Электронная почтовая служба

Протоколы Интернета: SMTP

Эта статья продолжает цикл «Протоколы Интернета». В предыдущем номере было дано представление о самом понятии «протокол», а также описано средство передачи гипертекста — HTTP. В этот раз вы узнаете о том, как работает протокол SMTP, занимающийся доставкой электронной почты.

Цифровые письма

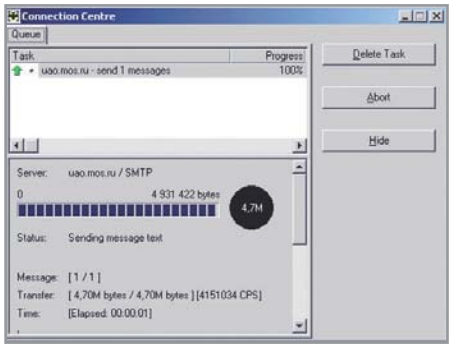
Одной из самых популярных сетевых служб является электронная почта — многофункциональный сервис обмена электронными сообщениями. Каждое такое сообщение может содержать обыкновенный текст, текст со сложным форматированием и разнообразными шрифтами, встроенные изображения, звуки, видеофрагменты. К письму можно прилагать любые файлы: архивы, программы, все что угодно. Для отправки и приема сообщений используется web-интерфейс, терминальное соединение или программа-клиент. Почтовыми уведомлениями могут пользоваться самые разные сетевые службы: антивирусные комплексы и детекторы сетевых атак уведомят администраторов об опасной активности в сети; сервисы обслуживания форумов, почтовых рассылок и порталов оповестят пользователей о текущих событиях и т. д.

Сообщение от отправителя к адресату идет по протоколу SMTP (Simple Mail Transfer Protocol — простой протокол электронной почты). Сам протокол довольно прост и не сильно изменился по сравнению со своим первоначальным видом. Дополнительная функциональность реализуется с помощью расширений протокола (extensions). Их количество на данный момент довольно велико и использование в реальных условиях зависит от конкретной почтовой системы.

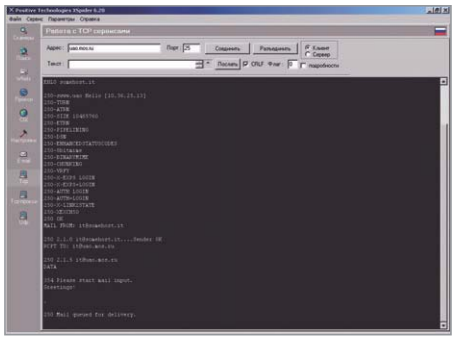
Мой адрес не дом и не улица

Прежде всего, чтобы узнать, как письмо оказывается у получателя, нужно по- »

нять, как идентифицируется этот получатель. Адрес электронной почты заканчивается именем, которому предшествует специальный символ @. Доменное имя в адресе необязательно является именем сервера обработки электронной почты. Это может быть и имя домена, но при помощи службы DNS можно найти почтовый сервер (или даже несколько) для этого домена. Символу @ предшествует имя, уникальное в пределах одного почтового сервиса. Обычно одним почтовым ящиком владеет один пользователь. Но бывают и другие варианты. Ящик может принадлежать группе пользователей, которые читают все входящие письма и письма, отправленные своими коллегами. Такой вариант может использоваться для организации корпоративной почты.



Почтовый клиент TheBat! завершает соединение с SMTP-сервером



Отправка письма через терминальное соединение

Передача письма

Итак, пользователь написал письмо и отправил его. В настройках почтового клиента обычно указывается передающий (relay) SMTP-сервер. Это может быть сервер организации, какой-либо бесплатной почтовой службы или провайдера, который предоставляет пользователю доступ в Интернет. Если пользователь находится внутри какой-либо организации, то, скорее всего, он будет использовать корпоративный передающий сервер. Программа-клиент устанавливает TCP-соединение с почтовым сервером на 25-й порт и передает сообщение, используя протокол SMTP. Служба передачи определяет адрес почтового сервера, который способен доставить сообщение в ящик получателя (delivery). Затем сервер передачи соединяется с сервером доставки и пересылает письмо опять-таки по протоколу SMTP. Сервер доставки помещает полученное сообщение в почтовый ящик, откуда получатель может скачать свое письмо.

