Санкт-Петербургский политехнический университет Петра Великого
Кафедра компьютерных систем и программных технологий

Отчёт по лабораторной работе

Дисциплина: Разработка сетевых приложений

Тема: Изучение прикладных протоколов в командной строке Linux

Выполнил студент гр. 43501/3 Мальцев М.С.
Преподаватель Зозуля А.В.

Санкт-Петербург
17 февраля 2019 г.

1 SMTP

1.1 Основные сведения о протоколе

Simple Mail Transfer Protocol (SMTP) - это интернет протокол для обмена почтой. Впервые был зафиксирован в RFC 821 в 1982 году. Был изменен в 2008 году RFC 5321. Используется по сегодняшний день.

1.2 Основные команды

Команды SMTP:

- EHLO - используется для приветствия в протоколе ESMTP. Рекомендуется к использованию по возможности
- HELO - команда приветствия. Используется для начала сессии
- MAIL FROM - задается адрес отправителя
- RCPT TO - указывается получатель
- DATA - текст сообщения
- QUIT - выход
- HELP - списокк доступных команд или описание запрашиваемой команды
- NOOP - пустая команда, предположительно используется для поддержания соединения
- RSET - сброс

1.3 Область применения и ограничения протокола

Простой протокол передачи почты (SMTP), используется для связи с удаленным сервером и последующей отправке сообщений с локального клиента на удаленный сервер, и в конечном итоге на сервер получателя сообщений. На вашем сервере электронной почты, этот процесс контролируется специальной службой (MTA). Стоит упомянуть, что SMTP используется исключительно для отправки сообщений.

Порты SMTP:
Порт 25 – порт без шифрования
Порт 465 – порт SSL/TLS, также известный как SMTPS

1.4 Пример использования

```
openssl s_client -connect smtp.yandex.ru:465
                    [...]
220 smtp4o.mail.yandex.net ESMTP (Want to use Yandex.Mail for your domain? Visit
    http://pdd.yandex.ru)
helo host
250 smtp4o.mail.yandex.net
auth login
334 VXNlcm5hbWU6
byolo1234Tk3
334 UGFzc3dvcmQ6
N3XoyolobHlyolouamyoloRjyoloQm123jM=
235 2.7.0 Authentication successful.
mail from: <mikle9997@yandex.ru>
250 2.1.0 <mikle9997@yandex.ru> ok
rcpt to: <mikle9997@yandex.ru>
250 2.1.5 <mikle9997@yandex.ru> recipient ok
data
354 Enter mail, end with "." on a line by itself
From: mikle9997@ya.ru
To: mikle9997@ya.ru
Subject: Hello world!

This is the test message...
new line
.
250 2.0.0 Ok: queued on smtp4o.mail.yandex.net as 1550417106-ffkNcyAJLD-NlO4FHGx
quit
221 2.0.0 Closing connection.
read:errno=0
```

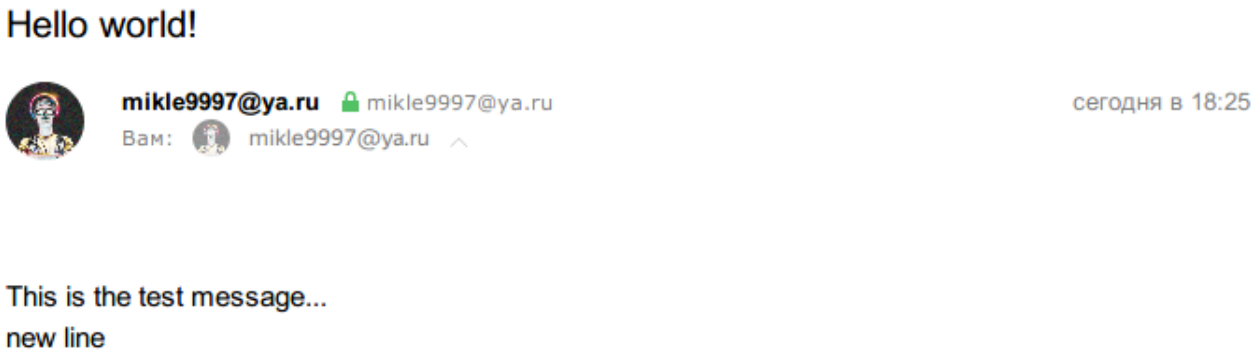

Рис. 1.1: Собщение отправленное с использованием протокола smtp

2 POP3

2.1 Основные сведения о протоколе

POP3 (англ. Post Office Protocol Version 3 — протокол почтового отделения, версия 3) — стандартный интернет-протокол прикладного уровня, исполь-

зуемый клиентами электронной почты для получения почты с удалённого сервера по TCP-соединению.

