# ПРОТОКОЛЫ ЭЛЕКТРОННОЙ ПОЧТЫ

SMTP — Simple Mail Transfer Protocol

RFC 821 — август 1982, ..., RFC 5321 — октябрь 2008,
RFC 5336 — поддержка utf-8 в адресах (2007)

Internet Message Format

RFC 822 — август 1982, ..., RFC 5322 — октябрь 2008,
RFC 5335 — поддержка utf-8 в заголовках (2007)

POP3 — Post Office Protocol

RFC 1081 — ноябрь 1988, ..., RFC 1939 — май 1996,
RFC 2449, ... — расширения POP3 (1998)

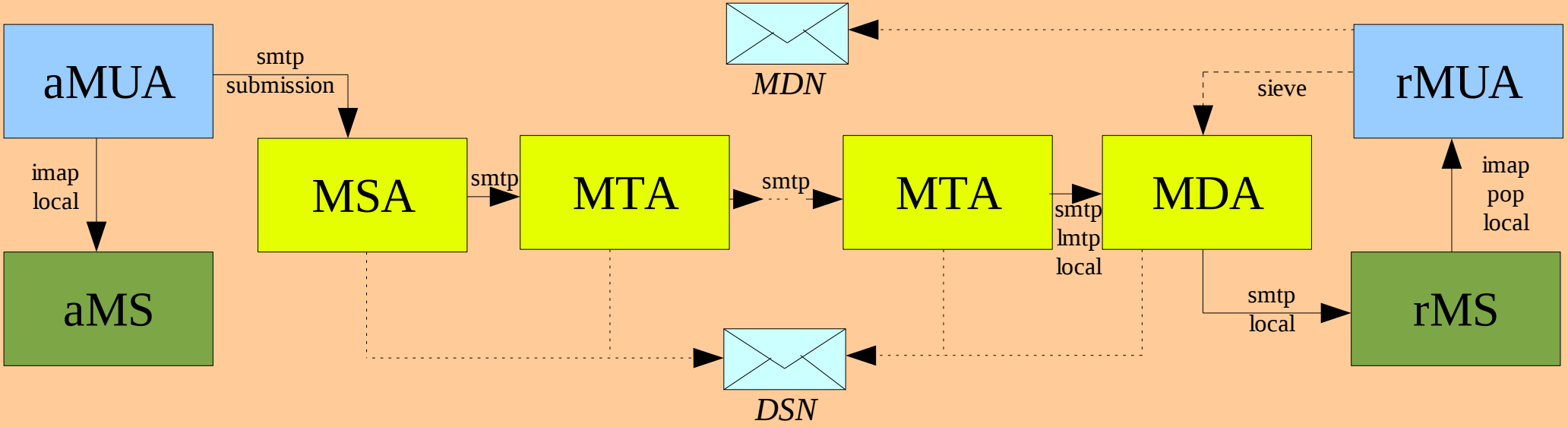
IMAP4 — Internet Message Access Protocol

RFC 1730 — декабрь 1994, ..., RFC 3501 — март 2003,
RFC 4466, 4469, 4551, 5032, 5182, 5738, ... — расширения

© Петрозаводский госуниверситет, А. В. Соловьев, А. П. Мощевикин, 2003-2010

# СХЕМА ТРАНСПОРТА Э-ПОЧТЫ

## RFC 5598 — Internet Mail Architecture (июль 2009)




«a» = author's (отправитель), «r» = recipient's (получатель)

MUA = Message User Agent (например, Thunderbird, The Bat, ...)
MS = Message Store (например, mbox, maildir)
MSA = Message Submission Agent (например, postfix, exim4, ...)
MTA = Message Transfer Agent (например, postfix, exim4, ...)
MDA = Message Delivery Agent (например, cyrus, procmail, ...)
MRA = Message Retrieval Agent (например, fetchmail)

*DSN = Delivery Status Notification* (получатель — SMTP.MailFrom)
*MDN = Message Disposition Notification* (получатель — Disposition-Notification-To)

© Петрозаводский госуниверситет, А. В. Соловьев, А. П. Мощевикин, 2003-2010

# СХЕМА ТРАНСПОРТА Э-ПОЧТЫ

## Message User Agent:

- отображение и редактирование текста письма;
- формирование заголовков RFC 5335;
- SMTP-клиент для вз.д. с MSA/MTA;
- Message Retrieval Agent (POP-, IMAP-клиент)

