OTUS

ОНЛАЙН-ОБРАЗОВАНИЕ

Онлайн-образование

Не забыть включить запись!

Меня хорошо видно && слышно?

Ставьте + , если все хорошо

Напишите в чат, если есть проблемы

Правила вебинара

Активно участвуем

Задаем вопрос в чат или голосом

Off-topic обсуждаем в Slack #канал группы или #general

Вопросы вижу в чате, могу ответить не сразу

Почта: SMTP, IMAP, POP3

Викирюк Павел

Системный инженер

Маршрут вебинара

Протокол SMTP

↓

DKIM, DMARC, SPF

↓

Postfix

↓

Dovecot (IMAP, POP3)

Цели занятия | После занятия вы сможете

1 Отправлять почтовые сообщения с помощью протокола SMTP

2 Принимать почтовые сообщения с помощью протоколов POP3 и IMAP

3 Понимать необходимость почтовых очередей и работать с ними

Цели занятия | После занятия вы сможете

4 Понять как работает MTA Postfix

5 Понять как работает почтовый сервер Dovecot

6 Усвоить основные принципы обхода механизмов борьбы со спамом

Смысл | Зачем вам это уметь

1. Чтобы понимать, как работает электронная почта и ее основные протоколы

2. Чтобы отлаживать процессы отправки и получения почтовых сообщений

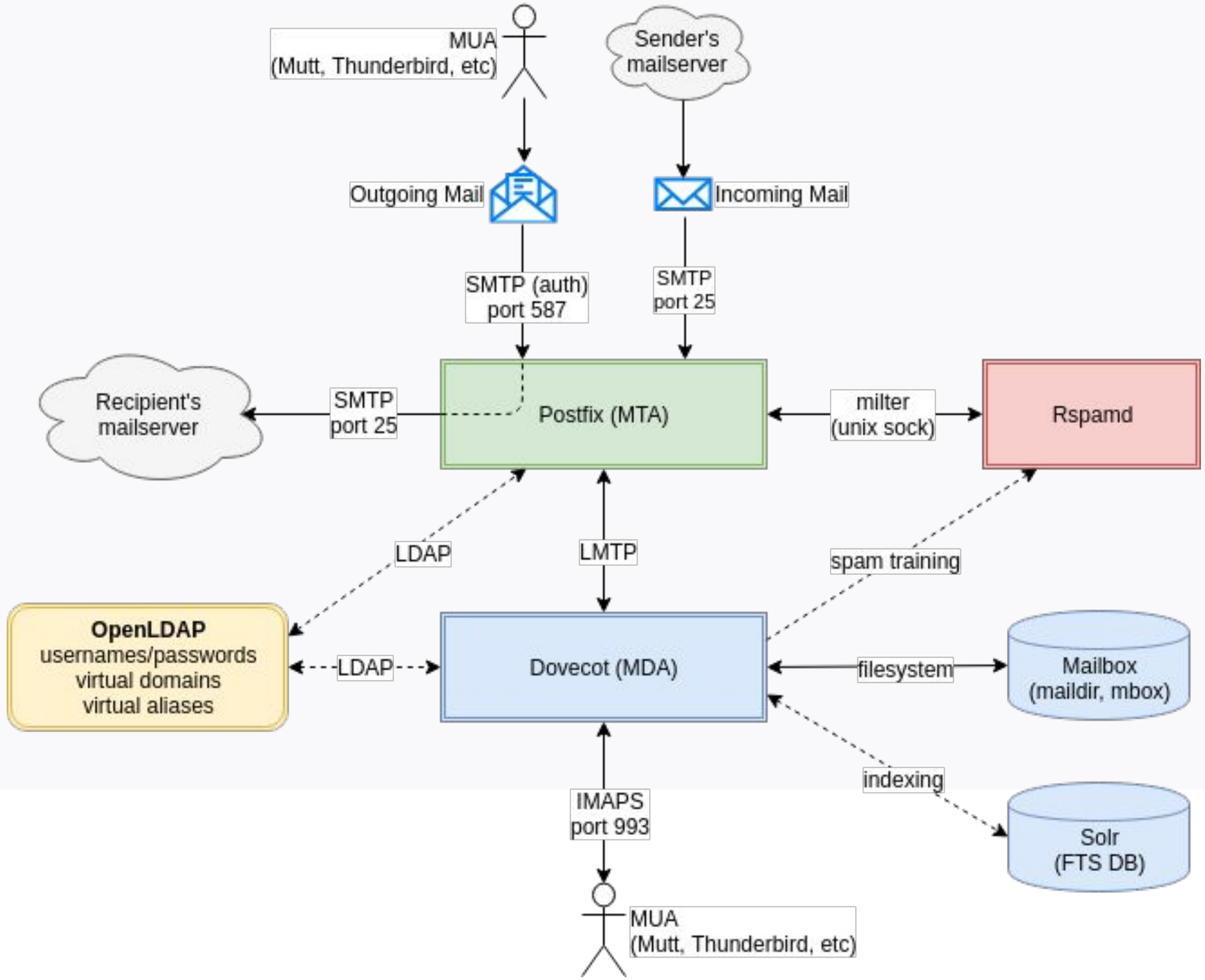
3. Чтобы самостоятельно развернуть безопасный почтовый сервер

Протокол SMTP

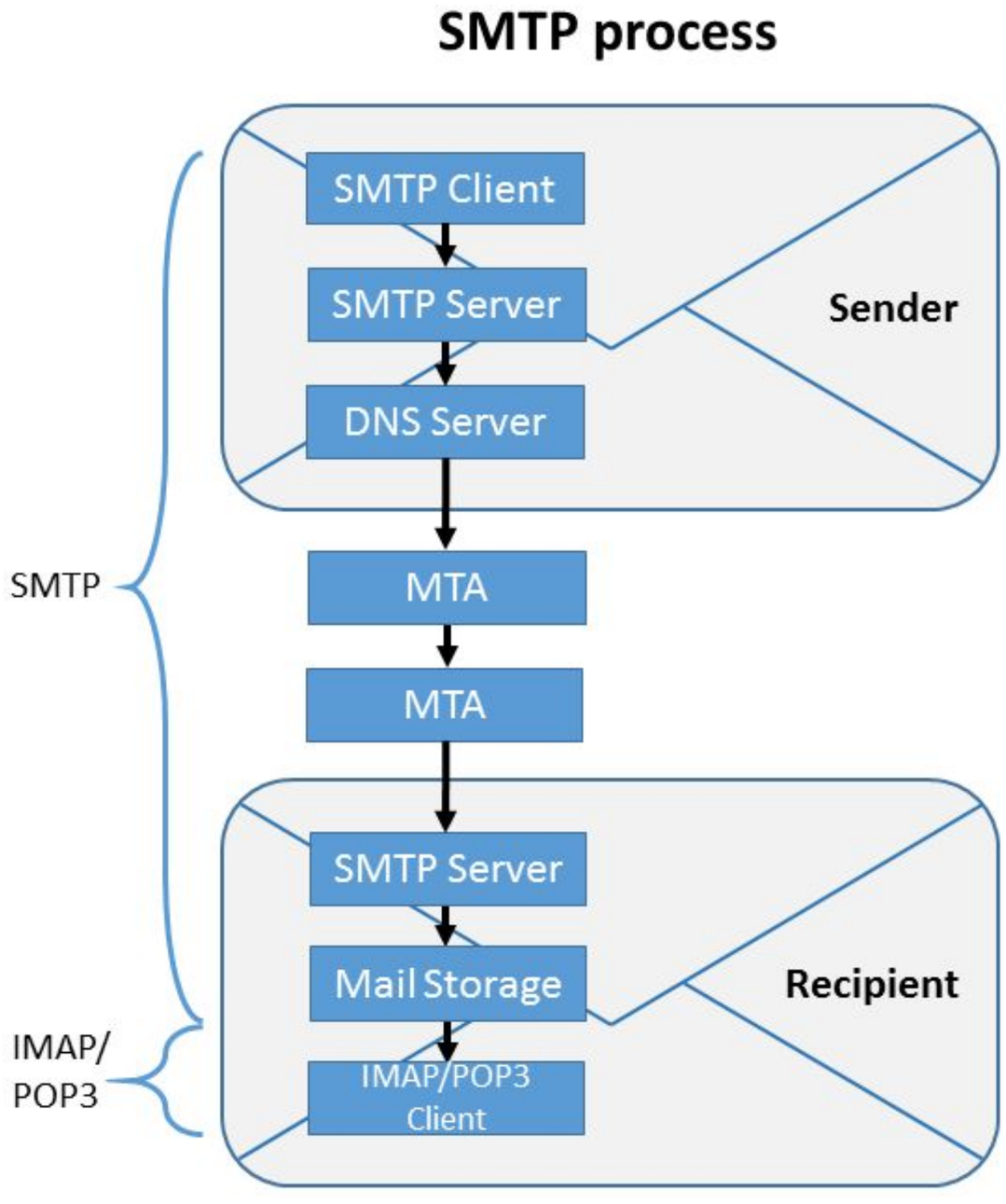
Вопрос к аудитории:

Зачем нужен протокол SMTP?

