Тема:
Основные сервисы на Linux .
Почтовый сервер.

План занятия:

1.Процесс отправки и доставки электронной почты. основные этапы

2. Протоколы электронной почты

Электронная почта похожа на обыкновенную почту.
Только вместо бумаги и ручки вы используете клавиатуру,
набирая текст письма в окне почтовой программы или браузера.

В роли почтовых отделений выступают почтовые серверы, а почтальонами служат каналы Интернета. Почтовые серверы хранят электронные почтовые ящики пользователей. Как только пользователь заглянет в свой почтовый ящик, он сразу увидит поступившие письма.

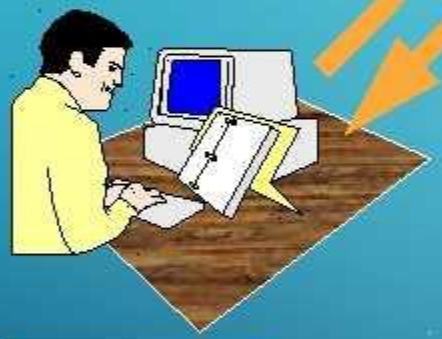
Почтовый сервер – это мощный компьютер, а как мы знаем вся информация на компьютере хранится в виде файлов.
Поэтому электронный ящик – это не что иное, как некоторая область на жестком диске компьютера (дисковое пространство), выделенная под хранение входящих и исходящих писем конкретного пользователя.

Электронная почта

почтовый сервер

www.mail.ru

www.yahoo.com



petr@mail.ru

почтовый ящик

почтовый сервер

bill@yahoo.com

почтовый ящик

почтовый сервер

1.Процесс отправки и доставки электронной почты. основные этапы:

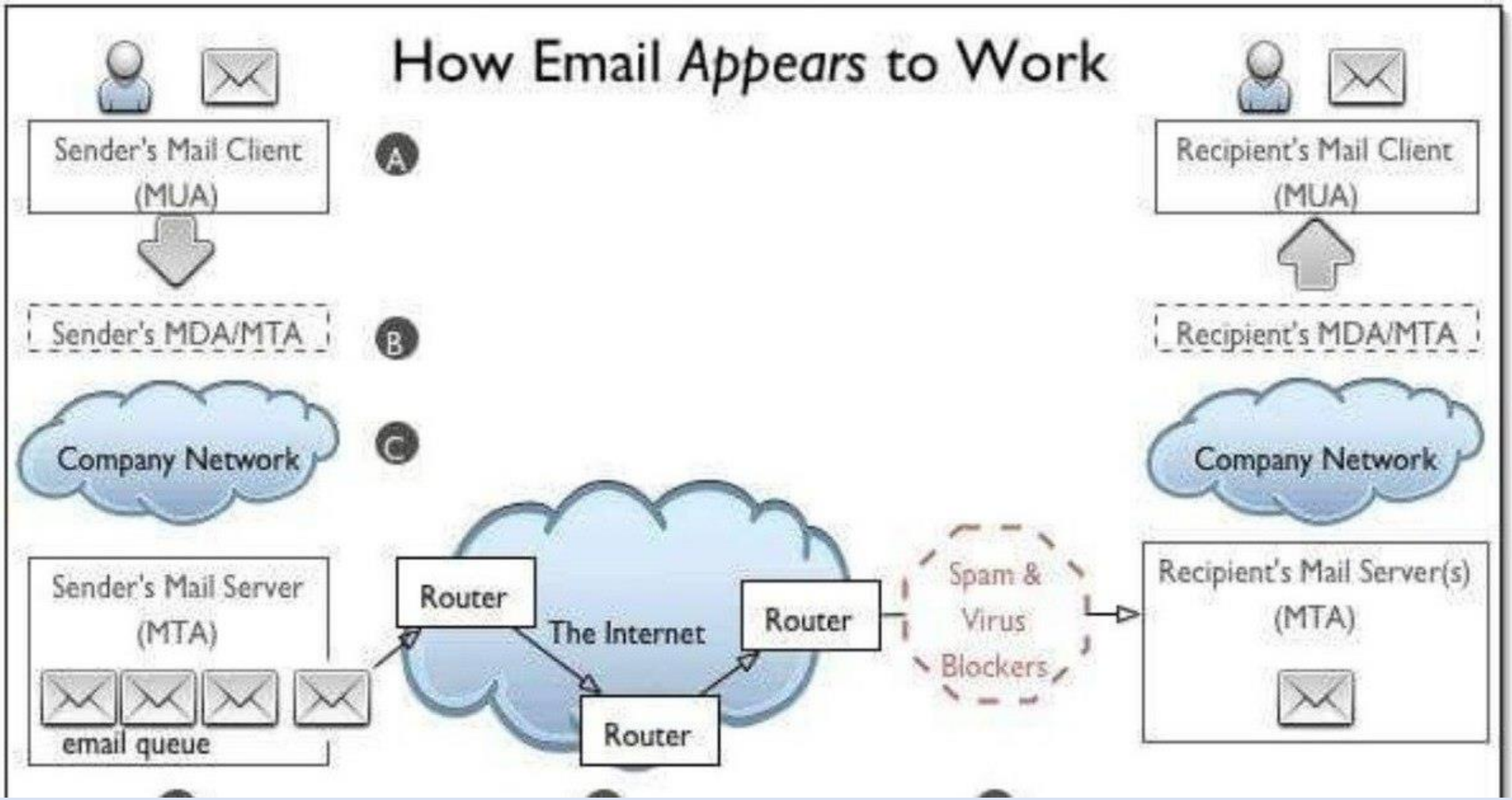
Создание письма. Пользователь создает новое электронное письмо с помощью почтового клиента. Пользователь вводит адреса получателей, тему письма, текст сообщения и при необходимости прикрепляет файлы.

