# Занятие 5. Протоколы электронной почты SMTP, IMAP, POP. Протокол передачи файлов FTP. Система DNS

### ПРОТОКОЛ SMTP

SMTP (Simple Mail Transfer Protocol) - это текстовый протокол, работающий поверх TCP, предназначенный для передачи электронной почты. В 1970-х годах с развитием компьютерных сетей были разработаны стандарты того, как пользователи различных систем могли писать друг другу электронные сообщения, они и стали основой для протокола SMTP. Ранние реализации включали в себя FTP Mail и Mail Protocol, разработанные в 1973 году, а в 1980-х был разработан сначала протокол Mail Transfer Protocol, благодаря которому протокол FTP перестал быть основой для передачи почты. Стандарт протокола SMTP был впервые опубликован в 1982 году. Первые реализации протокола и почтовых серверов обслуживали компании и доставляли почту в корпоративные сети, однако с ростом количества сетей и подключенных к ним пользователей, SMTP стал использоваться и для доставки электронной почты конкретным пользователям. Это привело к необходимости расширения протокола и введения механизмов аутентификации, был разработан стандарт ESMTP (Enchanced SMTP) - расширения протокола для стандарта SMTP, сейчас под протоколом SMTP так же подразумевают и его расширения.

SMTP - это протокол доставки почты, он используется при отправке исходящей почты пользователем и при передаче электронной почты между почтовыми серверами. Со стороны пользователя электронная почта представлена MUA (Mail User Agent, почтовым клиентом), для отправки исходящей почты клиент использует MSA (Mail Submission Agent, агент отправки почты), с которым клиент взаимодействует по протоколу TCP (25, 587 или 465 порты), а агент отправки почты доставляет почту MTA (Mail Transfer Agent, агент пересылки почты). MSA и MTA являются SMTP-серверами, например, Sendmail, Postfix, Exim, Microsoft Exchange и т.п.

SMTP-сессия состоит из команд, посылаемых SMTP-клиентом, и соответствующих ответов SMTP-сервера. В качестве SMTP-клиентом может выступать как MUA, так и MTA. Сессия может включать в себя несколько операций, состоящий из набора текстовых команд клиента и ответов сервера.

Коды ответов сервера сгруппированы по типу:

- 2XX - успешные (250 - OK, 220 - сервис готов),
- 3XX - запрос дополнительных данных от клиента (354 - требуется передача тела сообщения),
- 4XX - временные ошибки/проблемы отправки (450 - почтовый ящик временно недоступен, 421 - сервис временно недоступен),
- 5XX - постоянные ошибки/проблемы отправки (например, 550 - почтовый ящик пользователя недоступен, 521 - сервер не принимает почту).

Одни и те же коды могут использоваться для ответа на различные команды клиента. В случае получения 5XX кода отправка сообщения прерывается, в случае получения 4XX кода сообщение может быть поставлено в очередь повторной отправки на определенное время.

Чтобы бороться со злоупотреблениями при отправке или пересылке электронной почты (например, спамом или подделкой отправителя) на MSA и MTA вводятся различные ограничения. Самым простым является ограничение по адресам сетей, из которых пользователи могут могут подключаться и отправлять исходящую почту. Современные серверы обычно используют аутентификацию пользователя для предоставления возможности отправки почты. Если SMTP-сервер не имеет никаких ограничений для отправки электронной почты, он называется Open Relay, однако такие сервера считаются «дурным тоном», поскольку являются небезопасными как для пользователей, так и для других почтовых серверов. Так же существует ряд ограничений при взаимодействии MSA и MTA или MTA и MTA, например, проверки принадлежности домена отправителя серверу исходящей почты, которым пользуется клиент, дополнительных записей в DNS-зоне домена, наличие IP-адреса SMTP-сервера в одном из публичных спам-листов.

Протокол SMTP используется только для отправки электронной почты пользователями или доставки сообщений между почтовыми серверами, для получения электронной почты пользователями используется один из двух протоколов IMAP или POP.

**ПРОТОКОЛ IMAP**

IMAP (Internet Message Access Protocol) - один из наиболее распространенных протоколов прикладного уровня для обеспечения работы пользователей с почтовыми ящиками и сообщениями.