Протокол SMTP



Протокол SMTP



Протокол SMTP

SMTP (англ. *Simple Mail Transfer Protocol* — простой протокол передачи почты)

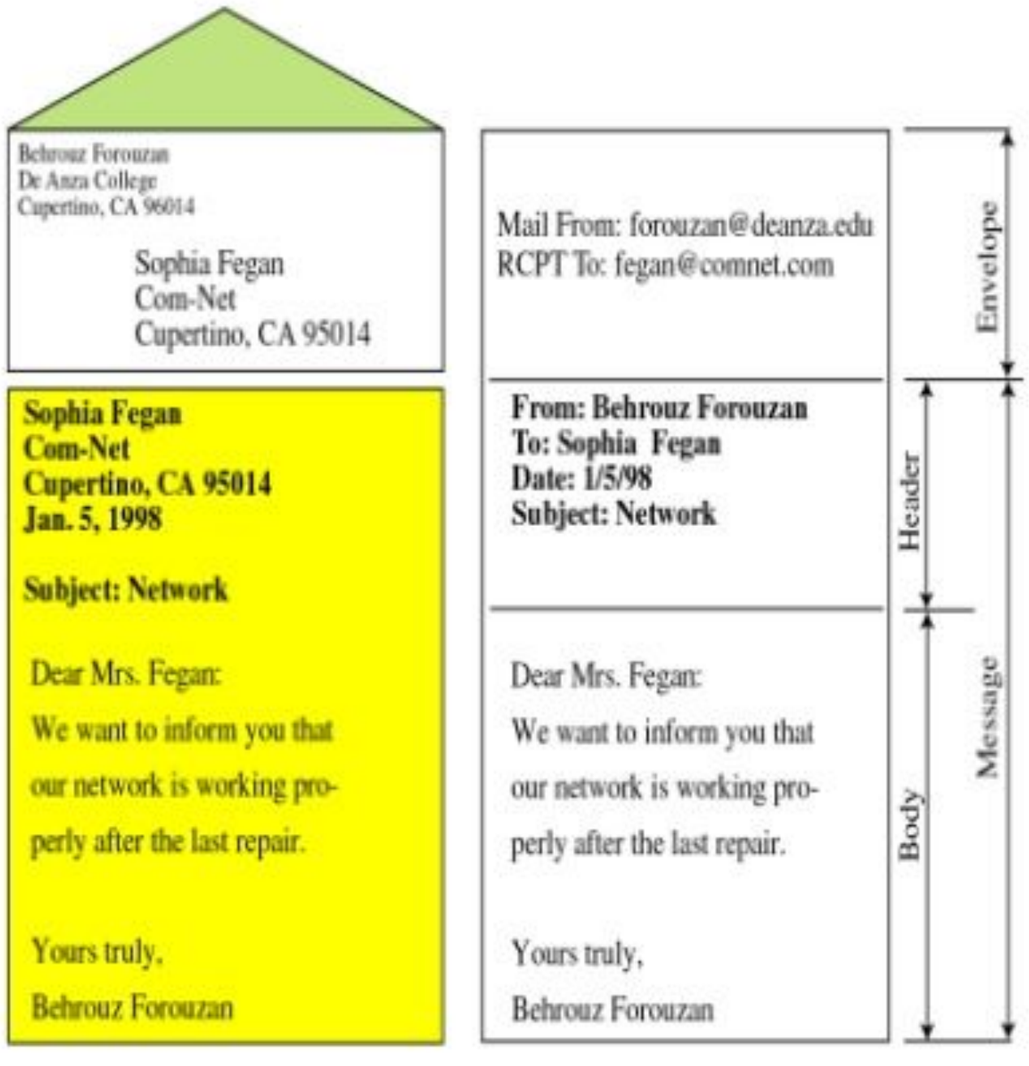
- появился в 1985 году (то есть на 10 лет раньше HTTP)
- используется для передачи электронной почты в сетях
- актуальное описание в RFC https://tools.ietf.org/html/rfc5321 (2008 год)
- использует порт 25/TCP
- представляет из себя текстовый протокол

Протокол SMTP

Структура письма

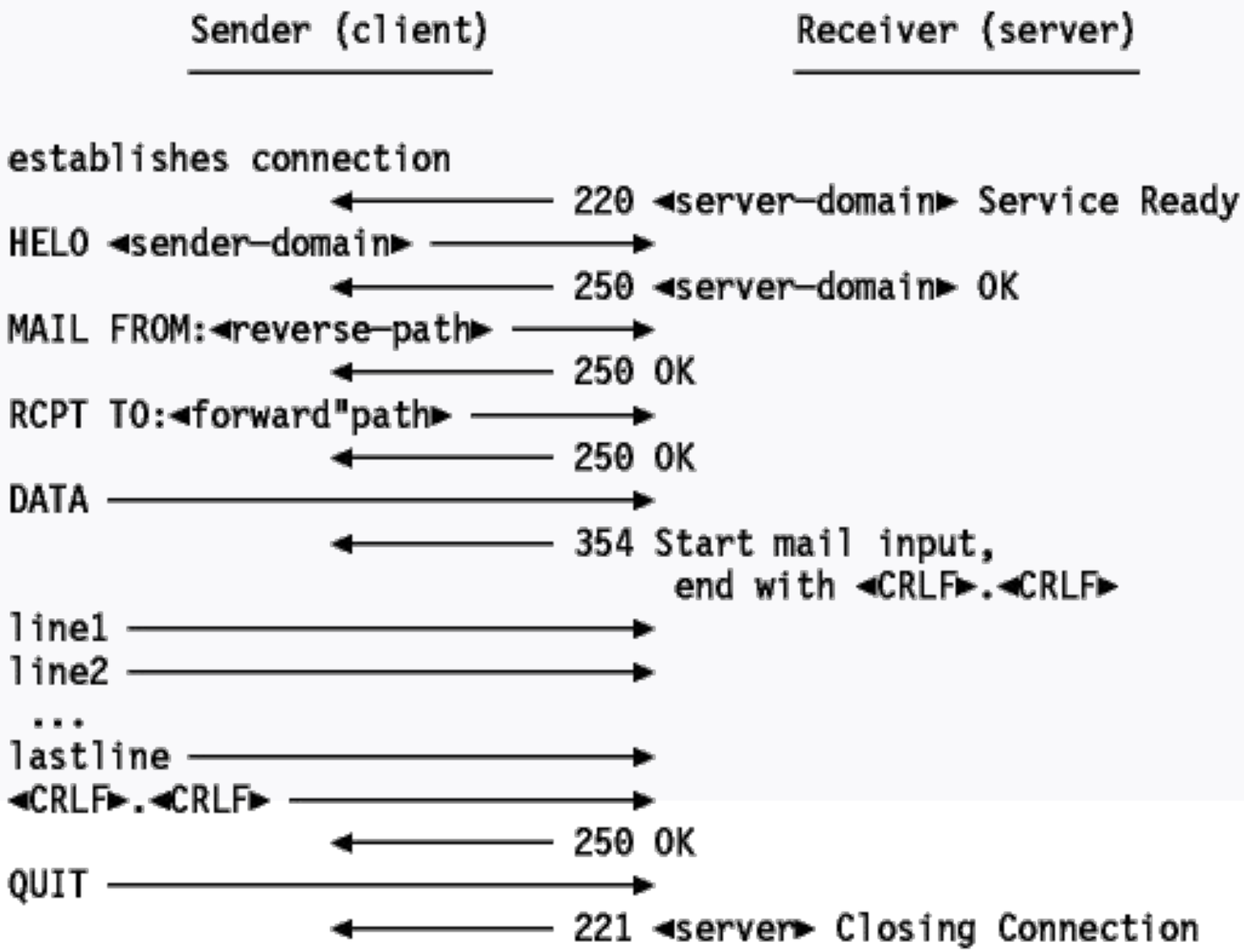
Format of an email

- Mail is a text file
- Envelope –
  - sender address
  - receiver address
  - other information
- Message –
  - Mail Header – defines the sender, the receiver, the subject of the message, and other information
  - Mail Body – Contains the actual information in the message



Протокол SMTP

Процесс отправки письма



Протокол SMTP

Процесс отправки письма

1. Подключаемся к почтовому серверу:

```
telnet 127.0.0.1 25
```

Протокол SMTP

Процесс отправки письма

1. Подключаемся к почтовому серверу:

```
telnet 127.0.0.1 25
Trying 127.0.0.1...
Connected to mydomain.ru.com.
Escape character is '^]'
220 mail.mydomain.ru.com ESMTP Postfix (Debian/GNU)
```

Протокол SMTP

Процесс отправки письма

2. Представляемся почтовому серверу:

```
telnet 127.0.0.1 25
Trying 127.0.0.1...
Connected to mydomain.ru.com.
Escape character is '^]'
220 mail.mydomain.ru.com ESMTP Postfix (Debian/GNU)
EHLO mail.mydomain.ru
```

Протокол SMTP

Процесс отправки письма

2. Представляемся почтовому серверу:

```
telnet 127.0.0.1 25
Trying 127.0.0.1...
Connected to mydomain.ru.com.
Escape character is '^]'
220 mail.mydomain.ru.com ESMTP Postfix (Debian/GNU)
EHLO mail.mydomain.ru
250-mail.mydomain.ru
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250 SMTPUTF8
```

Протокол SMTP

Процесс отправки письма

2. Представляемся почтовому серверу:

HELO - команда приветствия из RFC821

EHLO - (extended HELO) более современный вариант приветствия из RFC5321

Протокол SMTP

Процесс отправки письма

3. Указываем имя отправителя:

```
mail from: <pavel@mydomain.ru>
```

Протокол SMTP

Процесс отправки письма

3. Указываем имя отправителя:

```
mail from: <pavel@mydomain.ru>
250 2.1.0 Ok
```

Протокол SMTP

Процесс отправки письма

3. Указываем имя получателя:

```
mail from: <pavel@mydomain.ru>
250 2.1.0 Ok
rcpt to: <pavel@domain.ru.com>
```

Протокол SMTP

Процесс отправки письма

3. Указываем имя получателя:

```
mail from: <pavel@mydomain.ru>
250 2.1.0 Ok
rcpt to: <pavel@domain.ru.com>
250 2.1.5 Ok
```

Протокол SMTP

Процесс отправки письма

4. Формируем сообщение:

```
DATA
```

Протокол SMTP

Процесс отправки письма

4. Формируем сообщение:

```
DATA
354 End data with <CR><LF>.<CR><LF>
```

Протокол SMTP

Процесс отправки письма

4. Формируем сообщение:

```
DATA
354 End data with <CR><LF>.<CR><LF>
From: Pavel Vikiryuk <pavel@mydomain.ru>
To: Pavel <pavel@domain.ru.com>
Subject: Test subject
Content-Type: text/plain

Hi!

Bye
```

Протокол SMTP

Процесс отправки письма

5. Завершаем сообщение:

```
DATA
354 End data with <CR><LF>.<CR><LF>
From: Pavel Vikiryuk <pavel@mydomain.ru>
To: Pavel <pavel@domain.ru.com>
Subject: Test subject
Content-Type: text/plain

Hi!

Bye
.
250 2.0.0 Ok: queued as 278EE6047B
```

Протокол SMTP

Процесс отправки письма

6. Закрываем соединение:

```
quit
```

Протокол SMTP

Процесс отправки письма

6. Закрываем соединение:

```
quit
221 2.0.0 Bye
```

Ваши вопросы?

