Работу выполнил студент

Абраамян Александр Манвелович,
группа 5130904/10101,
4 курс

Ответы на вопросы

1.1 MTA, MDA, MUA

MTA – Почтовый транспортный агент

Это нужно для пересылки почты с одного почтового сервера на другой. Этот компонент отвечает за пересылку почты между серверами. Он получает письмо от отправителя и передаёт его дальше по маршруту к серверу получателя. MTA работает по протоколу SMTP (Simple Mail Transfer Protocol).

> Примеры:
>
> - Postfix
> - Exim
> - Sendmail
> - Microsoft Exchange

MDA (Mail Delivery Agent) – Почтовый агент доставки

Простыми словами - это хранилище. После того как письмо попадает на почтовый сервер получателя, его нужно доставить в почтовый ящик пользователя. Этим занимается MDA. Он получает письмо от MTA и кладёт его в соответствующий почтовый ящик на сервере.

> Примеры:
>
> - Dovecot
> - Procmail
> - Maildrop

MDA может работать с разными форматами хранения почты, например:

> - Maildir (каждое письмо — отдельный файл)
> - mbox (все письма в одном файле)

3. MUA (Mail User Agent) – Почтовый клиент Это то, чем мы пользуемся ежедневно. Это программа, которой пользователь читает и отправляет письма. MUA может быть как десктопным приложением, так и веб-клиентом.

> - Примеры:

> - Thunderbird
> - Outlook

> - Apple Mail
> - Roundcube (веб-клиент)

MUA получает письма с сервера с помощью POP3 (Post Office Protocol 3) или IMAP (Internet Message Access Protocol), а отправляет через SMTP.

1.2 SMTP, POP3, IMAP

SMTP

SMTP — это протокол для отправки электронной почты между серверами и клиентами. Он работает по TCP-порту 25 (для серверов), 587 (для аутентифицированной отправки), или 465 (с шифрованием SSL).

SMTP не используется для получения почты — для этого есть IMAP и POP3.

Код	Описание
220	Сервер готов
250	Команда принята успешно
354	Ожидается ввод данных письма
421	Сервер перегружен, попробуйте позже
450	Почтовый ящик временно недоступен
550	Почтовый ящик не существует
530	Требуется аутентификация
235	Аутентификация успешна

Выполнив команду `nc smtp.google.com 25` мы можем увидеть подобный результат:

```
220 mx.google.com ESMTP 38308e7fff4ca-30925e1ebeesi45649441fa.480 - gsmtp
```

Это означает что сервер готов к взаимодействию Отправим ему стркоу `EHLO google.com` означающую что мы хотим подключиться к домену google.com В ответ получим список доступных расширений:

```
250-mx.google.com at your service, [95.214.9.46]
250-SIZE 157286400 - максимальный размер письма
250-8BITMIME - поддержка 8-битных MIME-приложений
250-STARTTLS - поддержка TLS
250-ENHANCEDSTATUSCODES - поддержка расширённых кодов состояний
250-PIPELINING - поддержку одновременно нескольких комманд
250-CHUNKING - поддержку передачи больших писем
250 SMTPUTF8 - Поддержку UTF-8 в письмах
```

Продолжить общение мы не сможем поскольку google требует авторизации для использования комманд. `nc` не поддерживает шифрование, однако мы можем использовать `openssl` чтобы продолжить общение с почтовым сервером `openssl s_client -connect smtp.gmail.com:587 -starttls smtp` Данная команда инициализирует безопасное соединение с почтовым сервером. Введем далее `AUTH LOGIN` чтобы войти в свой гугл аккаунт. Получим пример ответа:

```
334 VXNlcm5hbWU6
```

Это означает что сервер ждет что мы введем ему логин и пароль закодированные в формате base64. После отправки и того и другого мы получим следующий ответ:

```
535-5.7.8 Username and Password not accepted. For more information, go to
535 5.7.8  https://support.google.com/mail/?p=BadCredentials 2adb3069b0e04-
5461eecf4fcsm1144677e87.172 - gsmtp
```

Дело в том что сервера гугл ограничивают доступ к их почтовому серверу сторонним программам с целью улучшения безопасности.

POP3

POP3 — это более старый и простой протокол, предназначенный для загрузки почты с сервера на локальный компьютер.