## Message Submission Agent:

SMTP, порт 587

- авторизация и аутентификация;
- проверка всех заголовков, модификация, добавление (доменные имена,обязательные заголовки, ...);
- применение локальных политик

RFC 4409 (апрель 2006)

## Message Transfer Agent:

SMTP, порт 25

- релей (передача почты на другой SMTP-сервер на основе MX-записи DNS);
- приём входящей почты;
- тело письма не модифицируется, только добавляются trace-заголовки (Received)

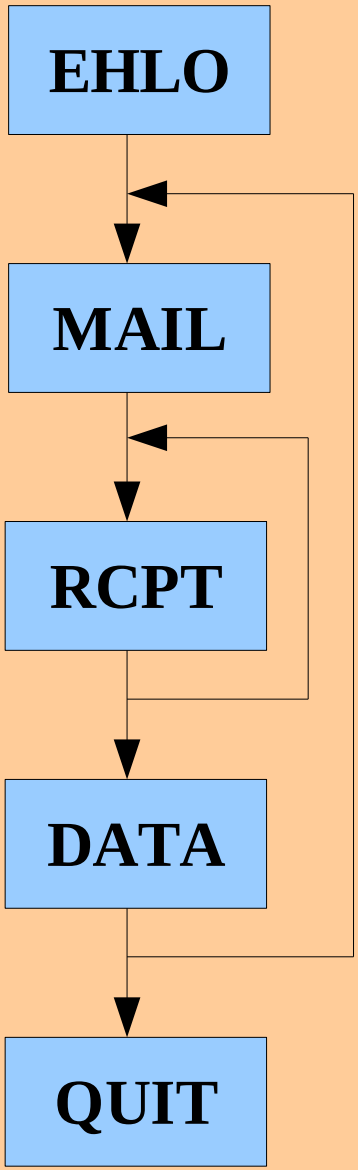
## Message Delivery Agent:

- помещение сообщения в почтовый ящик пользователя;
- добавлется заголовок Return-Path и последний Received;
- перенаправление письма, применение локальных политик

© Петрозаводский госуниверситет, А. В. Соловьев, А. П. Мощевикин, 2003-2010

# ОСОБЕННОСТИ ПРОТОКОЛА SMTP

RFC 5321 — Simple Mail Transfer Protocol (октябрь 2008)




Назначение: транспортировка сообщений э-почты (MSA/MTA).

В сеансе SMTP может передаваться несколько сообщений (MAIL x*N*) для многих получателей (RCPT x*N*).

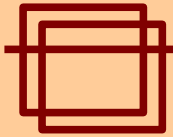
Возможна транспортировка почты непосредственно от хоста отправителя на хост получателя либо через промежуточные хосты.

Очередной SMTP-хост в цепочке определяется по DNS-записи MX.

При прохождении через SMTP-хост добавляется заголовок Received. Кроме того, MDA добавляет Return-Path.

© Петрозаводский госуниверситет, А. В. Соловьев, А. П. Мощевикин, 2003-2010

# КОМАНДЫ SMTP



`EHLO/HELO` *`host`*
— начало сеанса, приветствие и идентификация клиента

`MAIL FROM:<`*`reverse-path`*`>`
— начало транзакции, адрес отправителя

`RCPT TO:<`*`forward-path`*`>`
— адрес получателя

`DATA`
— тело сообщения (RFC 5322 — IMF), заканчивается <CRLF>.<CRLF>

`HELP` *`[command]`*
— подсказка по командам

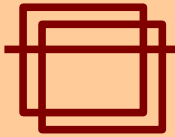
`RSET`
— прервать транзакцию

`NOOP`
— пустая операция

`QUIT`
— завершение сеанса

© Петрозаводский госуниверситет, А. В. Соловьев, А. П. Мощевикин, 2003-2010

# ОТКЛИКИ SMTP



В ответ на каждую команду сервер генерирует численный отклик. Клиент не должен посылать новую команду, пока не получит отклик на предыдущую (исключение: RFC 2920 - Pipelining).