Отправка письма. Почтовый клиент отправляет созданное письмо на почтовый сервер отправителя. Для этого клиент использует протокол SMTP, SMTP устанавливает соединение с почтовым сервером отправителя и передает ему информацию о письме, включая адреса получателей и содержание сообщения.

Пересылка почты между почтовыми серверами (пересылка через MTA). Если получатель имеет почтовый адрес на другом сервере, письмо пересылается через MTA (Mail Transfer Agent) к почтовому серверу получателя. Этот этап включает маршрутизацию сообщений через сеть интернет и взаимодействие между различными почтовыми серверами.

Доставка письма на почтовый сервер получателя. Письмо доставляется на почтовый сервер, ответственный за домен получателя. Этот сервер хранит почтовые ящики пользователей и обрабатывает входящую почту для них.

Получение письма получателем. Получатель использует почтовый клиент для получения электронной почты с почтового сервера. Почтовый клиент отправляет запрос на сервер при помощи протоколов POP3 или IMAP, чтобы получить новые сообщения. Сообщения скачиваются на устройство получателя и отображаются в его почтовом клиенте.


How Email Appears to Work
Sender's Mail Client (MUA)
A
Recipient's Mail Client (MUA)
Sender's MDA/MTA
B
Recipient's MDA/MTA
Company Network
C
Company Network
Sender's Mail Server (MTA)
Router
The Internet
Router
Router
Spam & Virus Blockers
Recipient's Mail Server(s) (MTA)
email queue

2. Протоколы электронной почты

SMTP (Simple Mail Transfer Protocol). Это основной протокол, используемый для отправки электронной почты между почтовыми серверами. SMTP используется почтовыми клиентами для отправки писем на почтовые серверы. Он работает на порту **25** (обычно) и обеспечивает доставку почты по принципу "точка к точке".