1. Почтовый клиент (например, Thunderbird, Outlook) подключается к почтовому серверу.
2. Получает все письма и скачивает их на локальный компьютер.
3. По умолчанию письма удаляются с сервера после загрузки (но можно настроить хранение копий).
4. Почтовый клиент разрывает соединение.

Плюсы POP3:

> - Работает без постоянного соединения с сервером.
> - Можно читать почту офлайн.
> - Уменьшает нагрузку на сервер (почта хранится локально).

Минусы POP3:

> - Нет синхронизации между устройствами (если скачать письма на один ПК, на другом они не появятся).
> - Папки не поддерживаются (вся почта хранится в одном списке).
> - При утере компьютера письма могут быть утеряны, если не было резервных копий.

Порты POP3:

> 110 – обычное подключение 995 – POP3 с SSL (защищённое соединение)

Команды:

```
USER your_login
PASS your_password
LIST  # список писем
RETR 1  # загрузка письма №1
DELE 1  # удаление письма №1
QUIT  # выход
```

IMAP

IMAP — более современный протокол, который позволяет работать с почтой прямо на сервере. Он подходит, если ты используешь почту на нескольких устройствах.

1. Почтовый клиент открывает подключение к серверу.
2. Клиент загружает только заголовки писем (а не всё письмо сразу).
3. Когда пользователь открывает письмо, оно загружается с сервера.
4. Письма остаются на сервере, синхронизация происходит автоматически.

Плюсы IMAP:

> - Синхронизация на всех устройствах (читаешь письмо на одном — оно прочитано везде).
> - Можно управлять папками (входящие, архив, спам и т.д.).
> - Письма хранятся на сервере → не потеряются при сбое ПК.
> - Можно искать письма прямо на сервере без загрузки всех сообщений.

Минусы IMAP:

> - Требует постоянного интернет-соединения для работы.
> - Занимает больше места на сервере.

Порты IMAP:

> - 43 – обычное подключение
> - 993 – IMAP с SSL (защищённое соединение)

Команды:

```
telnet mail.example.com 143
a1 LOGIN your_login your_password
a2 LIST "" "*"
a3 SELECT INBOX
a4 FETCH 1 BODY[]
a5 LOGOUT
```

Подключение по SMTP и отправка письма

```
openssl s_client -connect smtp.yandex.ru:465
```

```
220 mail-nwsmtp-smtp-production-main-91.iva.yp-c.yandex.net Ok 1739976765-
iqXj0G0Og0U0
EHLO yandex.ru
250-mail-nwsmtp-smtp-production-main-91.iva.yp-c.yandex.net
250-8BITMIME
250-PIPELINING
250-SIZE 53477376
250-STARTTLS
250-AUTH LOGIN PLAIN XOAUTH2
250-DSN
250 ENHANCEDSTATUSCODES
------------- AUTH LOGIN
334 VXNlcm5hbWU6
------------- base64 login nononomisterfish@yandex.ru
334 UGFzc3dvcmQ6
------------- base64 application password
235 2.7.0 Authentication successful. 1739976850-iqXj0G0Og0U0
MAIL FROM:<nononomisterfish@yandex.ru>
250 2.1.0 Ok
RCPT TO:<nononomisterfish@yandex.ru>
250 2.1.5 Ok
DATA
354 Enter message, ending with "." on a line by itself
Subject: Test email from openssl

This is a test email sent from openssl.
.
250 2.0.0 Ok: queued as 1739976850-iqXj0G0Og0U0
QUIT
```