2yz — положительный окончательный отклик

```
220  <domain> Service ready
221  <domain> Service closing transmission channel
250  Requested mail action okay, completed
251  User not local
```

3yz — положительный промежуточный отклик

```
354  Start mail input; end with <CRLF>.<CRLF>
```

4yz — временный отрицательный отклик

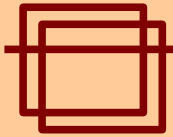
```
421  <domain> Service not available
450  Requested mail action not taken: mailbox unavailable
```

5yz — постоянный отрицательный отклик

```
500  Syntax error
503  Bad sequence of commands
551  User not local
```

© Петрозаводский госуниверситет, А. В. Соловьев, А. П. Мощевикин, 2003-2010

# ПОЛУЧАТЕЛИ



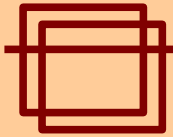
Получатели сообщения определяются MUA по задаваемым пользователем IMF-заголовкам:

| | |
|---|---|
| `To:` | - основные получатели |
| `Cc:` | - копии (carbon copy) |
| `Bcc:` | - скрытые копии (blind carbon copy) |

Любой из этих заголовков может содержать список адресов, разделённых запятой. Для каждого получателя должна быть сгенерирована отдельная команда RCPT, а содержимое заголовка Bcc должно быть очищено (или удалён сам заголовок). MTA не анализирует тело письма на предмет получателей. Эта задача возлагается на MUA или MSA.

© Петрозаводский госуниверситет, А. В. Соловьев, А. П. Мощевикин, 2003-2010

# ПРИМЕР SMTP-СЕАНСА



Сервер (S) пассивно ожидает соединения на TCP-порт 25
Клиент (C) инициирует соединение на TCP-порт 25 SMTP-сервера

```
S: 220 mail.server.ru SMTP ready
C: HELO my.domain.name
S: 250 mail.server.ru
C: MAIL FROM:<alex@alpha.ru>
S: 250 OK
C: RCPT TO:<boris@beta.ru>
S: 250 OK
C: RCPT TO:<paul@beta.ru>
S: 550 No such user here
C: RCPT TO:<paula@beta.ru>
S: 250 OK
C: DATA
S: 354 Start mail input; end with <CRLF>.<CRLF>
C: Blah blah blah...
C: ...etc, etc, etc.
C: <CRLF>.<CRLF>
S: 250 OK
C: QUIT
S: 221 mail.server.arpa Service closing transmission channel
```

© Петрозаводский госуниверситет, А. В. Соловьев, А. П. Мощевикин, 2003-2010

# ФОРМАТ СООБЩЕНИЙ Э-ПОЧТЫ

**RFC 5322 — Internet Message Format (2008)**

- Ограничение 998/78
- Заголовки CRLF CRLF Тело
- «Сгибание» заголовков (folding)
- Формат адреса: John Smith <john@foobar.com>
- Формат даты: Mon, 31 Jun 2010 16:43:38 +0600
- Стандартные заголовки, их назначение и синтаксис

**MIME — Multipurpose Internet Mail Extensions**

- RFC 2045 (MIME Part 1, 1996): заголовки Content-Type, Content-Transfer-Encoding (8bit, base64, quoted-printable)
- RFC 2046 (MIME Part 2, 1996): общие описания типов для Content-Type, в том числе «multipart»

© Петрозаводский госуниверситет, А. В. Соловьев, А. П. Мощевикин, 2003-2010

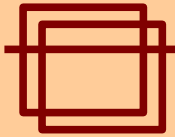
# ПРИМЕР IMF-СООБЩЕНИЯ

```
Return-path: <testing@mail.ru>
Envelope-to: somebody@dfe3300.karelia.ru
Delivery-date: Thu, 18 Apr 2002 09:19:13 +0400
Received: from mx10.mail.ru (mx10.mail.ru [194.67.57.20])
  by dfe3300.karelia.ru (8.9.0/8.9.0) with ESMTP id JAA02601
  for <somebody@dfe3300.karelia.ru>; Thu, 18 Apr 2002 09:19:13 +0400
Received: from mail by mx10.mail.ru with local (Exim FE.5)
  id 16y46o-000CfY-00
  for somebody@dfe3300.karelia.ru; Thu, 18 Apr 2002 09:05:26 +0400
Received: from [213.59.200.7] by win.mail.ru with HTTP;
  Thu, 18 Apr 2002 09:05:26 +0400
From: "Testing" <testing@mail.ru>
To: somebody@dfe3300.karelia.ru
Subject: For testing purposes only
Mime-Version: 1.0
X-Mailer: mPOP Web-Mail 2.19
X-Originating-IP: [213.59.200.7]
Date: Thu, 18 Apr 2002 09:05:26 +0400
Reply-To: "Testing" <testing@mail.ru>
Content-Type: text/plain; charset=koi8-r
Content-Transfer-Encoding: 8bit
Message-Id: <E16y46o-000CfY-00@f5.mail.ru>
X-UIDL: 74fb663e2be8352b3a0b88ca08030c1e

Тестовое сообщение.
```