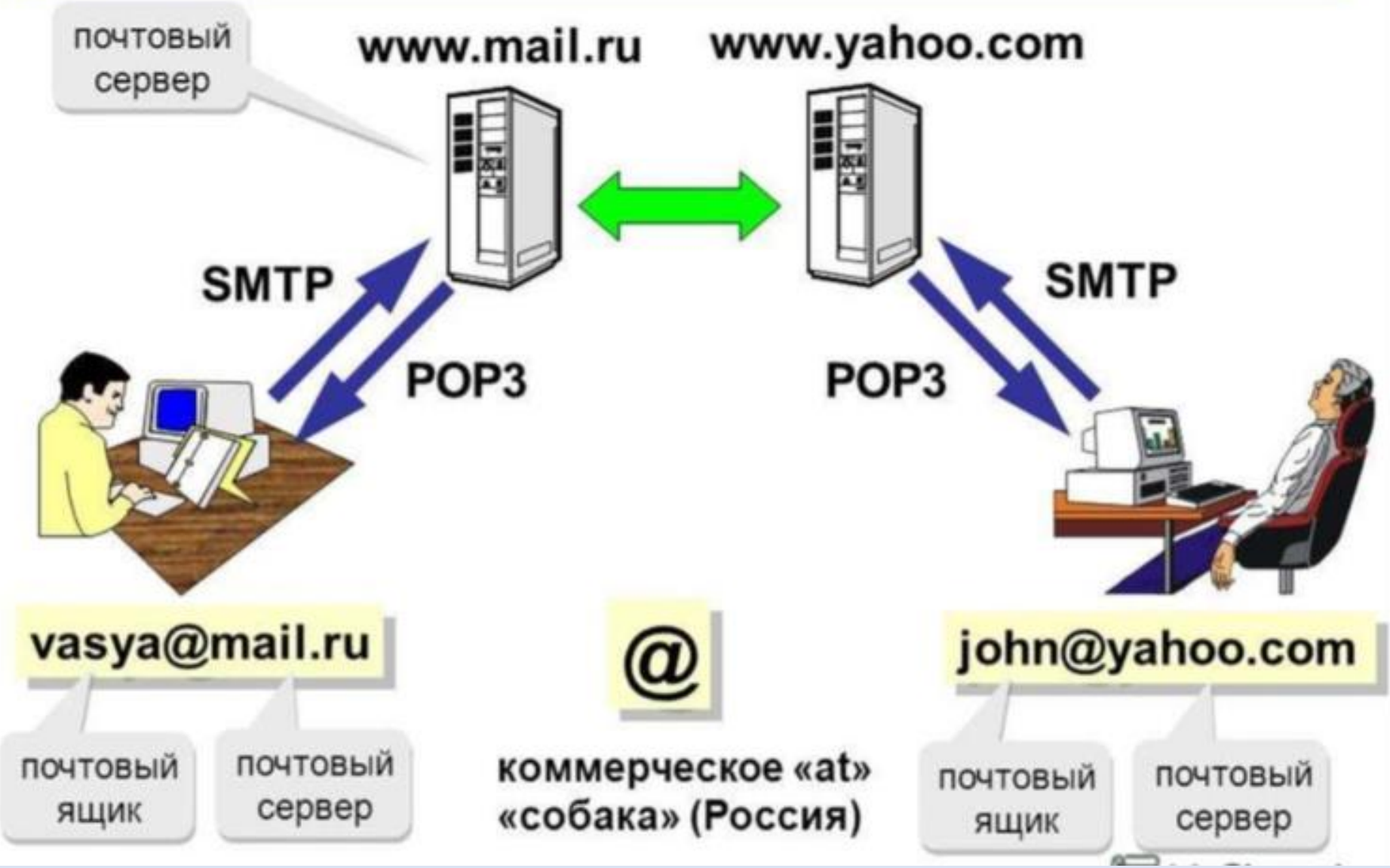
IMAP (Internet Message Access Protocol) — это протокол, также предназначенный для доступа к электронной почте на сервере, но с расширенными возможностями. В отличие от POP3, IMAP (порт **143**) позволяет пользователям оставлять копии писем на сервере, что позволяет им работать с электронной почтой с разных устройств. IMAP также поддерживает более широкий набор функций, таких как папки на сервере и синхронизация между клиентами.