Подключение по IMAP и получение писем

```
➜  ~ openssl s_client -connect imap.yandex.ru:993 -crlf
CONNECTED(00000003)
depth=2 OU = GlobalSign Root CA - R3, O = GlobalSign, CN = GlobalSign
verify return:1
depth=1 C = BE, O = GlobalSign nv-sa, CN = GlobalSign RSA OV SSL CA 2018
verify return:1
depth=0 C = RU, ST = Moscow, L = Moscow, O = YANDEX LLC, CN =
imap.yandex.ru
verify return:1
---
Certificate chain
 0 s:C = RU, ST = Moscow, L = Moscow, O = YANDEX LLC, CN = imap.yandex.ru
   i:C = BE, O = GlobalSign nv-sa, CN = GlobalSign RSA OV SSL CA 2018
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Sep 16 12:23:09 2024 GMT; NotAfter: Mar 16 20:59:59 2025
```

```
GMT
 1 s:C = BE, O = GlobalSign nv-sa, CN = GlobalSign RSA OV SSL CA 2018
   i:OU = GlobalSign Root CA - R3, O = GlobalSign, CN = GlobalSign
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Nov 21 00:00:00 2018 GMT; NotAfter: Nov 21 00:00:00 2028
GMT
 2 s:OU = GlobalSign Root CA - R3, O = GlobalSign, CN = GlobalSign
   i:C = BE, O = GlobalSign nv-sa, OU = Root CA, CN = GlobalSign Root CA
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Sep 19 00:00:00 2018 GMT; NotAfter: Jan 28 12:00:00 2028
GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIGzjCCBbagAwIBAgIMMERAs6b+6+z7RayHMA0GCSqGSIb3DQEBCwUAMFAxCzAJ
BgNVBAYTAkJFMRkwFwYDVQQKExBHbG9iYWxTaWduIG52LXNhMSYwJAYDVQQDEx1H
...
xDKybz5AaAgcvnBy8d5aMR/083eBrKEGf9E+p2fNma5LseD0JGW2LAWQrWiQWBQl
T7bIJazWoZ2d+x3CR/e8UVsY6T6pqdhhWAwFrMMQjXiiliMcNrUSc6ABTk7WEec7
lFU8r77xlCe94SRUEzIVGz76
-----END CERTIFICATE-----
subject=C = RU, ST = Moscow, L = Moscow, O = YANDEX LLC, CN =
imap.yandex.ru
issuer=C = BE, O = GlobalSign nv-sa, CN = GlobalSign RSA OV SSL CA 2018
---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA-PSS
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 4524 bytes and written 396 bytes
Verification: OK
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
---
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID:
168FF3509C10D7A47C925CCBC342E2ED1154897F88FC686FC46CAA7F67EB711A
    Session-ID-ctx:
    Resumption PSK:
6417EC688E54B1E281766A9D276A0A884CD0DFB0E2F4162C5BA5EEFCC17ED5B4242E9D07D1A
950DEA66D03193480A84B
    PSK identity: None
```

```
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - 28 f8 97 b6 92 72 b5 f2-16 2c 4c 5b 6a d8 51 76
(....r...,L[j.Qv
    0010 - 01 4c 7f 3c e7 e0 53 62-68 95 32 2e a8 fe 93 4b   .L.
<..Sbh.2....K
    0020 - 8e 12 d3 c1 36 bc b1 e1-20 36 37 87 1a ba 2b a6   ....6...
67...+.
    0030 - d1 e6 03 24 ea d9 1a 22-d3 3f c2 17 5c 61 fb 44
...$..."."?..\a.D
    0040 - c1 f2 87 30 2c ca 4e 00-31 7b ba 36 20 ce a3 6c   ...0,.N.1{.6
..l
    0050 - 4f 8b 1e 0b 06 9c 0b 19-e9 57 01 1b fc 25 ad f0
O........W...%..
    0060 - 00 96 79 e1 ed f1 b4 2e-3a 92 cb 5e f5 51 76 82
..y.....:..^.Qv.
    0070 - b2 75 9b 0d 0d 4a 94 e5-62 a9 cc 41 bd f4 53 e0