2.2 Основные команды

Команды POP3:

- USER - передаёт серверу имя пользователя
- PASS - передаёт серверу пароль почтового ящика.
- DELE - сервер помечает указанное сообщение для удаления. Сообщения, помеченные на удаление, реально удаляются только после закрытия транзакции (закрытие транзакций происходит обычно после посыла команды QUIT, кроме этого, например, на серверах закрытие транзакций может происходить по истечении определённого времени, установленного сервером).
- LIST - если был передан аргумент, то сервер выдаёт информацию об указанном сообщении. Если аргумент не был передан, то сервер выдаёт информацию обо всех сообщениях, находящихся в почтовом ящике. Сообщения, помеченные для удаления, не перечисляются
- NOOP - сервер ничего не делает, всегда отвечает положительно
- RETR сообщение - сервер передаёт сообщение с указанным номером
- RSET - этой командой производится откат транзакций внутри сессии. Например, если пользователь случайно пометил на удаление какие-либо сообщения, он может убрать эти пометки, отправив эту команду
- STAT -сервер возвращает количество сообщений в почтовом ящике и размер почтового ящика в октетах. Сообщения, помеченные как удалённые, при этом не учитываются.
- TOP - сервер возвращает заголовки указанного сообщения, пустую строку и указанное количество первых строк тела сообщения.

2.3 Область применения и ограничения протокола

POP3 (протокол почтового отделения версия 3) часто используется для связи с удаленным сервером электронной почты и загрузки сообщений на локальный почтовый клиент с последующим удалением его на сервере, к примеру Outlook, Thunderbird, Windows Mail, Mac Mail и т.д. Однако обычно почтовые клиенты предлагают выбор – оставлять или нет копии сообщений на

сервере. Если вы используете несколько устройств для отправки сообщений, то рекомендуется оставлять эту функцию включенной, в противном случае, на другом устройстве у вас не будет доступа к отправленным сообщениям, которые не были сохранены на удаленном сервере. Также стоит отметить, что POP3 – протокол работающий только в одном направлении, это означает, что данные берутся с удаленного сервера и отправляются на локальный клиент.

Порты POP3, по умолчанию являются такими:

Порт 110 – порт без шифрования

Порт 995 – порт SSL/TLS, также известный как POP3S

2.4 Пример использования

```
openssl s_client -connect pop.yandex.ru:995
        [...]
+OK POP Ya! na@8o 4vVwfiwuP0U1
user mikle9997@yandex.ru
+OK password, please.
pass yoloyoloyoloyoloyolo
+OK 141 8600172
stat
+OK 141 8600172
list
+OK 141 8600172
1 1714
2 8768
        [...]
140 7116
141 9267
.
noop
+OK noop
top 1 0
+OK 1714 octets.
X-Yandex-FolderName: Inbox
Received: from mxback13j.mail.yandex.net ([127.0.0.1])
    by mxback13j.mail.yandex.net with LMTP id SsFBoMrt
    for <mikle9997@yandex.ru>; Sun, 17 Feb 2019 18:25:06 +0300
Received: from mxback13j.mail.yandex.net (localhost.localdomain [127.0.0.1])
    by mxback13j.mail.yandex.net (Yandex) with ESMTP id 2F97268C1381
    for <mikle9997@yandex.ru>; Sun, 17 Feb 2019 18:25:06 +0300 (MSK)
X-Yandex-Internal: 1
Received: from smtp4o.mail.yandex.net (smtp4o.mail.yandex.net [2a02:6b8:0:1a2d
    ::28])
    by mxback13j.mail.yandex.net (nwsmtp/Yandex) with ESMTP id MbcW9nq0Ig-
    P6TuLGrX;
    Sun, 17 Feb 2019 18:25:06 +0300
X-Yandex-Front: mxback13j.mail.yandex.net
X-Yandex-TimeMark: 1550417106
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yandex.ru; s=mail; t
    =1550417106;
    bh=oMGQU4hVaHd+pvDa94cg5wNw8zPI8KCe9zxGqUAP3Wg=;
    h=Message-Id:Date:From:To:Subject;
    b=Se3jbrZfgy6Nz0YpKkEJS2uiPxYB/HhciwfWJUJtLP0mYlgcUYsy897kDLz5nKPY9
     otEKZCclw7lVgda/KhUck60jFCeqcIchBtZzzzHQS3RJUcXbTjrcw3Cfw0NR5WsC1o
```

```
40       x6n7SMIZe4AyNKjusoPI/X3VT1xCo3ddYQ9VaaGE=
41 Authentication-Results: mxback13j.mail.yandex.net; dkim=pass header.i=@yandex.ru
42 Received: by smtp4o.mail.yandex.net (nwsmtp/Yandex) with SMTP id ffkNcyAJLD-
       NlO4FHGx;
43      Sun, 17 Feb 2019 18:23:55 +0300
44      (using TLSv1.2 with cipher ECDHE-RSA-AES128-GCM-SHA256 (128/128 bits))
45      (Client certificate not present)
46 X-Yandex-Front: smtp4o.mail.yandex.net
47 X-Yandex-TimeMark: 1550417035
48 Message-Id: <20190217182505.NlO4FHGx@smtp4o.mail.yandex.net>
49 Date: Sun, 17 Feb 2019 18:25:05 +0300
50 X-Yandex-Spam: 1
51 From: mikle9997@ya.ru
52 To: mikle9997@ya.ru
53 Subject: Hello world!
54 Return-Path: mikle9997@yandex.ru
55 .
56 quit
57 +OK shutting down.
58 read:errno=0
```