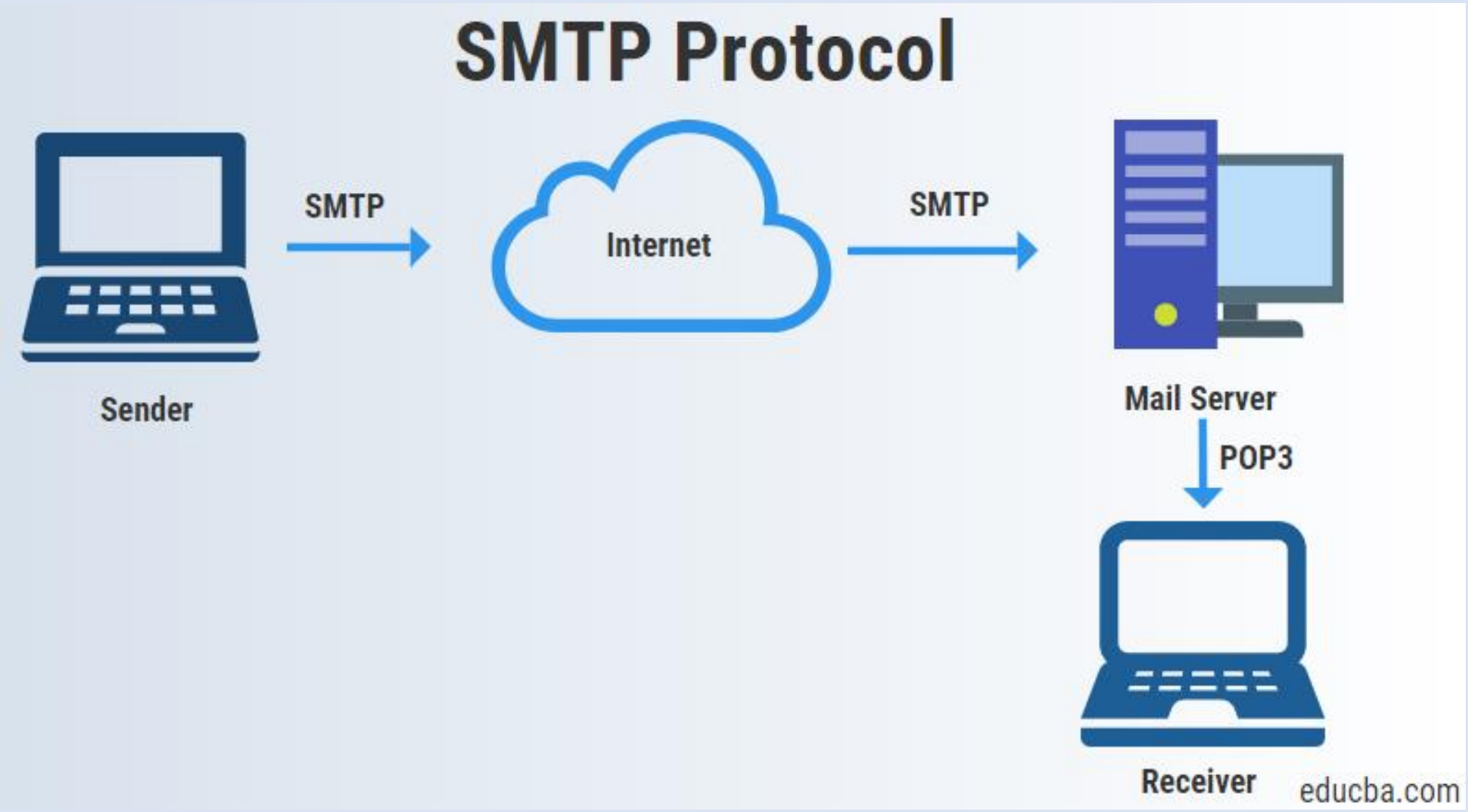
SMTPS (SMTP Secure) и **IMAPS** (IMAP Secure). Это защищенные версии протоколов SMTP и IMAP, которые используют шифрование для защиты конфиденциальности данных во время передачи. SMTPS работает на порту **465**, а IMAPS — на порту **993**.