MTA, MDA, LDA

Вопрос к аудитории:

MTA, MDA, LDA - что это? Есть предположения?

MTA, MDA, LDA

MTA (Mail Transfer Agent) - сервис передачи сообщения

MDA (Mail Delivery Agent) - сервис получения и доставки сообщения пользователю

LDA (Local Delivery Agent) - сервис получения и доставки сообщения **локальному** пользователю (в пределах **одной** системы)

MTA, MDA, LDA

Примеры MTA:

- sendmail https://www.proofpoint.com/us/open-source-email-solution
- Postfix http://www.postfix.org/
- qmail http://cr.yp.to/qmail.html
- Exim http://www.exim.org/

Примеры MDA:

- Dovecot https://www.dovecot.org/

Примеры LDA:

- Postfix
- Dovecot

Ваши вопросы?

Немного о DNS

Вопрос к аудитории:

Какие типы DNS-записей вы помните?

Немного о DNS

PTR запись

Зачем она нужна?

Запись подтверждает связь домена с IP-адресом сервера отправителя

Особенности:

- возвращает имя хоста по его IP-адресу

Немного о DNS

PTR запись

Зачем она нужна?

Запись подтверждает связь домена с IP-адресом сервера отправителя

Особенности:

- возвращает имя хоста по его IP-адресу
- прописывается хостером или оператором связи, которому принадлежит сеть
- негласное правило: должна быть PTR запись на каждую A запись

Немного о DNS

MX запись

Зачем она нужна?

- возвращает **A запись** почтового сервера для домена. По A записи возвращается IP-адрес сервера
- указывает порядковый номер предпочтения почтового сервера (приоритет)
- позволяет осуществлять балансировку почты

Особенности:

- разрешается указывать **только** имя, а не IP-адрес или CNAME
- A запись, на которую ссылается MX должна существовать
- MX записей может быть несколько

Немного о DNS

A записи

Зачем они нужны?

- чтобы задать имена почтового сервера, MX-сервера, сервера отправки

Ваши вопросы?

Маршрут вебинара

Протокол SMTP

↓

DKIM, DMARC, SPF

↓

Postfix

↓

Dovecot (IMAP, POP3)

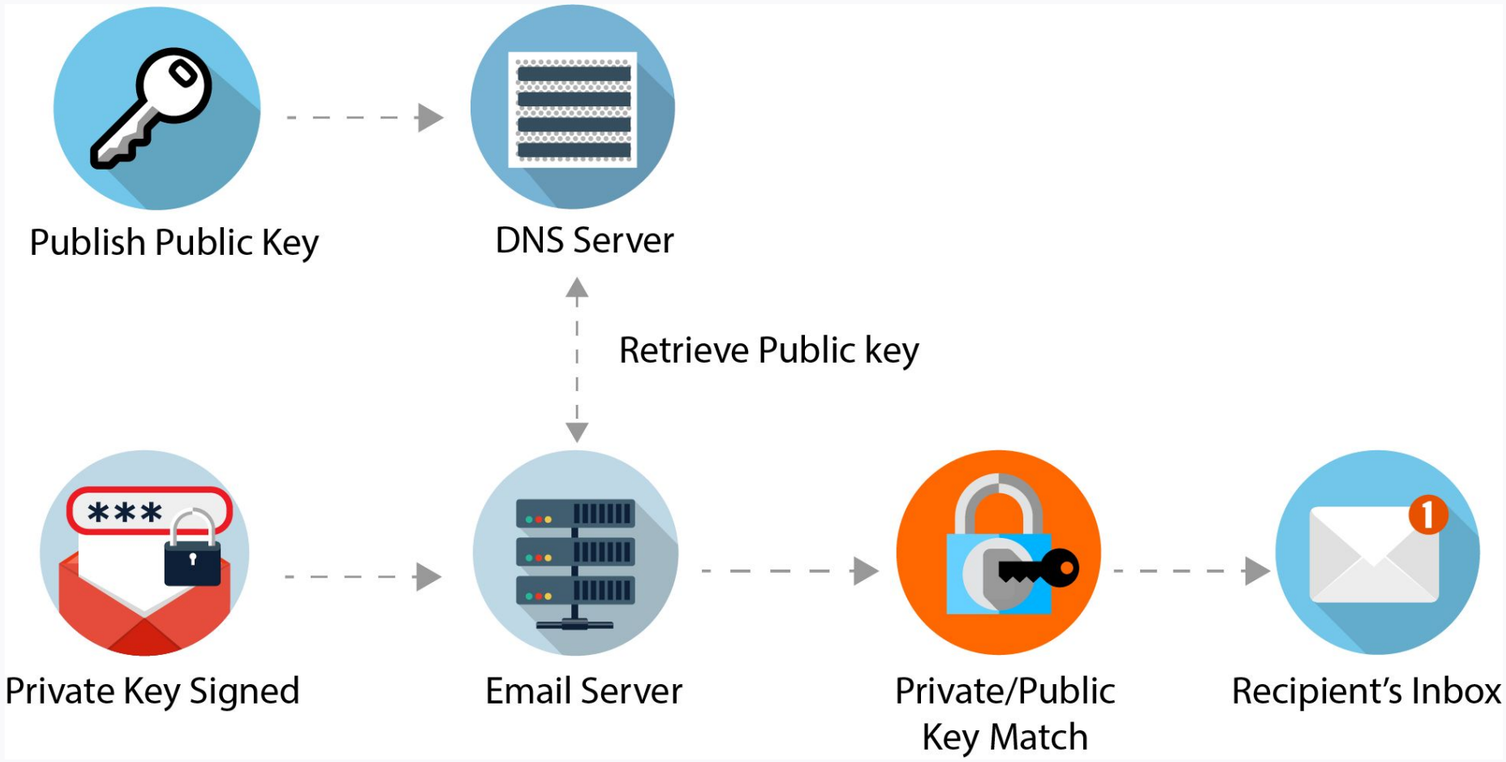
DKIM, DMARC, SPF

Вопрос к аудитории:

Что за механизмы DKIM, DMARC и SPF?

DKIM

DKIM


Publish Public Key
DNS Server
Retrieve Public key
***
Private Key Signed
Email Server
Private/Public
Key Match
Recipient's Inbox

DKIM

DKIM (Domain Keys Identified Mail) - это цифровая подпись, которая подтверждает подлинность отправителя и гарантирует целостность доставленного письма

Особенности:

- используются два ключа шифрования: **приватный** для подписи сообщений и **публичный** для проверки подписи
- для доступа к публичному ключу по технологии DomainKeys используется DNS
- ключи добавляются в служебные заголовки писем
- подпись автоматически проверяется почтовым сервером в соответствии с заданными политиками

DKIM

Примеры записей:

```
_domainkey.mydomain.ru IN      TXT     "t=s\; o=~\;"
```

t=s — означает, что запись будет использована только для домена, к которому относится запись, не рекомендуется, если используются субдомены
o=~ - не особо строгая проверка, означает, что некоторые сообщения с этого домена подписываются DKIM
o=- - строгая проверка, означает, что **все** сообщения с этого домена подписываются
; - разделитель

DKIM

Примеры записей:

```
_domainkey.mydomain.ru IN      TXT     "t=s\; o=~\;"
mail._domainkey.mydomain.ru    IN      TXT     "v=DKIM1; k=rsa;
p=MIGfMA0GCS**********************************************************************
**********************************************************************
**********************************************wp9QIDAQAB"
```

v=DKIM1 - версия, обязательный аргумент, всегда принимает значение DKIM1
k=rsa - тип используемого ключа
p= - собственно публичный RSA-ключ

DKIM

Примеры записей:

```
_domainkey.mydomain.ru IN      TXT     "t=s\; o=~\;"
mail._domainkey.mydomain.ru    IN      TXT     "v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDeq19vZmGfwkiEtxnE0OWJvKrOKKMs8WyvvYUpWo
824is24pE4GIgAnNBtn9U9DMH4gcYA9XliXY7xUxP2Y9Qq4kSZtkdPT3HbvlmrXbsMtyxurhbNflymoYw8s2ws
JHVLX7Pk9pgoHnFpMJdm0eUP1x4Hepeqq6aEkKlgbUwp9QIDAQAB"
_adsp._domainkey.mydomain.ru.  IN      TXT     "dkim=all"
```

ADSP запись, определяет, обязательно ли письмо должно быть подписано, или нет
dkim=all - означает, что все письма должны быть подписаны

DMARC

DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) - это механизм защиты от спама и от несанкционированной рассылки почты с домена

Особенности:

- информирование почтового сервера получателя о наличии записей DKIM, SPF и их использовании
- рекомендации почтовому серверу получателя об обработке почты с невалидными DKIM и SPF
- получение обратной связи от серверов получателей в формате RFC 5969 и RFC 5070, которые позволяют, в частности, узнать о несанкционированной рассылке с домена

DMARC

Примеры записей:

С домена отправляется почта (мягкий вариант):

```
_dmarc   TXT   "v=DMARC1;p=none;fo=1;rua=mailto:admin@example.com;ruf=mailto:admin@example.com"
```

v=, **версия**, обязательный параметр и должен быть первым со значением **DMARC1**
p=, **policy**. Значение **none** — нет рекомендации почтовому серверу
fo=, **fail policy**, значение 1 - отправляет обратный отчет, если какая-то из проверок невалидна
rua=, список почтовых адресов через запятую, на которые высылать агрегированные отчеты
ruf=, опциональный, список почтовых адресов через запятую, на которые высылать fail-отчеты (о невалидной почте)

DMARC

Примеры записей:

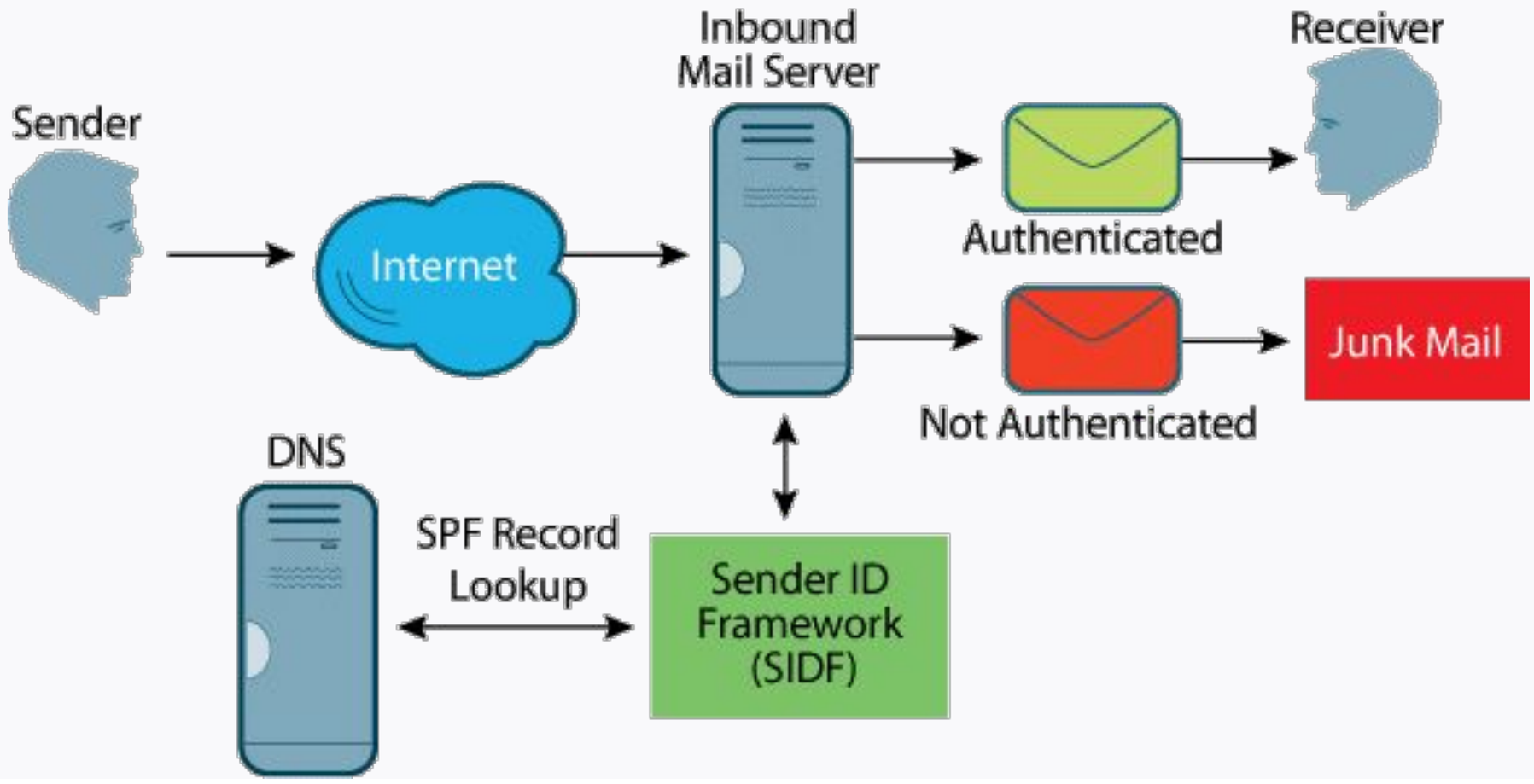
С домена отправляется почта (более строгий вариант):

```
_dmarc   TXT
"v=DMARC1;p=reject;sp=reject;pct=100;aspf=r;fo=1;rua=mailto:admin@mydomain.ru;ruf=mailto:admin@mydomain.ru"
```

p=, **policy**, значение **reject** — рекомендация почтовому серверу отклонять сообщения, не прошедшие проверку DKIM и SPF
fo=, **fail policy**, значение 1 - отправляет обратный отчет, если какая-то из проверок невалидна
aspf=, значение **r** (**relaxed**, по умолчанию) для SPF, требует совпадения ответа команды MAIL FROM и заголовка From письма, разрешает субдомены

SPF

SPF


Inbound
Mail Server
Receiver
Sender
Internet
Authenticated
Junk Mail
Not Authenticated
DNS
SPF Record
Lookup
Sender ID
Framework
(SIDF)

SPF

SPF (Sender Policy Framework) — это подпись, содержащая информацию о серверах, которые могут отправлять почту с вашего домена.

Особенности:

- наличие SPF снижает вероятность попадания вашего письма в спам
- может быть только одна SPF запись для одного домена
- но в записи могут быть перечислены несколько серверов

SPF

Примеры записей:

```
@       IN      TXT     "v=spf1 ip4:1.1.1.1 a mx include:_spf.google.com ~all"
```

v=spf1 - версия SPF, обязательный параметр
ip4: - параметр указывает адрес (несколько адресов, или подсеть)
a - разрешает отправляет письма с адреса, который указан в A записи домена отправителя
mx - разрешает отправлять письма с адреса, который указан в MX записи домена
include - включает в себя хосты, разрешенные SPF-записью указанного домена
~all - описывает все остальные сервера, не перечисленные в SPF-записи. Параметр **~** означает SoftFail или мягкое отклонение не соответствующих сообщений

SPF

Примеры записей:

```
@       IN      TXT     "v=spf1 mx a ip4:1.1.1.121 ip4:2.2.1.0/29 ip4:18.40.40.22 include:_spf.yandex.ru -all"
```

ip4: - параметр указывает адрес (несколько адресов, или подсеть)
a - разрешает отправляет письма с адреса, который указан в A записи домена отправителя
mx - разрешает отправлять письма с адреса, который указан в MX записи домена
include - включает в себя хосты, разрешенные SPF-записью указанного домена
-all - описывает все остальные сервера, не перечисленные в SPF-записи. В данном случае запись рекомендует отклонять письма, не соответствующие политике

Ваши вопросы?

SPAM

SPAM

Причины:

- боты и ботнеты
- открытые почтовые релеи
- зомби-сервера
- интерфейсы iKVM, iLo и прочие
- взломанные аккаунты почтовых систем
- некорректно настроенные тикет-системы (битва роботов)

SPAM

Отличительные черты:

- невалидный обратный адрес
- неправильные заголовки
- хост отправления не является публичным MX
- не повторяют отправку
- тело письма содержит спам

SPAM

Что делать, чтобы почта отправлялась?

- hostname сервера = A запись + PTR запись
- сервер должен быть в MX записях
- адрес отправителя должен быть валиден
- настроен SPF
- настроен DKIM
- настроен DMARC
- в maillist отсутствуют honeypot

SPAM

Как проверить?

- https://whatismyipaddress.com/blacklist-check
- https://mxtoolbox.com
- http://www.anti-abuse.org/multi-rbl-check
- https://toolbox.googleapps.com/apps/checkmx

SPAM

Как защититься?

- проверка PTR записей
- проверка MX записей
- проверка SPF, DKIM
- проверка отправителя и получателя
- graylist (сервер временно недоступен)
- Blacklist, DNSBL (RBL) - не рекомендуется, но бывает
- использовать **SpamAssassin** или **rspamd**

Маршрут вебинара

Протокол SMTP

DKIM, DMARC, SPF

Postfix

Dovecot (IMAP, POP3)

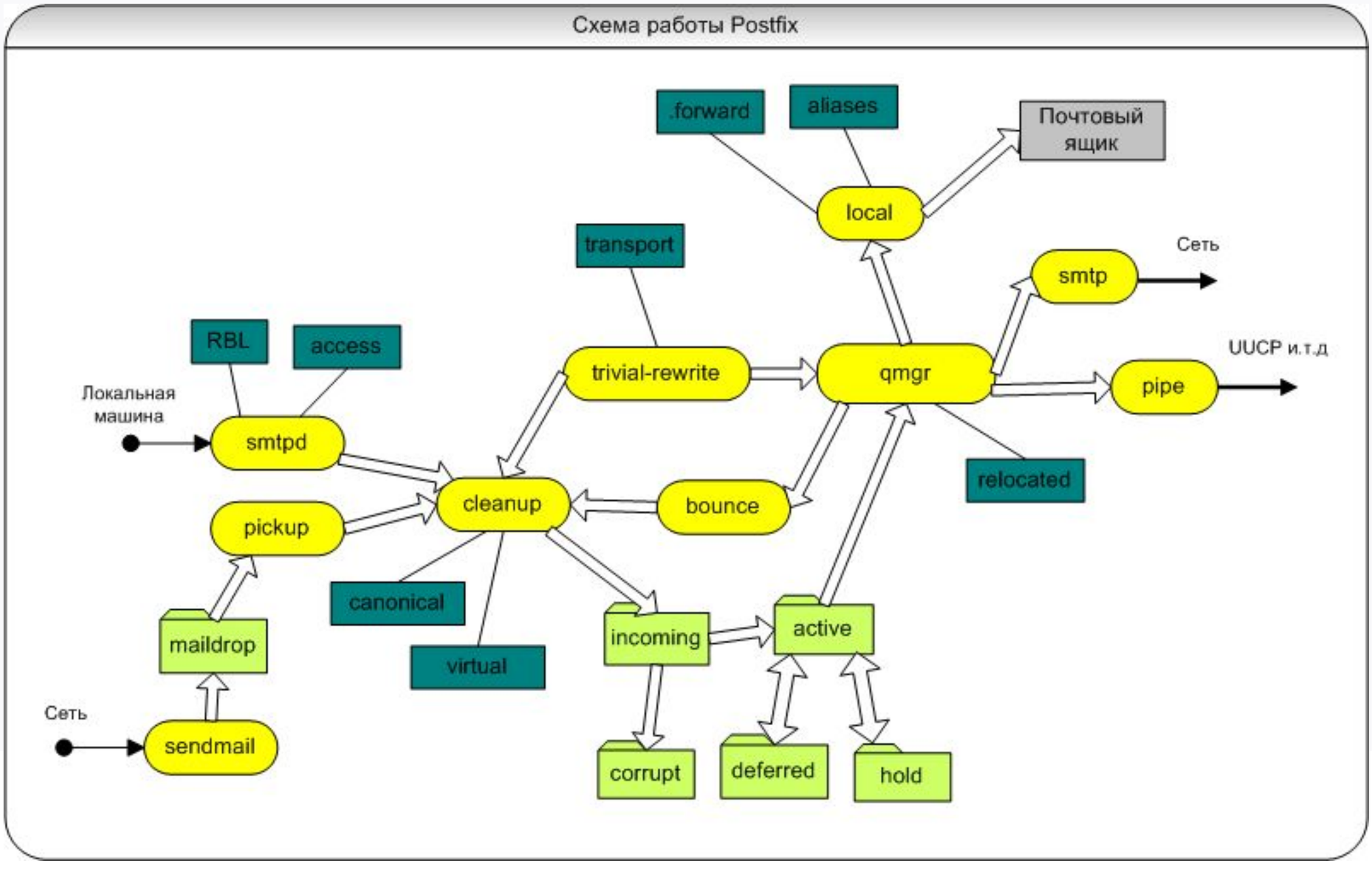
Postfix

Вопрос к аудитории:

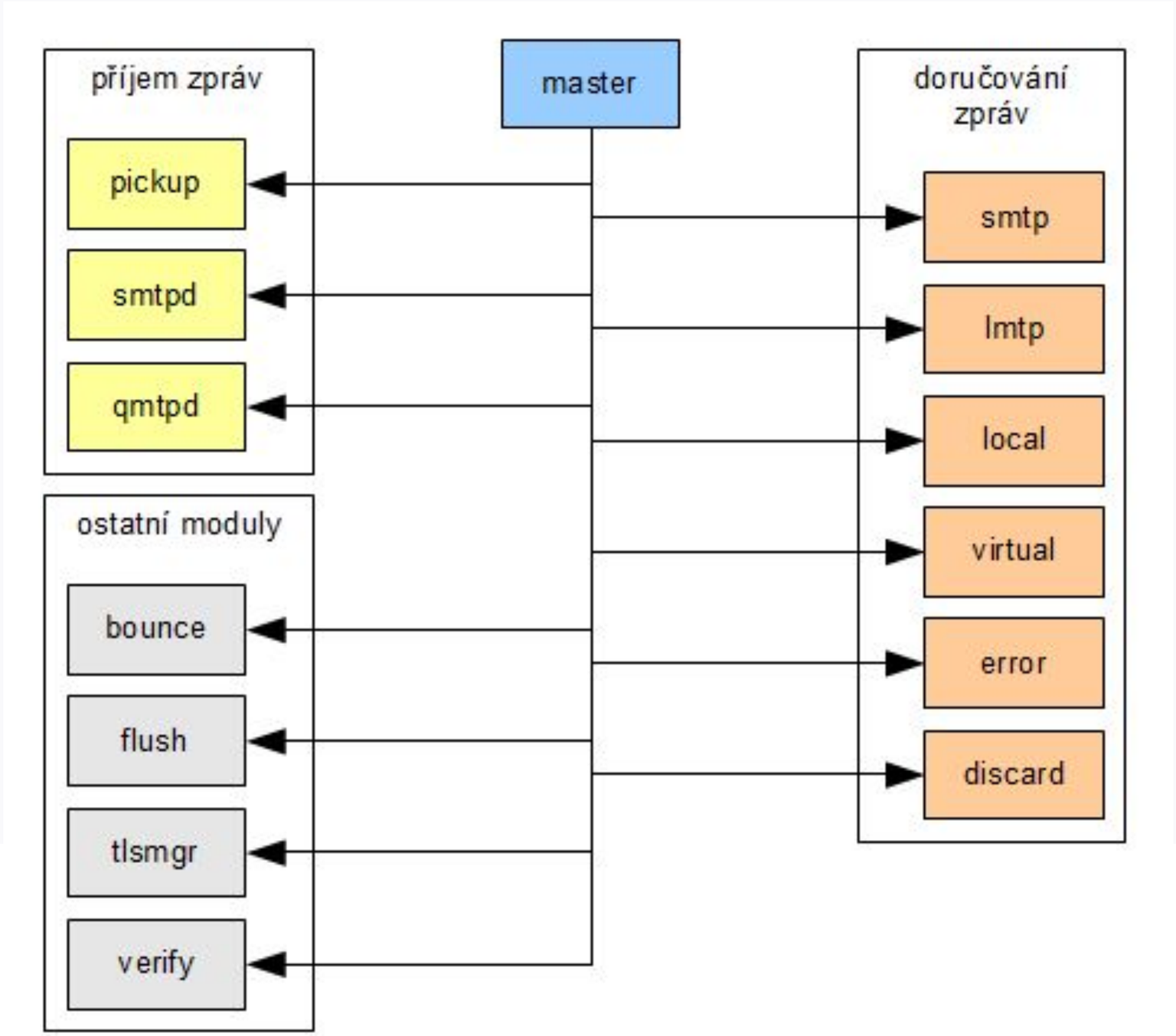
Кто-нибудь из вас уже использует Postfix?

Postfix: архитектура

Postfix: архитектура



Postfix: архитектура



Postfix: архитектура

Архитектура:

- модульный, состоит из многих демонов
- демоны общаются через unix-сокеты
- основной процесс вызывает вспомогательные демоны по мере необходимости
- модульность позволяет включать только необходимые демоны
- память для рабочих процессов выделяет динамически

Postfix: очереди

Postfix: очереди

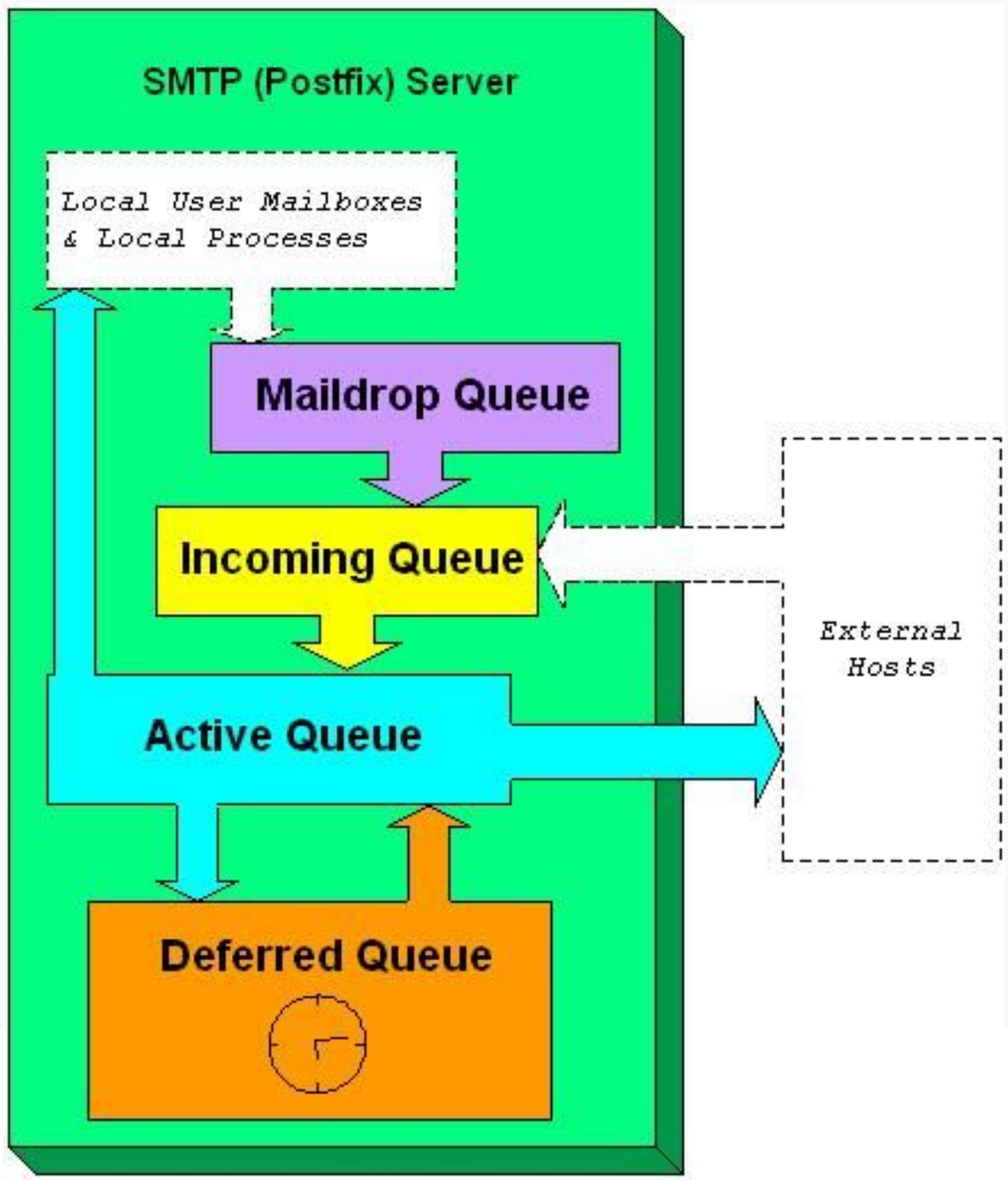


Figure 1: Postfix Queues

Postfix: очереди

Очереди:

- **maildrop** — в эту очередь попадают письма, отосланные командой sendmail
- **hold** — очередь, в которую попадают письма, которые согласно настроек postfix не могут попасть в нормальную обработку
- **deferred** — сюда попадают письма, для которых отправка не удалась. Очередь писем периодически сканируется и предпринимается попытка отослать их
- **incoming** — сюда попадают все письма после отправки, где они сканируются и передаются в одну из других очередей
- **active** — письма, готовые к отправке (или в процессе отправки). В отличии от предыдущих очередей (которые сохраняются на диске), данная очередь сохраняется в оперативной памяти