3 IMAP

3.1 Основные сведения о протоколе

IMAP (англ. Internet Message Access Protocol) — протокол прикладного уровня для доступа к электронной почте.

IMAP предоставляет пользователю обширные возможности для работы с почтовыми ящиками, находящимися на центральном сервере. Почтовая программа, использующая этот протокол, получает доступ к хранилищу корреспонденции на сервере так, как будто эта корреспонденция расположена на компьютере получателя. Электронными письмами можно манипулировать с компьютера пользователя (клиента) без постоянной пересылки с сервера и обратно файлов с полным содержанием писем.

3.2 Основные команды

Команды IMAP:

- LOGIN - позволяет клиенту при регистрации на сервере IMAP использовать идентификатор пользователя и пароль в обычном текстовом виде. Это не самый лучший метод, но иногда это единственная возможность подключиться к серверу
- CLOSE - закрывает почтовый ящик. Когда почтовый ящик закрыт с помощью этой команды, то сообщения, помеченные флагом DELETED, удаляются из него. Не имеет параметров

- LOGOUT - завершает сеанс для текущего идентификатора пользователя
- DELETE - применяется к почтовым ящикам. Сервер IMAP при получении этой команды попытается удалить почтовый ящик с именем, указанным в качестве аргумента команды. Сообщения удаляются вместе с ящиками и восстановлению не подлежат
- LIST - получить список всех почтовых ящиков клиента; имеет два параметра
- LSUB - в отличие от команды LIST используется для получения списка ящиков, активизированных командой SUBSCRIBE. Параметры — такие же, как у LIST
- EXPUNGE - удаляет из почтового ящика все сообщения, помеченные флагом DELETED, при этом почтовый ящик не закрывается. Ответ сервера на команду EXPUNGE представляет собой отчёт о новом состоянии почтового ящика
- FETCH - получить текст почтового сообщения. Команда применяется только для отображения сообщений. В отличие от POP3, клиент IMAP не сохраняет копию сообщения на клиентском ПК
- SEARCH - поиск сообщений по критериям в активном почтовом ящике с последующим отображением результатов в виде номера сообщения. Возможен поиск сообщений, в теле которых имеется определённая текстовая строка, или имеющих определённый флаг, или полученных до определённой даты и т.д.
- NOOP - команда ничего не делает

3.3 Область применения и ограничения протокола

IMAP, также как и POP3 используется для получения сообщений электронной почты на локальный клиент, однако, он имеет существенное отличие – загружаются только лишь заголовки электронных сообщений, сам текст письма остается на сервере. Данный протокол связи работает в две стороны, если происходят изменения на локальном клиенте, они передаются и на сервер. В последнее время IMAP стал более популярным, так как такие гиганты-провайдеры услуг электронной почты, как Gmail, стали рекомендовать использовать его вместо POP3.

Для отправки писем используется обычно протокол SMTP, так как собственная команда отправки протокола IMAP, называемая APPEND, считается «неудачной» и «небезопасной»

Порты IMAP, по умолчанию являются такими:
Порт 143 – порт без шифрования
Порт 993 – порт SSL/TLS, также известный как IMAPS

3.4 Пример использования

```
1 openssl s_client -crlf -connect imap.yandex.ru:993
2             [...]
3 a login username pass
```

4 HTTP

4.1 Основные сведения о протоколе

HTTP (англ. HyperText Transfer Protocol — «протокол передачи гипертекста») — протокол прикладного уровня передачи данных. Изначально — в виде гипертекстовых документов в формате «HTML», в настоящий момент используется для передачи произвольных данных.