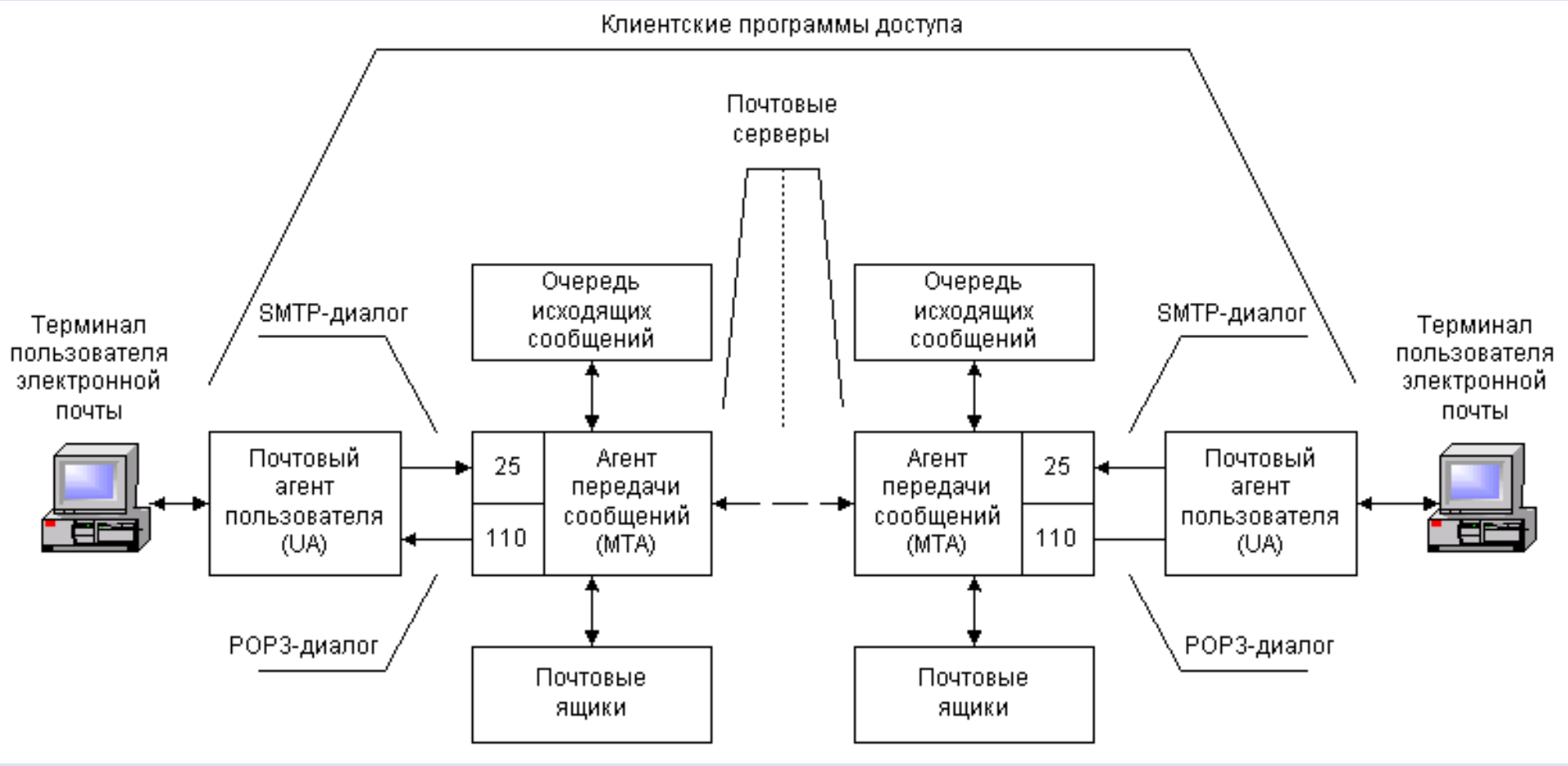
POP3 (Post Office Protocol version 3). POP3 (порт **110**) представляет собой протокол для получения электронной почты с почтового сервера на локальное устройство. Он позволяет почтовым клиентам загружать электронные сообщения с сервера и хранить их на устройстве пользователя. POP3 удаляет письма с сервера после их загрузки на клиентское устройство (по умолчанию).