.u...J..b..A..S.
    0080 - ef 07 d5 88 cc ef 31 15-af 53 bd dd 64 d8 03 e3
......1..S..d...
    0090 - 26 9b 10 10 4c e5 36 70-1f e2 a5 6a c5 3e 2a a9
&...L.6p...j.>*.
    00a0 - ef e7 71 0c 10 b0 6a 09-a3 7f df 5b 8b d6 8c ab   ..q...j....
[....
    00b0 - de f5 e9 15 1e 1e 65 21-52 57 e1 22 dd 93 ef e7
......e!RW."....

    Start Time: 1739977449
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID:
5E4BC7C26AADBA44AA6217FC344044C752B2999E7932FBAB44CC4B83CFBAF5B2
    Session-ID-ctx:
    Resumption PSK:
566813BEE10EA5BD6E3A41F2EFEE6027771383D7153CA9D6AE9551CB372839DF9710183F297
AD0AC490E1111938EA1F1
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - 28 f8 97 b6 92 72 b5 f2-16 2c 4c 5b 6a d8 51 76
(....r...,L[j.Qv
```

```
    0010 - 26 2b 51 8c e6 2d 58 f2-d3 b3 a7 69 a1 ee d7 43   &+Q..-
X....i...C
    0020 - a2 d0 57 29 04 ab 92 67-88 fb fb 80 1b 6f a9 0f
..W)...g.....o..
    0030 - 37 80 e3 36 c5 c3 30 fe-77 09 a5 e4 bf 6d a8 da
7..6..0.w....m..
    0040 - 23 6a 92 97 86 3f 6c 5a-4c b1 d8 8a 7c 46 8a a7   #j...?
lZL...|F..
    0050 - 05 7d a8 7a d3 99 50 ec-cb 17 a2 e7 69 75 06 02
.}.z..P.....iu..
    0060 - 2d 9a cf 25 1c 30 fa af-20 06 b6 59 c1 17 be 4e   -..%.0..
..Y...N
    0070 - 40 fb be 15 e2 44 b2 50-e8 c2 93 d3 88 0c 79 33
@....D.P......y3
    0080 - 35 47 5a 35 81 63 b9 db-d6 e6 75 e8 e7 75 88 02
5GZ5.c....u..u..
    0090 - de 34 de 5d f0 01 5a 37-84 a2 46 93 5d 0b ba 83
.4.]..Z7..F.]...
    00a0 - 5c d1 e8 2b 08 92 42 a8-b3 0f a9 86 2e 58 5f 86
\..+..B......X_.
    00b0 - 1e 05 ee 14 52 4a 9f 6d-d3 f4 3c 1b 6f fb 40 fc   ....RJ.m..
<.o.@.

    Start Time: 1739977449
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
* OK Yandex IMAP4rev1 at mail-imap-production-main-914.iva.yp-
c.yandex.net:993 ready to talk with ::ffff:104.28.254.16:12010, 2025-Feb-19
18:04:09, 84YdbG07SiE0
a1 LOGIN nononomisterfish@yandex.ru vdyspdaotnvtzswk
* CAPABILITY IMAP4rev1 CHILDREN UNSELECT LITERAL+ NAMESPACE XLIST UIDPLUS
ENABLE ID IDLE MOVE
a1 OK LOGIN Completed.
a2 LIST "" "*"
* LIST (\HasNoChildren \Unmarked \Sent) "|"
"&BB4EQgQ,BEAEMAQyBDsENQQ9BD0ESwQ1-"
* LIST (\HasNoChildren \Unmarked) "|" "&BBgEQQRFBD4ENARPBEkEOAQ1-"
* LIST (\HasNoChildren \Unmarked \Junk) "|" "&BCEEPwQwBDw-"
* LIST (\HasNoChildren \Unmarked \Trash) "|" "&BCMENAQwBDsENQQ9BD0ESwQ1-"
* LIST (\HasChildren \Unmarked \Drafts) "|" "&BCcENQRABD0EPgQyBDgEOgQ4-"
* LIST (\HasNoChildren \Unmarked \Templates) "|"
"&BCcENQRABD0EPgQyBDgEOgQ4-|template"
* LIST (\HasNoChildren \Marked \NoInferiors) "|" INBOX
a2 OK LIST Completed.
a3 SELECT INBOX
* FLAGS (\Answered \Seen \Draft \Deleted $Forwarded)
* 1476 EXISTS
* 434 RECENT
* OK [UNSEEN 870]
* OK [PERMANENTFLAGS (\Answered \Seen \Draft \Flagged \Deleted $Forwarded
```

```
\*)] Limited
* OK [UIDNEXT 1621] Ok
* OK [UIDVALIDITY 1486825895] Ok