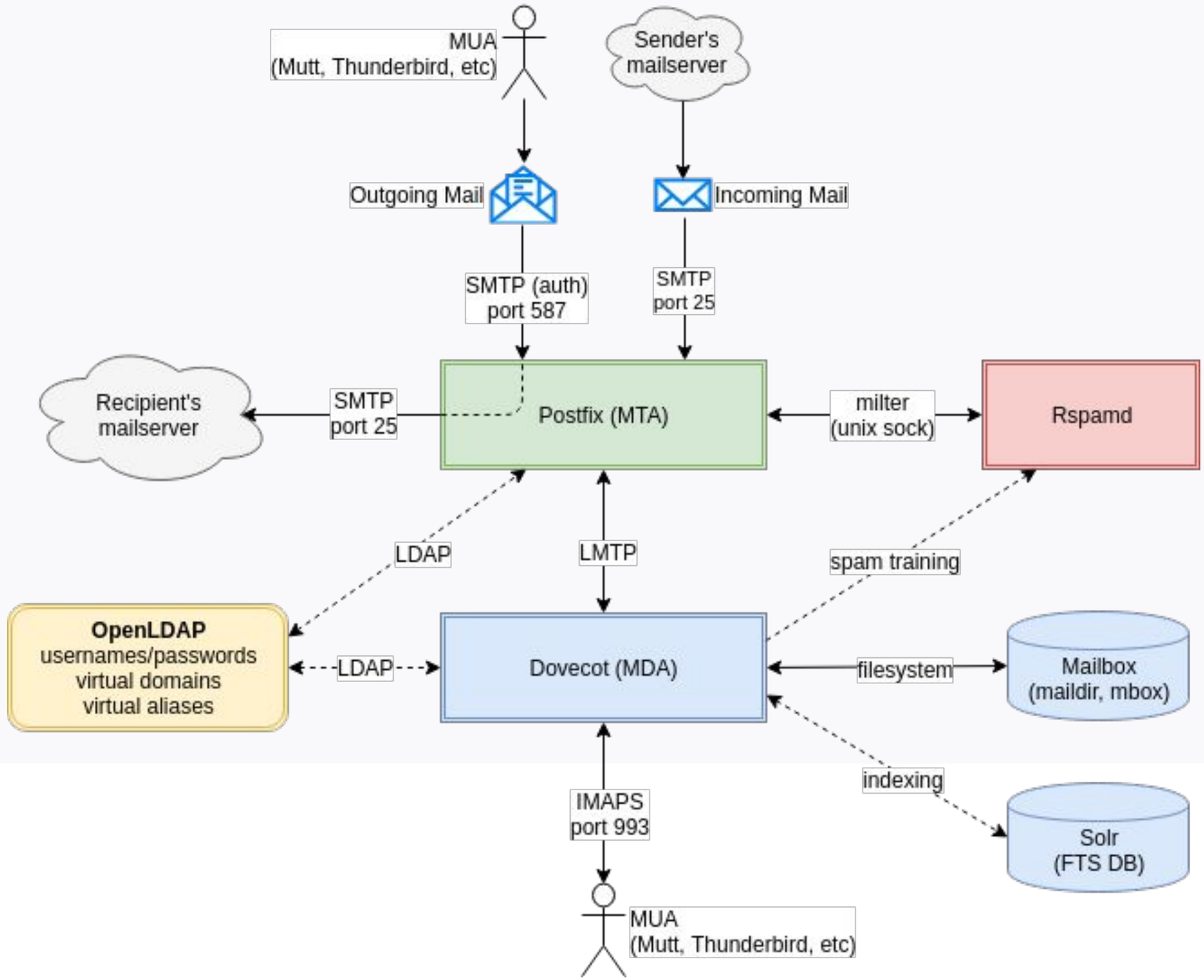
Postfix: очереди

Особенности:

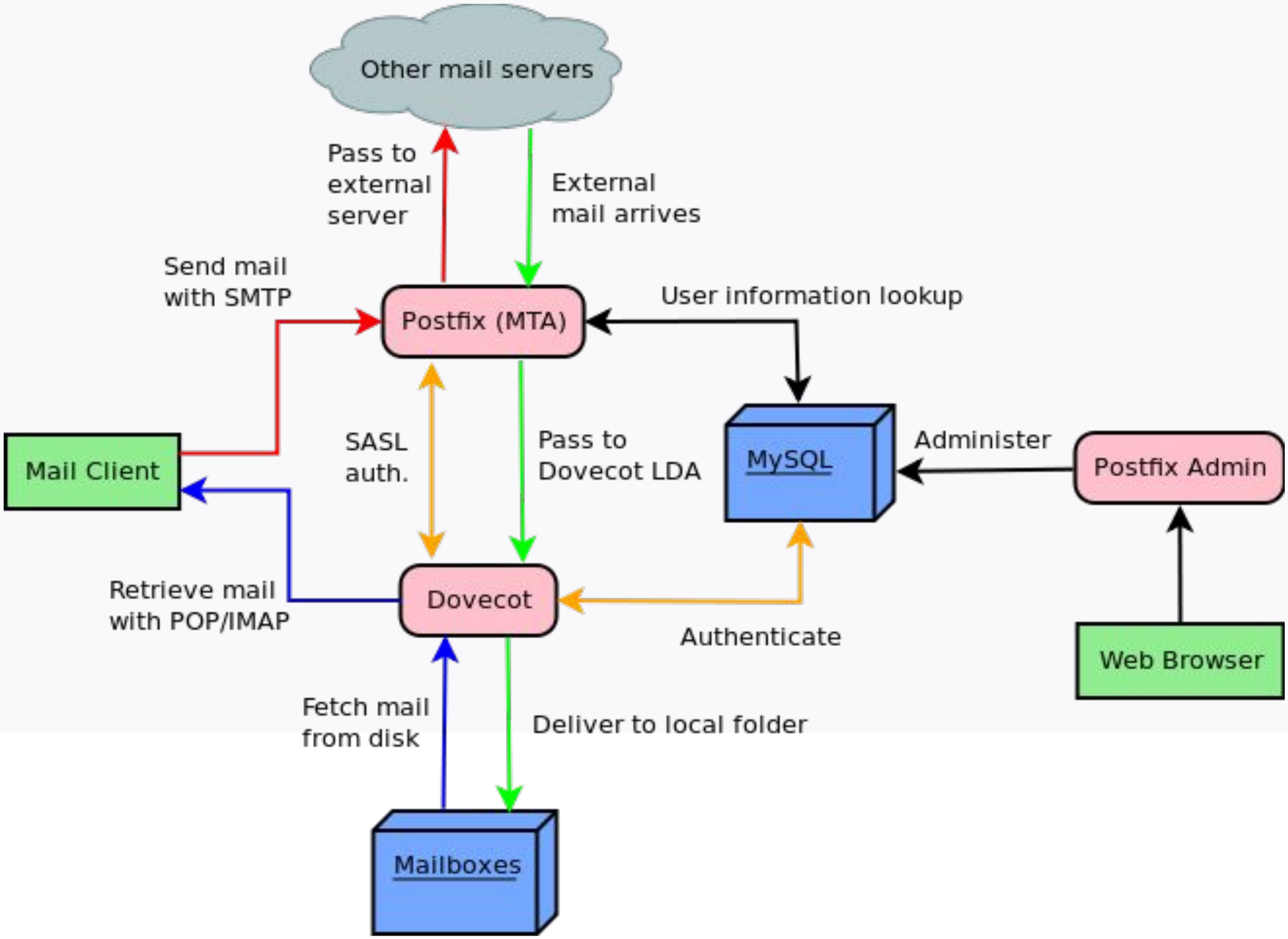
- нужны только затем, чтобы не потерять почту в процессе
- по сути являются файлами (mailbox) и каталогами (maildir)
- очереди являются слабым местом в производительности почтового сервера
- лучше располагать на отдельном массиве из SSD дисков
- можно монтировать в tmpfs, но учесть при этом объем свободной оперативной памяти на сервере

Postfix: конфигурация

Postfix: конфигурация



Postfix: конфигурация



Postfix: конфигурация

Основные конфигурационные файлы:

main.cf - конфигурация всей почтовой системы

Минимальная конфигурация:

```
myhostname = mail.test.ru
myorigin = test.ru
mydestination = $myhostname, mail.test.ru, localhost.localdomain,
localhost
inet_interfaces = localhost
inet_protocols = ipv4
```

mydestination определяет домены, которые будут считаться локальными для данного сервера, соответственно postfix будет искать пользователей этих доменов в локальных таблицах

Postfix: конфигурация

Основные конфигурационные файлы:

main.cf - конфигурация всей почтовой системы

База данных пользователей:

```
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
```

Postfix: конфигурация

Основные конфигурационные файлы:

main.cf - конфигурация всей почтовой системы

Виртуальные почтовые ящики:

```
virtual_mailbox_domains = mysql:/etc/postfix/sql/vdomains.cf
virtual_mailbox_base = /var/vmail
virtual_mailbox_maps = mysql:/etc/postfix/sql/vmailbox.cf
virtual_minimum_uid = 1150
virtual_uid_maps = static:1150
virtual_gid_maps = static:8
virtual_transport = dovecot
dovecot_destination_recipient_limit = 1
```

Postfixadmin - веб-интерфейс для работы с пользователями в базе

http://postfixadmin.sourceforge.net/

Postfix: конфигурация

Основные конфигурационные файлы:

main.cf - конфигурация всей почтовой системы

Почтовый релей:

```
mynetworks = 127.0.0.0/8 [::1]/128
smtpd_relay_restrictions = permit_mynetworks, permit_sasl_authenticated,
defer_unauth_destination
```

Postfix: конфигурация

Основные конфигурационные файлы:

main.cf - конфигурация всей почтовой системы

DKIM milter:

```
milter_default_action = accept
milter_protocol = 2
smtpd_milters = inet:localhost:8891
non_smtpd_milters = inet:localhost:8891
```

OpenDKIM: http://www.opendkim.org/

Postfix: конфигурация

Основные конфигурационные файлы:

main.cf - конфигурация всей почтовой системы

Open relay + DNSBL + RBL + Postgrey :

```
permit_mynetworks =
relay_domains =
virtual_mailbox_domains =
mydestination =

smtpd_client_restrictions =
permit_inet_interfaces,
permit_mynetworks,
permit_sasl_authenticated,
reject_rbl_client dnsbl.sorbs.net, reject_maps_rbl,
reject_unknown_client_hostname,
reject_unknown_reverse_client_hostname,
check_policy_service inet:localhost:10023 # postgrey
permit | defer | reject
```