4.2 Основные команды

Команды HTTP:

- OPTIONS - используется для определения возможностей веб-сервера или параметров соединения для конкретного ресурса
- GET - используется для запроса содержимого указанного ресурса
- HEAD - аналогичен методу GET, за исключением того, что в ответе сервера отсутствует тело
- POST - применяется для передачи пользовательских данных заданному ресурсу
- PUT - применяется для загрузки содержимого запроса на указанный в запросе URI
- DELETE - удаляет указанный ресурс

4.3 Область применения и ограничения протокола

HTTP — протокол прикладного уровня; аналогичными ему являются FTP и SMTP. Обмен сообщениями идёт по обыкновенной схеме «запрос-ответ».

Для идентификации ресурсов HTTP использует глобальные URI. В отличие от многих других протоколов, HTTP не сохраняет своего состояния. Это означает отсутствие сохранения промежуточного состояния между парами «запрос-ответ». Компоненты, использующие HTTP, могут самостоятельно осуществлять сохранение информации о состоянии, связанной с последними запросами и ответами (например, «куки» на стороне клиента, «сессии» на стороне сервера). Браузер, посылающий запросы, может отслеживать задержки ответов. Сервер может хранить IP-адреса и заголовки запросов последних клиентов. Однако сам протокол не осведомлён о предыдущих запросах и ответах, в нём не предусмотрена внутренняя поддержка состояния, к нему не предъявляются такие требования.

4.4 Пример использования

```
1 openssl s_client -crlf -connect imap.yandex.ru:993
2             [...]
3 a login username pass
```

5 FTP

5.1 Основные сведения о протоколе

FTP (англ. File Transfer Protocol) — протокол передачи файлов по сети. Гарантирует передачу (либо выдачу ошибки) за счёт применения квитируемого протокола TCP.FTP является одним из старейших прикладных протоколов, появившимся задолго до HTTP, и даже до TCP/IP, в 1971 году. В первое время он работал поверх протокола NCP. Он и сегодня широко используется для распространения ПО и доступа к удалённым хостам.

5.2 Основные команды

Команды FTP:

- ABOR — прервать передачу файла
- CDUP — сменить каталог на вышестоящий
- CWD — сменить каталог
- DELE — удалить файл (DELE filename)
- EPSV — войти в расширенный пассивный режим. Применяется вместо PASV

- HELP — выводит список команд, принимаемых сервером
- LIST — возвращает список файлов каталога. Список передаётся через соединение данных
- MDTM — возвращает время модификации файла
- MKD — создать каталог
- NLST — возвращает список файлов каталога в более кратком формате, чем LIST. Список передаётся через соединение данных
- NOOP — пустая операция
- PASS — пароль
- PASV — войти в пассивный режим. Сервер вернёт адрес и порт, к которому нужно подключиться, чтобы забрать данные. Передача начнётся при введении следующих команд: RETR, LIST и т.д.
- PORT — войти в активный режим. Например PORT 12,34,45,56,78,89. В отличие от пассивного режима для передачи данных сервер сам подключается к клиенту
- PWD — возвращает текущий каталог
- QUIT — отключиться
- REIN — реинициализировать подключение
- RETR — скачать файл. Перед RETR должна быть команда PASV или PORT
- RMD — удалить каталог
- RNFR и RNTO — переименовать файл. RNFR — что переименовывать, RNTO — во что
- SIZE — возвращает размер файла
- STOR — закачать файл. Перед STOR должна быть команда PASV или PORT
- SYST — возвращает тип системы (UNIX, WIN, . . .)
- TYPE — установить тип передачи файла (бинарный, текстовый)
- USER — имя пользователя для входа на сервер

5.3 Область применения и ограничения протокола

Типичное применение FTP-протокола — загрузка сайтов и других документов с частного устройства разработки на общедоступные сервера хостинга. Протокол FTP (как и HTTP) имеет двоичный режим передачи, что сокращает накладные расходы трафика и уменьшает время обмена данными при передаче больших файлов.

Стандартный порт управления FTP-соединением — 21.