IMAP предоставляет пользователю широкие возможности для работы с почтовыми ящиками, находящимися на почтовом сервере. Почтовый клиент, использующий этот протокол, получает доступ к хранилищу сообщений на сервере так, как будто они расположены на компьютере получателя, сообщения при этом хранятся на почтовом сервере. Электронными письмами можно манипулировать с компьютера пользователя без постоянной пересылки с сервера и обратно полного содержания писем. Он предоставляет пользователям возможность получения электронной почты из одного и того же ящика из разных мест, предоставлять доступ к почтовому ящику или его частям другим пользователям, перемещать сообщения внутри ящика и между ними, благодаря системе флагов сообщений пользователи могут отслеживать состояние сообщения (не прочитано, переслано, отвечено, черновик, входящее и т.п.)

IMAP-сервер прослушивает порт 143/TCP, для подключения к IMAP-серверу с использованием шифрованного соединения используется протокол IMAPS и порт 993/TCP.

**ПРОТОКОЛ POP**

POP (Post Office Protocol) - второй из наиболее распространенных протоколов прикладного уровня для извлечения почты с почтовых серверов клиентами. Протокол работает поверх TCP, он был разработан в нескольких версиях, версии POP и POP2 уже устарели, актуальной используемой является POP3.

POP поддерживает простые требования «загрузи-и-удали» для доступа к удалённым почтовым ящикам. Хотя большая часть POP-клиентов предоставляет возможность оставить почту на сервере после загрузки, использующие POP клиенты обычно соединяются, извлекают все письма, сохраняют их на пользовательском компьютере как новые сообщения, удаляют их с сервера, после чего разъединяются. Изначальная спецификация POP3

поддерживала только незашифрованный механизм входа в систему. На данный момент POP3 поддерживает различные методы аутентификации для предоставления разных уровней защиты от незаконного доступа к пользовательской почте. Большинство из них предоставлено механизмами расширения, однако в протоколе не намеревались поощрять расширения, считая что роль POP3 заключается в предоставлении простой поддержки в основном для требования «загрузи-и-удали».

POP3-сервер прослушивает порт 110/TCP, в случае необходимости шифрования связи соединение с использованием SSL или TLS запрашивается после запуска протокола либо с помощью команды STLS (если она поддерживается) по тому же 110/TCP порту, либо с помощью протокола POP3S и специального порта 995/TCP.

**ПРОТОКОЛ FTP**

FTP (File Transfer Protocol) является одним из самых старейших прикладных протоколов. Как уже упоминалось ранее, первая реализация протокола FTP имела отношение к процессу обмена электронными сообщениями. Сейчас протокол FTP используется для передачи файлов между клиентом и сервером и в отличие от большинства протоколов использует разные сетевые соединения для передачи команд и передачи данных.

Для установления соединения между клиентом и сервером используется порт 21/TCP, соединение на этом порту является управляющим и остается открытым на все время сессии, по нему передаются команды и другая информация, необходимая для работы. Для передачи данных открывается второе соединение, способ его открытия определяется режимом работы сервера - активным или пассивным. В случае активного режима работы сервера клиент после установки управляющего соединения отправляет серверу свой IP-адрес и произвольный номер порта и ждет, пока сервер со своей стороны установит соединение с клиентом по переданным адресу и порту. Для организации такого взаимодействия необходимо, чтобы клиент либо находился в той же сети, что и сервер, либо имел глобальный IP-адрес. В случае пассивного режима работы сервер передает клиенту в ответ на запрос свой IP-адрес и номер порта и ждет, пока клиент установит соединение для передачи данных. Этот режим работы используется в случаях, когда клиент находится в локальной сети, а сервер в глобальной.

В качестве аутентификации в протоколе FTP используется передача имени пользователя и пароля клиентом в специальных командах протокола (USER, PASS), если предоставленная пользователем информация верна, начинается сессия. В некоторых случаях клиенты могут подключиться к серверу без предоставления учетных данных, такие сервера называются «анонимными» и в основном предоставляют для неаутентифицированных пользователей ограниченный функционал (например, только скачивание файлов без загрузки или скачивание только части файлов). Большая часть вэб-браузеров поддерживает простое скачивание файлов по протоколу FTP, как с анонимных серверов, так и с закрытых аутентификацией, для загрузки файлов на FTP-сервера обычно используются специальные клиенты.