Разумеется, процесс доставки не всегда происходит по такому простому сценарию. Например, передающий сервер отправителя может не иметь доступа в Интернет. Внутри крупной организации может присутствовать множество собственных почтовых серверов, пересылающих сообщения на один передающий сервер — плацдарм (bridgehead), — имеющий доступ в Интернет. Также и сервер доставки получателя может не иметь прямого доступа в Глобальную сеть, а получать сообщения с промежуточного сервера. К тому же почтовый клиент пользователя необязательно связывается с передающим сервером по протоколу SMTP, а может пользоваться каким-нибудь другим (например, Microsoft Outlook может быть настроен на взаимодействие с сервером Microsoft Exchange по собственному протоколу).

Внутри протокола

Как происходит передача информации по протоколу SMTP? Общение между сервером и клиентом SMTP осуществляется посредством команд (command) от клиента и ответов (reply) от сервера. Команда клиента состоит из командного глагола и, возможно, аргументов, следующих после пробела. Ответы сервера обязательно начинаются с трехзначного числа (completion code), отражающего его реакцию и текущее состояние сессии. За кодом обычно следует текстовая строка.

После установки TCP-соединения сервер посылает клиенту ответ 220 (Service ready — служба готова), означающий, что соединение установлено и сервер готов к работе, и строку с дополнительной информацией (имя почтового домена, название и версия программного обеспечения, текущая дата и время). Клиент начинает свою сессию с команды EHLO. Аргументом к ней является полное доменное имя клиента или, если такового нет, некоторое другое имя (например, имя компьютера), с помощью

Дополнительные сведения

Requests for Comments — для заинтересовавшихся

Все RFC можно найти на официальном сайте IETF — www.ietf.org.

RFC 2821: «Simple Mail Transfer Protocol» — www.ietf.org/rfc/rfc2821.txt?number=2821 (описание протокола SMTP).

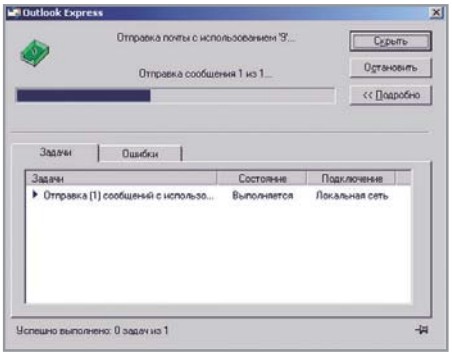
RFC 2554: «SMTP Service Extension for Authentication» — www.ietf.org/rfc/rfc2554.txt?number=2554 (описание расширения AUTH протокола SMTP).

RFC 1891: « Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)» — www.ietf.org/rfc/rfc1891.txt?number=1891 (описание расширения DSN протокола SMTP).

RFC 2045: «Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies» — www.ietf.org/rfc/rfc2045.txt?number=2045 (описание формата тела сообщений Интернета).

RFC 2046: «Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types» — www.ietf.org/rfc/rfc2046.txt?number=2046 (описание типов данных сообщений Интернета).

RFC 2047: «MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text» — www.ietf.org/rfc/rfc2047.txt?number=2047 (описание формата заголовка сообщений Интернета).



▲ Почтовый клиент Outlook Express может использовать свой протокол для отправки писем

» которого можно идентифицировать клиента. В ответ сервер возвращает список доступных SMTP-расширений (extension) и код успешного завершения — 250 OK. Надо заметить, что инициирование сеанса командой EHLO обязательно только в том случае, если в этой сессии будет происходить передача письма. В некоторых же других случаях такое инициирование необязательно. После этого сервер может проверить, соответствует ли доменное имя, указанное клиентом, его реальному IP-адресу.

Кто кому?