Postfix: конфигурация

Основные конфигурационные файлы:

main.cf - конфигурация всей почтовой системы

Postfix + SSL (smtp):

```
smtp_tls_security_level = may
smtp_tls_ciphers = export
smtp_tls_protocols = !SSLv2, !SSLv3

smtp_use_tls = yes

smtp_tls_mandatory_ciphers = high
smtp_tls_mandatory_protocols=!SSLv2,!SSLv3
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
```

Postfix: конфигурация

Основные конфигурационные файлы:

main.cf - конфигурация всей почтовой системы

Postfix + SSL (smtpd):

```
postconf -e smtpd_tls_cert_file='/etc/letsencrypt/live/mail.mydomain.com/cert.pem'
postconf -e smtpd_tls_key_file='/etc/letsencrypt/live/mail.mydomain.com/privkey.pem'
postconf -e smtpd_tls_CAfile='/etc/letsencrypt/live/mail.mydomain.com/chain.pem'

postconf -e smtp_tls_security_level = may
postconf -e smtpd_tls_security_level = may
```

Postfix: конфигурация

Основные конфигурационные файлы:

main.cf - конфигурация всей почтовой системы

Другие типы Postfix milter:

- clamav
- rspamd
- opendmarc

http://www.postfix.org/MILTER_README.html

Postfix: конфигурация

Основные конфигурационные файлы:

master.cf - конфигурация модулей почтовой системы

Конвейер для использования Dovecot:

```
dovecot unix - n n - - pipe
  flags=DRhu user=vmail:vmail argv=/usr/lib/dovecot/deliver -f ${sender}
-d $(recipient)
```

Postfix: утилиты

Postfix: утилиты

Утилиты:

- **postqueue** - смотрим очереди
- **postsuper** - работа с письмами в очередях (удаление, перезапуск)
- **postalias** - работа с базой данных алиасов
- **postconf** - работа с конфигурацией Postfix (просмотр, редактирование)
- **postlog** - запись данных в лог Postfix (например в скриптах)
- **postcat** - просмотр содержимого файла в очереди
- **postmap** - выполнение запросов к вспомогательным таблицам или создание этих таблиц

Postfix: утилиты

Примеры:

Просмотр очереди

```
postqueue -p
-Queue ID- --Size-- ----Arrival Time---- -Sender/Recipient------
BBC165EC0       399 Mon Aug 19 06:48:35  pavel@test.ru
                                         (address resolver failure)
                                         pavel@test.ru

0BB9C5ECF       417 Tue Aug 20 11:10:39  root@/etc/mailname
                                         (address resolver failure)
                                         pavel@test.ru

13C0E647D3      418 Fri Aug 23 17:26:56  pavel@test.ru
                                         (address resolver failure)
                                         pavel@test.ru.com
```

Postfix: утилиты

Примеры:

Просмотр сообщения в очереди

```
postcat -q 652E93A696
*** ENVELOPE RECORDS deferred/6/652E93A696 ***
message_size:            416             205               1               0             416
message_arrival_time: Fri Aug 23 19:38:44 2019
create_time: Fri Aug 23 19:38:44 2019
named_attribute: rewrite_context=local
sender_fullname: root
sender: root@test.ru
original_recipient: user@mydomain.ru
recipient: user@mydomain.ru
*** MESSAGE CONTENTS deferred/6/652E93A696 ***
Received: by mail.test.ru (Postfix, from userid 0)
        id 652E93A696; Fri, 23 Aug 2019 19:38:44 +0000 (UTC)
```

Postfix: утилиты

Примеры:

Просмотр сообщения в очереди

```
Date: Fri, 23 Aug 2019 19:38:44 +0000
To: user@mydomain.ru
Subject: test subject
User-Agent: Heirloom mailx 12.5 7/5/10
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Message-Id: <20190823193844.652E93A696@mail.test.ru>
From: root@test.ru (root)

Test
*** HEADER EXTRACTED deferred/6/652E93A696 ***
*** MESSAGE FILE END deferred/6/652E93A696 ***
```

Ваши вопросы?

Маршрут вебинара

Протокол SMTP

↓

Технологии DKIM, DMARC, SPF

↓

Postfix

↓

Dovecot (IMAP, POP3)

POP3 и IMAP

POP3

POP3 (англ. Post Office Protocol Version 3 — протокол почтового отделения, версия 3)

- порт 110/TCP (без SSL)
- порт 995/TCP (over SSL)
- загружает сообщения с сервера на локальный клиент
- удаляет сообщения с сервера
- работает только в одном направлении (сервер -> клиент)
- описан в https://tools.ietf.org/html/rfc1939
- аутентификация **SASL** (англ. Simple Authentication and Security Layer — простой уровень аутентификации и безопасности)

IMAP

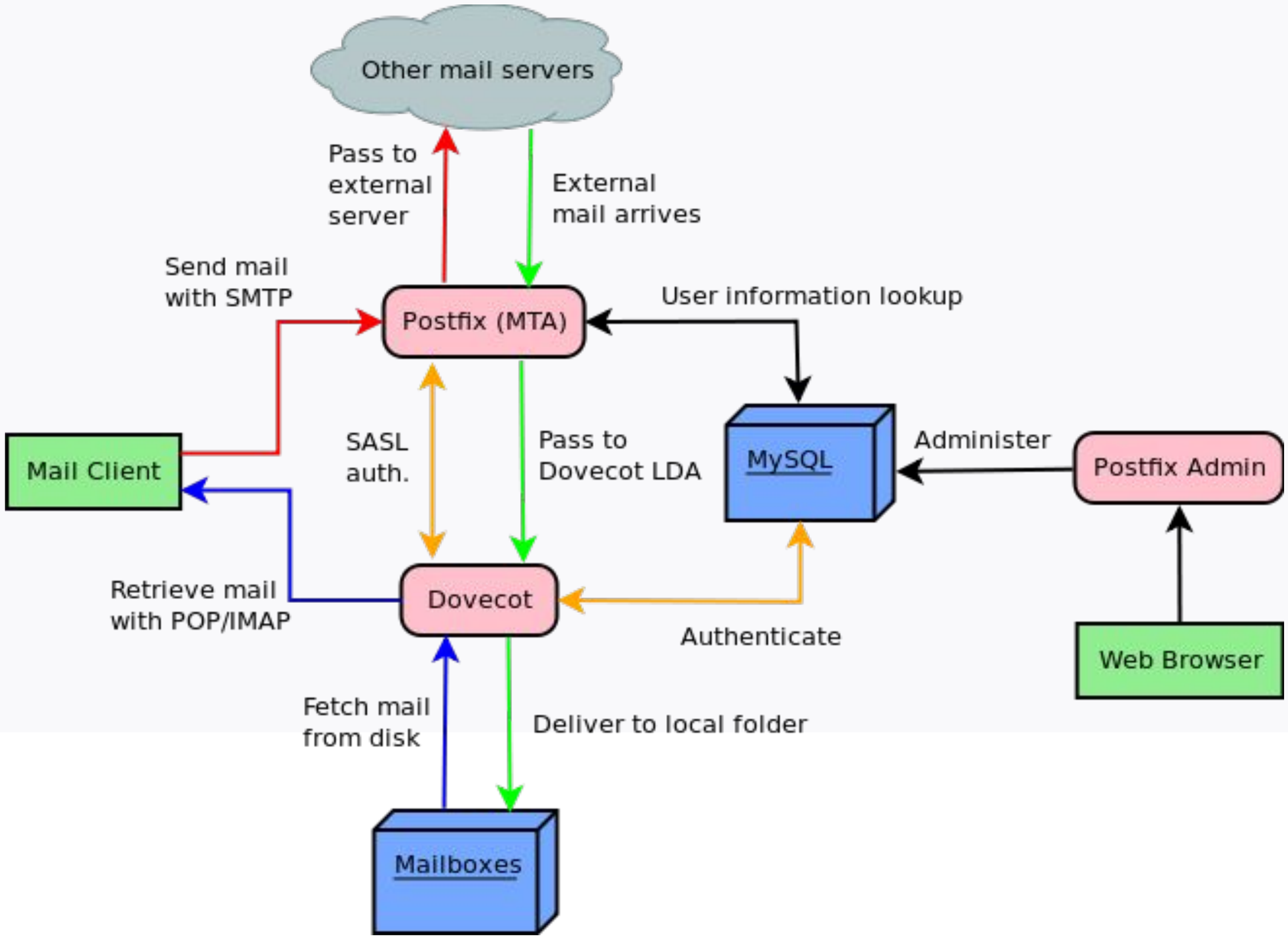
IMAP (англ. Internet Message Access Protocol)

- порт 143/TCP (без SSL)
- порт 993/TCP (over SSL)
- работает с сообщениями на сервере
- не требует пересылки полного содержания сообщений
- отслеживает состояние сообщений
- дает возможность работать нескольким клиентам с одним почтовым ящиком
- описан в https://tools.ietf.org/html/rfc3501 (версия 4, 2003 г.)