FTP не разрабатывался как защищённый протокол и имеет многочисленные уязвимости в защите, например, поскольку все команды по управляющему соединению отправляются в текстовом виде, то и учетные данные пользователя так же передаются в открытом текстовом виде. Для решения проблемы перехвата открытого трафика можно использовать либо версию протокола FTPS, поддерживающую TLS-шифрование соединения, либо другой более защищенный протокол SFTP, являющийся частью протокола SSH (Secure Shell) или же протокол FTP через SSH (в случае работы протокола FTP по установленному SSH-туннелю).

По управляющему соединению передаются не только команды от клиента серверу, но и коды ответов сервера. Коды ответов FTP-сервера трехзначные, первая цифра отвечает за тип кода:

- 2XX - успешный ответ
- 4XX/5XX - команда не может быть выполнена
- 1XX/3XX - ошибка или неполный ответ

Вторая цифра определяет тип произошедней ошибки:

- X0X - синтаксическая
- X1X - информационное сообщение
- X2X - информация об одном из соединений (управляющее или соединение передачи данных)
- X3X - аутентификация или проблема прав доступа
- X5X - ошибка состояния файловой системы

Для организации клиентом передачи данных между двумя FTP-серверами используется протокол FXP (File Exchange Protocol). При использовании этого протокола для передачи данных от одного сервера к другому без закачки файла на самого клиента, клиент открывает два разных соединения к разным FTP-серверам и, запрашивая файл на одном из серверов, указывает IP-адрес и порт другого FTP-сервера. При использовании FXP клиент не имеет проблем с глобальными адресами и пропускной способностью своих каналов к FTP-серверам. Однако этот протокол стал использоваться злоумышленниками для атак на FTP-серверы.

**СЛУЖБА DNS**

DNS (Domain Name System) - это распределенная иерархическая система для хранения и получения данных о доменных именах. Чаще всего используется для получения IP-адреса по имени домена.

Использование запоминающегося имени хоста вместо его IP-адреса использовалось еще в самых первых компьютерных сетях. Для сопоставления имен хостов с их адресами использовался текстовый файл hosts.txt, он составлялся и поддерживался вручную и с развитием сетей потребовался автоматизированный способ составления, хранения и передачи списков сопоставления адресов именам хостов. В 1984 году была создана первая версия сервера разрешения имен BIND (Berkley Internet Name Daemon).

Система DNS обладает следующими характеристиками:

- *Распределённость администрирования.* Ответственность за разные части иерархической структуры несут разные люди или организации.
- *Распределённость хранения информации.* Каждый узел сети в обязательном порядке должен хранить только те данные, которые входят в его зону ответственности, и (возможно) адреса корневых DNS-серверов.
- *Кэширование информации.* Узел может хранить некоторое количество данных не из своей зоны ответственности для уменьшения нагрузки на сеть.
- *Иерархическая структура*, в которой все узлы объединены в дерево, и каждый узел может или самостоятельно определять работу нижестоящих узлов, или делегироватьих другим узлам.
- *Резервирование.* За хранение и обслуживание своих узлов или зон отвечают несколько серверов, разделённые как физически, так и логически, что обеспечивает сохранность данных и продолжение работы даже в случае сбоя одного из узлов.

Ключевыми понятиями службы DNS являются:

*Домен (domain)* - узел в дереве имен вместе со всеми подчиненными ему узлами, то есть именованная ветвь или поддерево в дереве имен. Структура доменного имени отражает порядок следования узлов в иерархии. Доменное имя читается слева направо от младших доменов к доменам высшего уровня. Вверху находится корневой домен, имеющий идентификатор «.» (точка), ниже идут домены первого уровня (доменные зоны), например, .ru, .com, .рф, затем домены второго уровня, третьего и так далее. Например, i-ts.sirius-systems.ru.: домен первого уровня - ru, второго - sirius-systems.ru, третьего - i-ts.sirius-systems.ru. DNS позволяет не указывать точку корневого домена.

*Поддомен (subdomain)* - подчиненный домен, например, i-ts.sirius-systems.ru - поддомен домена sirius-systems.ru. Теоретически такая иерархия может достигать 127 уровней, а каждая метка может содержать до 63 символов, пока общая длина вместе с точками не достигнет 254 символов.