POP3S (Post Office Protocol version 3 Secure) представляет собой защищенную версию протокола POP3, которая использует шифрование для обеспечения безопасности передачи данных между почтовым клиентом и почтовым сервером. В основном POP3S работает на порту **995**.

Электронная почта (e-mail)




SMTP Protocol
SMTP
Internet
SMTP
Sender
Mail Server
POP3
Receiver
educba.com


Клиентские программы доступа
Почтовые серверы
Терминал пользователя электронной почты
SMTP-диалог
Очередь исходящих сообщений
Очередь исходящих сообщений
SMTP-диалог
Терминал пользователя электронной почты
Почтовый агент пользователя (UA)
25
110
Агент передачи сообщений (MTA)
Агент передачи сообщений (MTA)
25
110
Почтовый агент пользователя (UA)
POP3-диалог
Почтовые ящики
Почтовые ящики
POP3-диалог

3. Почтовые серверы: основные компоненты. Архитектура. Различные типы почтовых серверов и их функции.

Основных компоненты почтовых серверов:

MUA (Mail User Agent) или **почтовый клиент** - это программное обеспечение, которое используется пользователем для чтения, отправки и управления электронной почтой. Microsoft Outlook, Mozilla Thunderbird, The Bat и пр.

MTA (Mail Transfer Agent) или **почтовый сервер** - это программное обеспечение, которое отвечает за передачу электронной почты между почтовыми серверами. Postfix , Microsoft Exchange Server, Mailcow и пр.

MDA (Mail Delivery Agent) или **агент доставки электронной почты** - это программное обеспечение, которое отвечает за доставку входящей электронной почты на почтовый ящик пользователя. MDA принимает почтовые сообщения от почтового сервера (MTA) и выполняет их доставку в соответствующие почтовые ящики или хранилища. Procmail, Dovecot, Cyrus и пр.

SMTP-сервер - это компонент, отвечающий за прием и отправку почтовых сообщений с использованием протокола SMTP. SMTP-сервер обрабатывает исходящую почту от MUA, отправляет ее на другие почтовые серверы и принимает входящую почту от других серверов для доставки в почтовые ящики на сервере.

База данных - почтовые серверы часто используют базу данных для хранения информации о пользователях, почтовых ящиках, настройках и других сведениях, необходимых для обработки и доставки электронной почты.

Механизмы аутентификации, чтобы пользователи могли получать доступ к своей почте с использованием паролей или других методов проверки подлинности.

Дополнительные компоненты - почтовые серверы могут включать дополнительные компоненты, такие как антиспам-фильтры, антивирусные программы, системы резервного копирования и другие инструменты для обработки и защиты электронной почты.

4. Роль DNS в передаче электронной почты и почтовых серверах.

Разрешение доменных имен. DNS используется для разрешения доменных имен почтовых серверов в их соответствующие IP-адреса. Когда пользователь отправляет электронное письмо, почтовый клиент использует DNS для поиска IP-адреса почтового сервера, указанного в адресе получателя (например, smtp.example.com).

Определение MX-записей. DNS содержит записи типа MX (Mail Exchange), которые указывают, какие почтовые серверы отвечают за прием электронной почты для конкретного домена. Когда почтовой серверу требуется отправить письмо на адрес в определенном домене, он использует DNS для поиска MX-записей этого домена и определения, куда отправить письмо.

4. Роль DNS в передаче электронной почты и почтовых серверах.

Проверка обратных DNS-записей (PTR). Некоторые почтовые серверы проверяют наличие обратных DNS-записей (PTR-записей) для IP-адресов отправителей во избежание спама и фишинга. При получении письма почтовый сервер может использовать DNS для проверки обратных DNS-записей отправителя и подтверждения легитимности его источника.