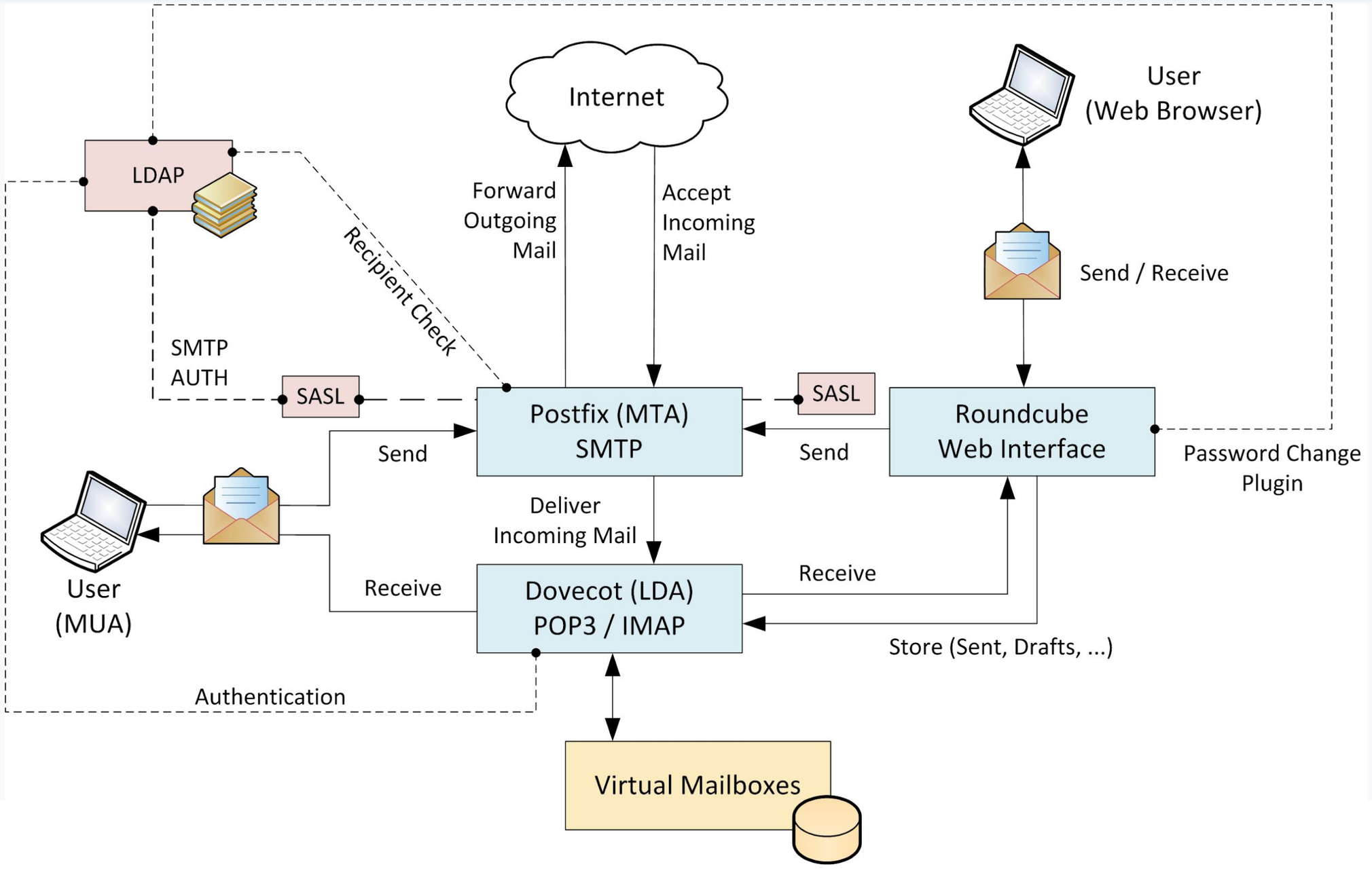
Ваши вопросы?

Dovecot

Dovecot


Other mail servers
Pass to external server
External mail arrives
Send mail with SMTP
Postfix (MTA)
User information lookup
Mail Client
SASL auth.
Pass to Dovecot LDA
MySQL
Administer
Postfix Admin
Retrieve mail with POP/IMAP
Dovecot
Authenticate
Web Browser
Fetch mail from disk
Deliver to local folder
Mailboxes

Dovecot


Internet
User
(Web Browser)
LDAP
Recipient Check
Forward
Outgoing
Mail
Accept
Incoming
Mail
Send / Receive
SMTP
AUTH
SASL
SASL
Postfix (MTA)
SMTP
Roundcube
Web Interface
Send
Send
Password Change
Plugin
Deliver
Incoming Mail
User
(MUA)
Receive
Receive
Dovecot (LDA)
POP3 / IMAP
Store (Sent, Drafts, ...)
Authentication
Virtual Mailboxes

Dovecot

Dovecot - свободный IMAP и POP3 сервер

- поддержка форматов почтовых ящиков mbox и Maildir, а также собственные форматы dbox и Cydir
- поддержка общих ящиков и папок (shared mailboxes and folders)
- поддерживает квоты
- высокое быстродействие благодаря индексации содержимого ящиков
- поддерживает LDAP и SSL
- расширяемый (поддерживает плагины)
- возможность модификации индексов с разных серверов
- безопасный

Dovecot: конфигурация

Варианты взаимодействия Postfix и Dovecot

Варианты взаимодействия Postfix и Dovecot

1. **Postfix - MTA + LDA, Dovecot - MDA**

Плюсы:

- наиболее простая конфигурация
- подходит для небольших инсталляций

Минусы:

- необходимость Dovecot сканировать maildir пользователя

Варианты взаимодействия Postfix и Dovecot

1. **Postfix - MTA + LDA, Dovecot - MDA**

/etc/postfix/main.cf
virtual_alias_domains = example.com ...other hosted domains…
virtual_alias_maps = hash:/etc/postfix/virtual
virtual_mailbox_base = /var/mail/mydomain
virtual_mailbox_maps = hash:/etc/postfix/vmailbox
virtual_minimum_uid = 100
virtual_uid_maps = static:5000
virtual_gid_maps = static:5000

/etc/postfix/vmailbox
info@example.com info/Maildir
sales@example.com sales/Maildir
Comment out the entry below to implement a catch-all.
@example.com catchall/Maildir
...virtual mailboxes for more domains…

/etc/postfix/virtual
postmaster@example.compostmaster

/etc/dovecot/dovecot.conf
mail_location = mailbox:/var/mail/mydomain/%u

Варианты взаимодействия Postfix и Dovecot

2. **Postfix - MTA, Dovecot - LDA + MDA**

Плюсы:

- подходит для любых инсталляций

Минусы:

- более сложная настройка

Варианты взаимодействия Postfix и Dovecot

2. **Postfix - MTA, Dovecot - LDA + MDA**

/etc/postfix/master.cf

```
dovecot unix - n n - - pipe
  flags=DRhu user=vmail:vmail argv=/usr/lib/dovecot/deliver -f ${sender} -d $(recipient)
```

/etc/postfix/main.cf

```
dovecot_destination_recipient_limit = 1
virtual_mailbox_domains = your.domain.here
virtual_transport = dovecot
```

/etc/dovecot/dovecot.conf

```
mail_home = /var/vmail
mail_location = mailbox:/var/vmail/mydomain/%u
passdb {
driver = passwd-file
args = scheme=sha256 username_format=%n /etc/dovecot/users
}
userdb {
driver = passwd-file
args = username_format=%n /etc/dovecot/users
default_fields = id=vmail id=vmail home=/var/vmail/%u
}
```

Варианты взаимодействия Postfix и Dovecot

2. **Postfix - MTA, Dovecot - LDA + MDA**

/etc/dovecot/users
user1:{SHA256}pmWkWSBCL51Bfkhn79xPuKBKHz//H6B+mY6G9/eieuM=::::::

doveadm pw -s SHA256
Enter new password:
Retype new password:
{SHA256}47DEQpj8HBSa+/TImW+5JCeuQeRkm5NMpJWZG3hSuFU=

Варианты взаимодействия Postfix и Dovecot

3. **Postfix - MTA, Dovecot - LDA + MDA (mysql)**

/etc/dovecot/conf.d/auth-sql.conf.ext

```
passdb {
  driver = sql
  # Path for SQL configuration file, see example-config/dovecot-sql.conf.ext
  args = /etc/dovecot/dovecot-sql.conf.ext
}
userdb {
  driver = sql
  args = /etc/dovecot/dovecot-sql.conf.ext
}
  #driver = static
  #args = uid=vmail gid=vmail home=/var/vmail/%u
```

/etc/dovecot/dovecot-sql.conf.ext

```
driver = mysql
connect = host=127.0.0.1 dbname=postfix user=postfixuser password=postfix
default_pass_scheme = MD5-CRYPT
password_query = SELECT username as user, password FROM mailbox WHERE username = '%u'
user_query = SELECT '/vmail/%d/%n' AS home, 1150 AS uid, 5000 AS gid, CONCAT('*:bytes=', CAST(quota AS
CHAR)) AS quota_rule FROM mailbox WHERE username = '%u' AND active = '1'
```

Варианты взаимодействия Postfix и Dovecot

4. **Postfix: авторизация через Dovecot**

/etc/dovecot/dovecot.conf

```
service auth {
...
unix_listener /var/spool/postfix/private/auth {
mode = 0660
# Assuming the default Postfix user and group
user = postfix
group = postfix
}
...
}
auth_mechanisms = plain login
```

/etc/postfix/main.cf

```
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_relay_restrictions = permit_mynetworks, permit_sasl_authenticated, ...
```

Варианты взаимодействия Postfix и Dovecot

4. **Dovecot + SSL:**

/etc/dovecot/conf.d/10-ssl.conf

```
ssl = yes

ssl_cert = </etc/letsencrypt/live/mydomain.ru/cert.pem
ssl_key = </etc/letsencrypt/live/mydomain.ru/privkey.pem
ssl_ca = </etc/letsencrypt/live/mydomain.ru/chain.pem
```

Ваши вопросы?

Рефлексия

Назовите 3 момента, которые вам запомнились в процессе занятия

Что вы будете применять в работе из сегодняшнего вебинара?

Список материалов для изучения

- Один из гайдов с Хабра: https://habr.com/ru/post/193220/
- Очень подробный гайд по Postfix: http://dummyluck.com/page/postfix_konfiguracia_nastroika
- Сервис проверки доменов в блэк-листах: https://whatismyipaddress.com/blacklist-check
- Сервис проверки доменов в блэк-листах: http://www.anti-abuse.org/multi-rbl-check
- Многофункциональный сервис онлайн-проверок: https://mxtoolbox.com
- Сервис для проверки SMTP-сервера: https://www.wormly.com/test-smtp-server

Заполните, пожалуйста,
опрос о занятии по ссылке в чате

Спасибо за внимание!

Приходите на следующие вебинары

Викирюк Павел

Системный инженер