*Ресурсная запись (record)* - единица хранения и передачи информации в DNS, каждая ресурсная запись привязана к доменному имени, имеет тип и поле данных.

*Зона (dns zone)* - часть дерева доменных имен, размещаемая как единое целое на некотором сервере доменных имен, DNS-сервере, а чаще на нескольких DNS-серверах.

Целью выделения части дерева в отдельную зону является передача ответственности за домен другому лицу или организации. Это называется *делегированием***.**

*DNS-сервер* - специализированное ПО для обслуживания DNS, а так же сервер, на котором это ПО запущено. DNS-сервер может быть ответственным за некоторые зоны и/или может перенаправлять запросы вышестоящим серверам.

*DNS-клиент* - специализированная библиотека или утилита для работы с DNS. В ряде случаев DNS-сервер выступает в роли DNS-клиента.

*Авторитетность, авторитативность (authoritative)* - признак размещения зоны на DNS-сервере. Ответы DNS-сервера могут быть двух типов: авторитетные (когда сервер заявляет, что сам отвечает за зону) и неавторитетные (non-authoritative), когда сервер обрабатывает запрос, и возвращает ответ других серверов.

Запись DNS (или ресурсная запись) является единицей хранения и передачи информации в системе DNS, каждая состоит из следующих полей: имя, тип, класс сети, TTL, длина данных и сами данные. Наиболее важные типы DNS-записей:

- *A (address record)* - связывает имя хоста с IPv4-адресом
- *AAAA (IPv6 address record)* - связывает имя хоста с IPv6-адресом
- *CNAME (canonical name record)* - запись, перенаправляющая на другое имя
- *MX (main exchange)* - указывает на сервера почтовой службы домена
- *NS (name server)* - указывает на DNS-сервер для домена
- *PTR (pointer)* - обратная запись, связывающая IP-адрес хоста с именем
- *SOA (start of authority)* - начальная запись зоны, описывает сервер, на котором хранится эталонная информация о домене
- *TXT (text record)* - текстовые записи в зоне, являющиеся служебными для некоторых сервисов

Система DNS содержит иерархию DNS-серверов, соответствующую иерархии зон. Каждая зона поддерживается как минимум одним авторитетным сервером, на котором расположена информация о домене. В случае, когда клиент запрашивает у DNS-сервера информацию о домене, которой он не владеет в своем управлении или кеше, DNS-сервер может осуществить рекурсивный поиск от имени клиента по всей системе DNS, обращаясь к другим DNS-серверам, включая корневой.

DNS используется в первую очередь для преобразования символьных имён в IP-адреса, но он также может выполнять обратный процесс. Для этого используются уже имеющиеся средства DNS. Дело в том, что с записью DNS могут быть сопоставлены различные данные, в том числе и какое-либо символьное имя. Существует специальный зарезервированный домен in-addr.arpa, записи в котором используются для преобразования IP-адресов в символьные имена. Доменное имя может состоять только из ограниченного набора ASCII-символов, позволяя набрать адрес домена независимо от языка пользователя. Однако для поддержки интернациональных доменных имен была утверждена основанная на Punicode (преобразование Unicode в ACE-последовательности, ASCII Compatible Encoding) система, преобразующая любую строку в Unicode в последовательность символов, допустимую в DNS.

Помимо системы DNS для хранения информации о доменных именах сущесвуют организации *Регистраторы доменных имен*. Эти организации уполномочены создавать (регистрировать) новые доменные имена, продлевать сроки действия существующих, хранить у себя и предоставлять информацию обо всех зарегистрированных у них доменных именах. Регистраторы требуются для следующих уровней доменов: корневого домена, доменов верхнего уровня и части доменов второго уровня (например, com.ru, co.uk, spb.ru). Функции регистратора доменов верхнего уровня (.com, .ru, .org и т.п.) выполняет организация ICANN (Internet Corporation for Assigned Names and Numbers), владельцем таких доменов может быть государство, негосударственное сообщество (в т.ч. международное), однако часто владельцы таких доменов выполняют роль координатора и лицензиара, а непосредственно регистрацию доменов в нем осуществляют уполномоченные организации (например, reg.ru, nic.ru, godaddy.com). Несколько регистраторов одного домена верхнего уровня должны использовать единую базу доменов для предотвращения конфликтов и обеспечения уникальности доменного имени.