SPF (Sender Policy Framework). SPF — это механизм аутентификации, используемый для определения, является ли конкретный почтовый сервер допустимым отправителем электронной почты от имени определенного домена. Для проверки SPF записей, почтовый сервер обращается к DNS, чтобы получить информацию о том, какие серверы имеют право отправлять почту от имени домена.

```
[root@mail ~]# dig mx gmail.com

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.15 <<>> mx gmail.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13137
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;gmail.com.                     IN      MX

;; ANSWER SECTION:
gmail.com.              1708    IN      MX      5 gmail-smtp-in.l.google.com.
gmail.com.              1708    IN      MX      40 alt4.gmail-smtp-in.l.google.com.
gmail.com.              1708    IN      MX      30 alt3.gmail-smtp-in.l.google.com.
gmail.com.              1708    IN      MX      20 alt2.gmail-smtp-in.l.google.com.
gmail.com.              1708    IN      MX      10 alt1.gmail-smtp-in.l.google.com.

;; Query time: 11 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Сб мар 23 18:43:02 +05 2024
;; MSG SIZE  rcvd: 161
```

```
[root@mail ~]# dig mx yandex.kz

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.15 <<>> mx yandex.kz
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15770
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;yandex.kz.                     IN      MX

;; ANSWER SECTION:
yandex.kz.              132     IN      MX      10 mx.yandex.ru.

;; Query time: 6 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Сб мар 23 18:38:34 +05 2024
;; MSG SIZE  rcvd: 66
```

```
[root@mail ~]# dig mx.yandex.ru

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.15 <<>> mx.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8200
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;mx.yandex.ru.                  IN      A

;; ANSWER SECTION:
mx.yandex.ru.           38      IN      A       77.88.21.249

;; Query time: 2 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Сб мар 23 18:41:25 +05 2024
;; MSG SIZE  rcvd: 57
```

```
[root@mail ~]# dig -x 77.88.21.249

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.15 <<>> -x 77.88.21.249
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28148
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;249.21.88.77.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
249.21.88.77.in-addr.arpa. 276  IN      PTR     mxfront.stable.qloud-b.yandex.net.

;; Query time: 27 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Сб мар 23 18:36:54 +05 2024
;; MSG SIZE  rcvd: 101
```

SPF (Sender Policy Framework) — это система проверки электронной почты, позволяющая предотвратить подделку адресов отправителя в электронных письмах, известную как email spoofing. SPF позволяет администраторам доменов указывать, какие почтовые серверы авторизованы отправлять почту от имени их доменов.

Администратор домена создает SPF-запись в DNS. Запись содержит список IP-адресов или доменов, которым разрешено отправлять почту от имени этого домена.

Когда почтовый сервер получает входящее письмо, он извлекает значение поля "Return-Path" (также известное как адрес обратной связи), которое указывает домен отправителя. Затем сервер выполняет DNS-запрос, чтобы получить SPF-запись для этого домена.

Если IP-адрес отправителя соответствует одному из IP-адресов в SPF-записи, письмо считается авторизованным. В противном случае оно может быть отмечено как неавторизованное или спам.

~all указывает, что почта, отправленная с серверов, не указанных в SPF-записи, должна быть принята, но помечена как не соответствующая SPF. Знак «**~**» означает "мягкое отказ", а «**-**» твердый отказ.

```
[root@mail ~]# dig TXT _spf.yandex.ru

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.15 <<>> TXT _spf.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11823
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;_spf.yandex.ru.                        IN      TXT

;; ANSWER SECTION:
_spf.yandex.ru.         839     IN      TXT     "v=spf1 include:_spf-ipv4.yandex.ru
.yandex.ru include:_spf-ipv4-yc.yandex.ru ~all"

;; Query time: 37 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Сб мар 23 18:54:54 +05 2024
;; MSG SIZE  rcvd: 154
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Сб мар 23 18:43:02 +05 2024
;; MSG SIZE  rcvd: 161
```

5. Конфигурация и администрирование почтовых серверов.

Установка и настройка программного обеспечения. Первым шагом является установка и настройка программного обеспечения для почтового сервера. Это может включать в себя установку MTA, MDA и других компонентов, таких как антиспам фильтры, антивирусное программное обеспечение и SSL-сертификаты.