a3 OK [READ-WRITE] SELECT Completed.
a4 FETCH 1476 BODY[TEXT]
* 1476 FETCH (BODY[TEXT] {28652}
PCFkb2N0eXBlIGh0bWw+CjxodG1sIGxhbmc9InJ1IiB4bWxucz0iaHR0cDovL3d3dy53My5vcmc
v
MTk5OS94aHRtbCIgeG1sbnM6dj0idXJuOnNjaGVtYXMtbWljcm9zb2Z0LWNvbTp2bWwiIHhtbG5
z
...
IG1zbyB8IElFXT48L3RkPjwvdHI+PC90YWJsZT48IVtlbmRpZl0tLT4KCgogICAgICA8L2Rpdj4
K
CiAgPC9ib2R5Pgo8L2h0bWw+
 FLAGS (\Seen \Recent encrypted system_hamon))
a4 OK FETCH Completed.
a4 FETCH 1476 BODY[HEADER]
* 1476 FETCH (BODY[HEADER] {2104}
Received: from postback2b.mail.yandex.net (postback2b.mail.yandex.net
[2a02:6b8:c02:900:1:45:d181:da02])
    by ex2h5p3b5xbxshul.sas.yp-c.yandex.net (notsolitesrv/Yandex) with
LMTPS id Tpe3f7gHY2vN-Z6ARGnAx
    for <nononomisterfish@yandex.ru>; Wed, 19 Feb 2025 17:46:22 +0300
Received: from mail-nwsmtp-yaback-production-main-31.iva.yp-c.yandex.net
(mail-nwsmtp-yaback-production-main-31.iva.yp-c.yandex.net
[IPv6:2a02:6b8:c0c:7315:0:640:79c0:0])
    by postback2b.mail.yandex.net (Yandex) with ESMTPS id CCF5A60910
    for <nononomisterfish@yandex.ru>; Wed, 19 Feb 2025 17:46:22 +0300 (MSK)
Received: from qavm-f636cfe0.qemu (passport-api-stable-passport-api-
81.sas.yp-c.yandex.net [2a02:6b8:c37:6a4c:0:657d:8ae3:0])
    by mail-nwsmtp-yaback-production-main-31.iva.yp-c.yandex.net
(yaback/Yandex) with ESMTPS id MkX06t2MeqM0-R6y4zJIB;
    Wed, 19 Feb 2025 17:46:22 +0300
X-Yandex-Fwd: 1
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=id.yandex.ru;
    s=mail; t=1739976382;
    bh=75xV3ItDrtn7oyEAubd5n0zxoyb6iWl1Z0RWBXDHjW0=;
    h=Message-Id:Reply-To:Date:Subject:To:From;
    b=eLt8ICRDvsYWNJPij9oCgbgElRTDP4N+8Pc3cZJUxzEYxu3E/zuzXYWlTs4U6g5r9
     D1sETwZGSoFpQv0olPf6yulf/x29i+ATj6CN+YBo6txG6Y7+AP3cCwf/bwGflwTsNI
     4JD9q6s+j48Tr2rdKfsLKNVnTsuHkL1pOK7OgYmA=
Authentication-Results: mail-nwsmtp-yaback-production-main-31.iva.yp-
c.yandex.net; dkim=pass header.i=@id.yandex.ru
X-Yandex-Spam: 1
Received: by qavm-f636cfe0.qemu (Postfix, from userid 0)
    id 6599F7A50BD5; Wed, 19 Feb 2025 17:46:22 +0300 (MSK)
Content-Type: text/html; charset="utf-8"
MIME-Version: 1.0
Content-Transfer-Encoding: base64
Subject: =?utf-8?b?
0JLRiyDRgdC+0LfQtNCw0LvQuCDQv9Cw0YDQvtC70Ywg0LTQu9GPINC/?=
 =?utf-8?b?
0YDQuNC70L7QttC10L3QuNGPINCyINCw0LrQutCw0YPQvdGC0LUgYWJyYWFteWFu?=
 =?utf-8?b?LnNodXJh?=
```

```
From: =?utf-8?b?0K/QvdC00LXQutGBIElEIA==?= <noreply@id.yandex.ru>
To: nononomisterfish@yandex.ru
Date: Wed, 19 Feb 2025 14:46:22 -0000
Reply-To: noreply@id.yandex.ru
Message-Id: <20250219144622.6599F7A50BD5@qavm-f636cfe0.qemu>
Return-Path: noreply@id.yandex.ru
X-Yandex-Forward: 9c98f71c1f5b6884b6ebda62d269353e

)
a4 OK FETCH Completed.
a6 LOGOUT
* BYE IMAP4rev1 Server logging out
a6 OK LOGOUT Completed.
40C7394A88740000:error:0A000119:SSL routines:ssl3_get_record:decryption
failed or bad record mac:../ssl/record/ssl3_record.c:613:
```