą.
 - IMAP paprastai naudoja TCP/IP ryšio tipą. Šio protokolo standartinis porto numeris yra 143.
-

Apsauga nuo nepageidaujamų laiškų (angl. Anti-spam)

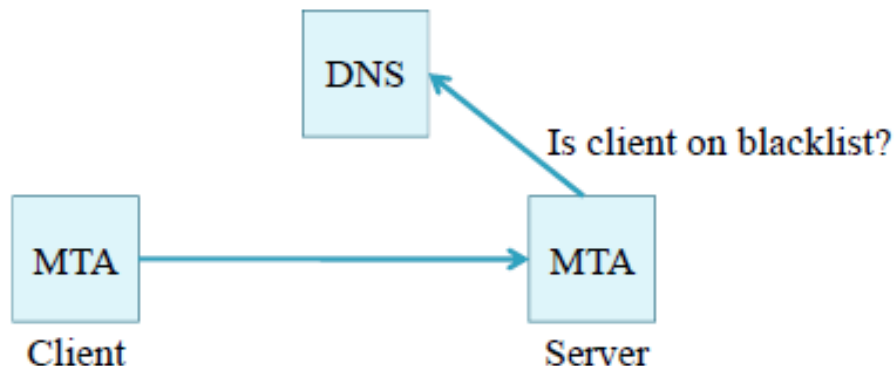
- Apie 100 milijardų „spam“ elektroninių laiškų yra išsiunčiama per dieną.
 - Keletas apsisaugojimo būdų, kaip kovoti su nepageidaujamais elektroniniais laiškais.
 - Nepageidaujami laiškai gali būti filtruojami arba blokuojami.
 - Apsisaugojimo metodai:
 - » DNS Blacklists (DNSBL) .
 - » Greylisting ir nolistig.
 - » Hashcash.
 - » Statistical Filters.
 - » Hybrids.
-

DNSBL

- DNS blacklists (juodieji sąrašai), dar vadinami DNS blokuojamieji sąrašai:
 - » Dar kitaip žinomi RBL (Realtime Blacklist).
 - IP adresų esančių juodajame sąrašė, kuriuos priskiria tiekėjas yra blokuojami, kovojant su nepageidaujamais laiškais.
-

DNSBL

- Serverio MTA gali patikrinti ar kliento MTA yra juodajame sąraše.



- Jeigu klientas yra juodajame sąraše, serveris gali imtis tam tikrų veiksmų kovojant su nepageidaujamais laiškais:
 - » Gali būti naudojama „angl. spam scoring system“.

DNSBL

- Lengva naudotis – IP adresai gali būti tikrinami naudojant DNS užklausas.

`IP(r).dnsbl.server.com`

- IP(r) - tai atvirkštinė bitų grupavimo tvarka skirta tikrinamajam IP adresui.
 - Keletas pavyzdžių: spamhaus, spamcop ir t.t.
-

DNSBL

- Keletas IP adresų gali būti blokuojami vieno juodojo sąrašo, bet negali būti blokuojamas kito juodojo sąrašo.
- Pavyzdys: Tikrinam IP 209.237.225.253

```
>nslookup 253.225.237.209.zen.spamhaus.org
Server:      ***
Address:     ***

**Server can't find 253.225.237.209.zen.spamhaus.org: NXDOMAIN

>nslookup 253.225.237.209.spam.dnsbl.sorbs.net
Server:      ***
Address:     ***

Non-authoritative answer:
Name: 253.225.237.209.spam.dnsbl.sorbs.net
Address: 127.0.0.6
```

DNSBL

Privalumai:

- » Galimybė pasirinkti juodąjį sąrašą pagal savo poreikį.
 - » „Aggressive lists“ - šio tipo juodasis sąrašas apsaugo nuo daugelio žinomiausių nepageidaujamų elektronio pašto „spamerių“, bet taip pat atmeta ir keletą teisėtų elektroninių paštų.
 - „Conservative lists“ – praleidžia keletą „spamerių“, bet mažesnis šansas atmesti teisėtus elektroninio pašto laiškus.
 - Žinutė gali būti atmetama prieš išsiunčiant, iki tol kol serveris neužmezga ryšio su klientu.
 - **Pastabos:**
 - » Tas pats pašto serveris gali būti naudojamas tiek teisėtų vartotojų tiek „spamerių“.
 - » Jei per klaidą patenkat į juodąjį sąrašą, gali būti labai sudėtinga iš jo ištrūkti.
-

Greylisting

- Daugelis spam programų nepilnai veikia su SMTP protokolu.
 - » Šios programos nevisada atlieka pakartotinį laiško persiuntimą į elektroninį paštą kuris atmetė siunčiamą laišką.
 - Idėja: Visada atmesti neatpažįstamas tranzakcijas.
 - Įeinančioms žinutėms, peržiūrėti:
 - » Angliškai: (SMTP Client IP, sender address, receiver address).
 - » Lietuviškai: (SMTP Kliento IP, siuntėjo adresą, gavėjo adresą).
 - Jeigu prieš tai nebuvo naudotas, tada išsaugoti duomenų bazėje ir laikinai atmesti žinutę (Transient Negative Completion reply).
 - Jeigu dažnai naudotas tada priimti žinutę.
-

Greylisting

- **Privalumai:**

- » Lengva panaudoti ir nereikalauja daug papildomų resursų palyginimams, lyginant su kitais metodais.
- » Gali būti naudojamas prieš kitus „spamo filtrus“ taip sumažinantis kitų filtrų apkrovą.

- **Pastabos:**

- » Elektroninis paštas nebėra „realaus laiko“, kadangi yra taikomas šis filtras kaip tarpinis komponentas laiško išsiuntimui.
-

Nolisting

- Daugelis spam programų nepilnai veikia su SMTP protokolu.
 - » Daugelis spamerių taikinyis yra aukščiausio prioriteto serveriai. Kadangi pašto serveriai gali turėti duomenų kopijų serverius ar kitos paskirties, kurie yra skirstomi pagal prioritetą.

```
server.com:  
10 dummy.server.com  
20 real1.server.com  
20 real2.server.com  
30 real3.server.com
```

Nolisting

- **Idėja.** Serveris su aukščiausiu prioritetu yra neegzistuojantis.
 - Taigi spameriai bandydami siųsti laišką į serverį turintį aukščiausią prioritetą, nieko nepasieks.
 - Dar viena iš spamerių strategijų yra naudoti atvirkštinį metodą siųsti į žemiausio prioriteto serverį. Taigi kitas sprendimas būtų:
 - » Naudoti netikrus serverius, gali būti ir labai prastas kompiuteris, į kurį nėra uždrausta siųsti bet kokią nepageidaujamą šlamštą.
-

Hybrid filters

Hibridiniai filtrai. Keletas arba visi prieš tai aptarti, taip pat daugelis kitų filtravimo metodų gali būti apjungiami į vieną.

- Praėję ar nepraėję testus, gali būti priskiriamas balas, pagal kurį vėliau yra atliekama priėmimo kaip teisėtą elektroninį laišką ar pripažinimo kaip šlamštą (angl. Spam).
 - » Jeigu balas yra aukštesnis nei yra nurodytas iš anksto, tada elektroninis laiškas yra laikomas kaip šlamštas (angl. Spam).
 - » Atviro kodo implementacija yra „SpamAssassin“.
 - » Gali būti naudojama MTA, MDA ir/arba MUA.
-