© Петрозаводский госуниверситет, А. В. Соловьев, А. П. Мощевикин, 2003-2010

# БЕЗОПАСНОСТЬ Э-ПОЧТЫ



**Шифрование SMTP-сеансов**

- команда STARTTLS
- пользователь может требовать шифрования только на первом участке передачи сообщения, на остальных участках — как получится...
- в ящик получателя сообщение помещается «как есть»

**Шифрование тела сообщения**

- S/MIME (на основе централизованной PKI)
- OpenPGP (на основе web of trust, «на взаимном доверии»)
- заголовки не шифруются

**Шифрование MRA**

- TLS/SSL

# БОРЬБА СО СПАМОМ

**DNSBL — DNS-based Blackhole List**

MTA после команды EHLO/HELO обращается к DNSBL с DNS-запросом. Если хост в списке, может быть опциональная TXT-запись, объясняющая причину.

Недостатки:
- в список попадают динамические или dial-up адреса
- у разных списков разная политика занесения/исключения из списка

Бывают DNSWL.

© Петрозаводский госуниверситет, А. В. Соловьев, А. П. Мощевикин, 2003-2010

# БОРЬБА СО СПАМОМ

## DKIM — DomainKeys Identified Mail, RFC 4686 (сентябрь 2006)

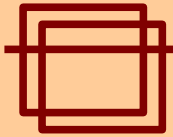
Цифровая подпись подтверждает, что письмо прошло через указанный MTA (MSA) и с тех пор не изменилось. Проверяется тело письма и IMF-заголовки.

```
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed; d=mail.ru; s=mail;
    h=Message-Id:Content-Transfer-Encoding:Content-Type:Reply-To:Date:Mime-
Version:Subject:To:From;
    bh=Yl3yi1nGD9QBYSGKMbxxmt0g2eJuG68hpyXVHj/R4yA=;
    b=qgbHJ1ASsaDXQKmJXYSeO9R2llJSv6IDxaRapviXeL/1y8Fx57uxxKRiwxjju6sEV6UtxwuaKt
    EyBy9t6BYu+IcMR/bGKg0xhtmOKFkNqJFVfK/OxEMqkpuml6IiAhrC;

mail._domainkey.mail.ru. TXT "v=DKIM1\; k=rsa\;
p=MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAODC5C9WNSkAFqb27aDBBJOahA+cmnlrh7fbLfaQ22QJLA
vLhhKOzYtol/2sGVQCpYv4jkf1maaQtwFqJ91jFiPYdjGvOb4e6LEnJYZ1tZt04Rf6eRSJ9vNcHrWAVD
vKTwIDAQAB"
```

© Петрозаводский госуниверситет, А. В. Соловьев, А. П. Мощевикин, 2003-2010

# БОРЬБА СО СПАМОМ



**SPF — Sender Policy Framework, RFC 4408 (апрель 2006)**

MTA проверяет через спец. записи в DNS (запись типа SPF, ранее TXT), что хост-клиент имеет право отправлять сообщения с отправителем из указанного домена (проверка HELO/EHLO, и MAIL FROM).

Если домен публикует SPF-запись, меньше вероятность, что спамеры будут подделываться под письма из этого домена. Поскольку такой домен будет менее привлекателен для спамеров, больше вероятность, что письма из него будут чаще из него доходить до получателей.

Не предусмотрен анализ самого сообщения.

```
mail.ru. TXT "v=spf1 ip4:94.100.176.0/20 ip4:217.69.128.0/21 ip4:195.218.168.66
~all"
```

+ или пусто = PASS, ? = NEUTRAL, ~ = SOFTFAIL, - = FAIL

© Петрозаводский госуниверситет, А. В. Соловьев, А. П. Мощевикин, 2003-2010