Следующий этап сессии SMTP обычно зависит от того, какие именно узлы представляют клиент и сервер в этом случае. Дело в том, что подавляющее большинство передающих SMTP-серверов (особенно те, которые имеют прямой доступ в Интернет) настроены так, что прием сообщений для «внутренних» получателей осуществляется от любого отправителя. «Внутренние» получатели — это получатели, почтовые ящики которых расположены или на том же сервере, или внутри организации. Другими словами, доставка в ящики этих получателей происходит с принимающего сервера посредством доставляющей службы, без использования службы пересылки. Пересылка же (relay) — отправка сообщений на другой внешний сервер по протоколу SMTP — требует от клиента обязательной авторизации и чаще всего доступна только «внутренним» отправителям. Таким образом, если почтовый клиент пользователя соединяется с SMTP-сервером, то перед началом передачи сообщения клиент проходит авторизацию. Выполняется она с помощью SMTP-расширения AUTH.

Авторизация

Клиент посылает команду AUTH до начала почтовой транзакции. После AUTH через пробел следует способ авторизации. Например, «AUTH PLAIN». В этом случае, если сервер готов принять авторизацию, то в ответ он посылает код 334 и строку «Username:». Клиент должен отправить имя пользователя, после чего сервер снова посылает код 334 и строку «Password:». В ответ на это клиент должен отправить верный пароль. Об успешной авторизации сервер извещает кодом 235. О неверной — 535. При использовании способа авторизации PLAIN имя пользователя и пароль отправляются в виде простого текста и поэтому легко подвержены «подслушиванию» злоумышленниками, находящимися в том же сегменте сети, что и клиент или сервер. Почти не меняет дела использование команды AUTH LOGIN, при которой имя пользователя и пароль передаются закодированными алгоритмом BASE64. Зашифрованные таким образом строки поддаются однозначному декодированию. Можно также их и не декодировать, а просто использовать повторно для авторизации.

Гораздо лучше противостоит подслушиванию метод авторизации CRAM-MD5, который основывается на необратимом алгоритме шифрования MD5. Если клиент хочет использовать этот метод авторизации, перед началом почтовой транзакции он посылает серверу команду AUTH CRAM-MD5. Сервер отвечает кодом 334 и посылает специальную строку (challenge), закодированную алгоритмом BASE64. Клиент шифрует эту строку алгоритмом MD5, используя свой пароль, добавляет имя пользователя, кодирует это все в BASE64 и отправляет на сервер. Сервер тоже шифрует эту же специальную строку с использованием пароля пользователя и сравнивает с принятой от клиента строкой. Преимущество этого метода заключается в том, что, даже подслушав всю SMTP-сессию, получить пароль из ответа клиента невозможно, так как он зашифрован необратимым алгоритмом. Также не даст результата и повторное использование этого ответа, потому что специальная строка, посылаемая сервером, постоянно меняется, следовательно, меняется и результат ее шифрования. К сожалению, немногие SMTP-серверы в Интернете используют такой алгоритм.

Конверт

В случае же, если другой передающий сервер соединяется с SMTP-узлом для доставки, авторизации не требуется, так как доставка будет происходить при участии принимающего SMTP-сервера.

После этих действий начинается процесс передачи непосредственно почтового объекта. Почтовый объект состоит из конверта (envelope) и содержимого (content). В конверте содержатся данные об отправителе, получателе и, возможно, некоторая дополнительная информация. Передача письма начинается именно с «заполнения» конверта (команда MAIL). Через пробел после «MAIL FROM:» следует адрес отправителя, заключенный в треугольные скобки. По этому адресу может быть отправлено сообщение о какой-либо ошибке, произошедшей в процессе доставки, или уведомление об успешной доставке. Если адрес отправителя приемлем, сервер возвращает уже известный ответ с кодом 250.

Следующий шаг — указание получателя. Для этого служит команда «RCPT »

Расширения

Не только письма отправлять

Иногда SMTP-сессия может и не содержать в себе почтовой транзакции. Например, если используется расширение протокола VRFY (verify). Эта команда позволяет проверить существование пользователя или узнать почтовые адреса, связанные с одним псевдонимом пользователя. Также существует расширение EXPN (expand). Если почтовый сервер поддерживает группы адресатов (mailing list), то команда EXPN возвращает список членов группы, переданной в аргументе.

» TO:», после которой через пробел следует адрес получателя в треугольных скобках. Если получателей несколько, то команда RCPT посылается клиентом несколько раз.