Настройка DNS записей. Необходимо сконфигурировать DNS-записи домена для обеспечения правильной маршрутизации электронной почты. Это включает в себя добавление MX-записей, SPF-записей, PTR-записей и др.

Управление почтовыми доменами и почтовыми ящиками. Администратор почтового сервера должен управлять почтовыми доменами и почтовыми ящиками пользователей.

Настройка безопасности и аутентификации. Необходимо настроить правила фильтрации спама и вредоносных писем, а также обеспечить аутентификацию пользователей при отправке и получении почты.

Мониторинг и отладка. Администратор почтового сервера должен мониторить работу сервера, чтобы обнаруживать проблемы и сбои, связанные с производительностью или безопасностью.

Резервное копирование и восстановление. Важно регулярно создавать резервные копии данных почтового сервера и иметь план восстановления в случае сбоев или утраты данных.

6. Безопасность почтовых серверов: защита от спама, фишинга и вирусов.

Фильтрация спама. Использование антиспам фильтров на почтовых серверах помогает идентифицировать и блокировать нежелательные сообщения, которые могут содержать спам, рекламу, фальшивые предложения и т. д. Фильтры спама могут базироваться на различных критериях, таких как содержание сообщения, IP-адрес отправителя, характеристики заголовков сообщения и т. д.

Антивирусная защита. Использование антивирусного программного обеспечения на почтовых серверах позволяет обнаруживать и блокировать вредоносные вложения в электронных сообщениях, такие как вирусы, трояны, черви и другие вредоносные программы. Антивирусные сканеры анализируют вложения и ссылки в электронных письмах на наличие угроз и блокируют доступ к вредоносным файлам.

Аутентификация отправителя (SPF, DKIM, DMARC). Использование механизмов аутентификации отправителя, таких как SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) и DMARC (Domain-based Message Authentication, Reporting, and Conformance), помогает проверять легитимность отправителей и предотвращать подделку адресов отправителей в электронных сообщениях. SPF определяет список серверов, которые имеют право отправлять письма от имени домена, DKIM использует криптографическую подпись для проверки целостности сообщения, а DMARC позволяет установить правила обработки писем, не прошедших проверку SPF и DKIM.

Мониторинг и анализ активности. Постоянный мониторинг и анализ активности почтовых серверов позволяет выявлять аномальные паттерны поведения, необычную активность или попытки атак, связанные с отправкой спама, фишинга или распространением вирусов.

7. Защита данных и приватность в электронной почте.

Основные методы обеспечения защиты данных и приватности в электронной почте:

Шифрование сообщений. Использование протокола шифрования, такого как TLS (Transport Layer Security) или его предшественника SSL (Secure Sockets Layer), обеспечивает защищенную передачу данных между почтовыми серверами и клиентами. Для обеспечения конфиденциальности содержимого сообщений рекомендуется также использовать методы end-to-end шифрования, такие как PGP (Pretty Good Privacy) или S/MIME (Secure/Multipurpose Internet Mail Extensions).

Аутентификация и авторизация. Использование сильных методов аутентификации пользователей при доступе к почтовым ящикам и отправке сообщений помогает предотвратить несанкционированный доступ к почтовой учетной записи. Многофакторная аутентификация (MFA) усиливает защиту, требуя от пользователей предоставление нескольких форм аутентификационной информации (например, пароль + одноразовый код).

Управление ключами. При использовании шифрования электронной почты важно правильно управлять ключами шифрования. Защищенное хранение и обмен ключами помогает предотвратить возможные атаки на шифрованные сообщения.

Фильтрация вредоносных сообщений. Использование антивирусного программного обеспечения на почтовых серверах помогает обнаруживать и блокировать вирусы и другие вредоносные программы, прикрепленные к электронным сообщениям. Дополнительные меры защиты, такие как анализ поведения и облачные сервисы защиты от угроз, могут помочь в борьбе с новыми видами вредоносных атак.

Домашнее задание:

1. Изучить дополнительные материалы.