5.4 Пример использования

```
1  220 Hello World!
2  USER anonymous
3  331 Anonymous login ok, send your complete email address as your password
4  PASS ************
5  230 Logged in anonymously.
6  PASV
7  227 Entering Passive Mode (192,168,254,253,233,92) Клиент// должен открыть
       соединение на переданный IP
8  LIST
9  150 Here comes the directory listing. Сервер// передает список файлов в каталоге
10 226 Directory send OK.
11 CWD incoming
12 250 Directory successfully changed.
13 PASV
14 227 Entering Passive Mode (192,168,254,253,207,56)
15 STOR example.avi
16 150 Ok to send data. Клиент// передает содержимое файла
17 226 File receive OK.
18 QUIT
19 221 Goodbye.
```

При помощи утилиты telnet загрузить файл с FTP-сервера ftp.sunet.se

6 TFTP

6.1 Основные сведения о протоколе

TFTP (англ. Trivial File Transfer Protocol — простой протокол передачи файлов) используется главным образом для первоначальной загрузки бездисковых рабочих станций. TFTP, в отличие от FTP, не содержит возможностей аутентификации (хотя возможна фильтрация по IP-адресу) и основан на транспортном протоколе UDP.

6.2 Основные команды

Сначала в TFTP-пакете идет поле размером в 2 байта, определяющее тип пакета:

- Read Request (RRQ, 1) — запрос на чтение файла
- Write Request (WRQ, 2) — запрос на запись файла
- Data (DATA, 3) — данные, передаваемые через TFTP
- Acknowledgment (ACK, 4) — подтверждение пакета
- Error (ERR, 5) — ошибка
- Option Acknowledgment (OACK, 6) — подтверждение опций

6.3 Область применения и ограничения протокола

Основное назначение TFTP — обеспечение простоты реализации клиента. В связи с этим он используется для загрузки бездисковых рабочих станций, загрузки обновлений и конфигураций в «умные» сетевые устройства, записи статистики с мини-АТС (CDR) и аппаратных маршрутизаторов/файрволов.

Порт 69.

6.4 Пример использования

```
1 123
```

При помощи утилиты netcat выяснить имя файла, который запрашивает удаленный хост (припомощи утилиты tftp) у данного хоста

7 WebDAV

7.1 Основные сведения о протоколе

WebDAV (Web Distributed Authoring and Versioning) или просто DAV — набор расширений и дополнений к протоколу HTTP, поддерживающих совместную работу пользователей над редактированием файлов и управление файлами на удаленных веб-серверах. В качестве миссии рабочей группы по созданию DAV было заявлено: "разработка дополнений к протоколу HTTP, обеспечивающих свободное взаимодействие инструментов распределенной разработки веб-страниц, в соответствии с потребностями работы пользователей". Однако в процессе эксплуатации DAV нашёл себе ряд других применений, выходящих за первоначально принятые рамки коллективной работы над веб-документами.

7.2 Основные команды

WebDAV расширяет HTTP следующими методами запроса:

- PROPFIND — Получение свойств объекта на сервере в формате XML. Также можно получать структуру репозитория (дерево каталогов);
- PROPPATCH — Изменение свойств за одну транзакцию;
- MKCOL — Создать коллекцию объектов (каталог в случае доступа к файлам);
- COPY — Копирование из одного URI в другой;
- MOVE — Перемещение из одного URI в другой;
- LOCK — Поставить блокировку на объекте. WebDAV поддерживает эксклюзивные и общие (shared) блокировки;
- UNLOCK — Снять блокировку с ресурса.

7.3 Область применения и ограничения протокола

Сегодня DAV применяется в качестве сетевой файловой системы, эффективной для работы в Интернете и способной обрабатывать файлы целиком, поддерживая хорошую производительность работы в условиях окружения с высокой временной задержкой передачи информации. Кроме того, DAV широко применяется в качестве протокола для доступа через Интернет и манипулирования содержимым систем документооборота (document management system). Ещё одной важной целью DAV является поддержка работы распределенных команд по разработке программного обеспечения. В качестве резюме задачу создания DAV можно указать так: на волне повсеместного использования HTTP в качестве стандартного уровня доступа к широкому кругу хранилищ информации расширить его возможности средствами записи информации (HTTP — доступ на чтение, DAV — доступ на запись).

7.4 Пример использования

```
1 123
```

При помощи утилиты curl загрузить файл, создать директорию, выгрузить файл на сервисdisk.yandex.ru.

8 Вывод

В ходе работы были использованы следующие протоколы: SMTP, POP3, IMAP, HTTP, FTP, TFTP, WebDAV.

Учитывая имеющиеся теоретические знания о работе рассматриваемых протоколов и небольшой опыт их использования, проделанная работа позволяет лучше проникнуться тонкостями работы с почтовыми серверами и веб-сервисами. В итоге работы были получены навыки и укреплены знания, благодаря которым разработка приложений с использованием рассматриваемых протоколов не вызовет больших сложностей.

Выполнение подобных заданий является полезным и необходимым действием перед написанием собственного приложения использующего указанные протоколы.