На этом передача конверта заканчивается. Нужно отметить, что конверт — это не заголовок письма. Само письмо вместе со своим заголовком содержится в теле почтового объекта. В этих заголовках тоже есть получатель и отправитель. И именно эта информация отображается почтовым клиентом у конечного получателя. В большинстве случаев, конечно, информация содержащаяся в конверте, дублируется в полях «From» и «To» письма. Но поля самого письма могут содержать еще и произвольный текст, идентифицирующий обе стороны обмена сообщениями. Кроме того, существуют и другие специальные случаи, когда поля в конверте могут не совпадать с соответствующими полями письма. Например, если отправитель использовал скрытую копию (blind copy), то для каждого адресата, указанного в поле BCC, будет послана отдельная команда RCPT. При этом в поле «To» самого письма будет содержаться лишь один адрес.

Если отсутствуют очевидные на этом этапе препятствия для доставки почты указанным адресатам, сервер возвращает код 250. Теперь возможна ситуация, когда адрес получателя указан в принципе правильно, но доставка невозможна. Это происходит в том случае, если клиент не прошел аутентификацию перед началом почтовой транзакции и пытается воспользоваться пересылкой (relay). Тогда сервер может вернуть ошибку 550 и попросить клиента аутентифицироваться.

Подтверждение о доставке

На этапе заполнения конверта может быть использовано расширение DSN (Delivery Status Notification). Оно позволяет запрашивать у сервера уведомление о доставке отправляемого сообщения. Если сервер может поддерживать расширение DSN, тогда он воспринимает и дополнительные параметры команд MAIL и RCPT. Параметры указывают через пробел, их значения следуют после знака «=» сразу же за названием параметра.

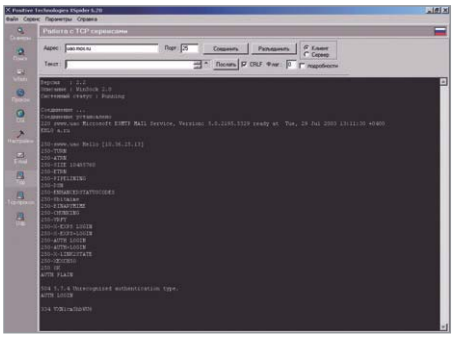
Параметр RET команды MAIL может иметь два значения — HDRS или FULL. Этот параметр отвечает за содержимое отчета о доставке. В первом случае этот отчет будет содержать только заголовки отправленного письма, во втором — письмо целиком.

Параметр NOTIFY команды RCPT указывает, в каких случаях должно приходить уведомление. Его значение может быть или NEVER (уведомление не будет отправлено при любом исходе доставки), или набор значений из списка: SUCCESS — уведомление об удачной доставке; FAILURE — уведомление о невозможности доставки; DELAY — уведомление об отложенной доставке (например, невозможно связаться с SMTP-сервером).

Письмо

После заполнения конверта клиент может перейти к отправке содержимого почтового объекта — собственно письма. Описание подробного внутреннего устройства письма выходит за рамки этой статьи, так как не описывается стандартами протокола SMTP. Можно лишь сказать, что письмо тоже состоит из заголовка (header) и тела (body). Их структура подробно описана в спецификациях MIME (Multipurpose Internet Mail Extensions).

Передача содержимого почтового объекта завершается командой «.» и знаком



▲ Установка соединения и авторизация на сервере

перевода строки. На этом почтовая транзакция заканчивается, и сервер сохраняет письмо для дальнейшей доставки. Письмо помещается в очередь для доставки на другой SMTP-сервер или в локальное хранилище писем (почтовый ящик).

В этой статье описаны назначение и применение протокола SMTP в Интернете, также в общих чертах рассмотрен принцип его работы. В принципе, сам протокол не очень сложен и не так изобилует различными деталями и тонкостями, как, например, HTTP. В то же время без внимания остались такие вопросы, как совместимость со старыми версиями протокола SMTP, совместимость различных почтовых систем и почтовые шлюзы (gateway). Упомянуты не все распространенные расширения протокола и методы авторизации. Но общее представление о функциях и возможностях протокола SMTP вы уже получили.

■ ■ ■ **Дмитрий Солошин**

Проблемы безопасности

Борьба со спамом настройками сервера

В последнее время все сильнее пользователей Интернета беспокоит проблема спама. Для массовой рассылки писем используются различные методы. Один из них связан со специфической настройкой передающего (relay) сервера. В некоторых случаях (по причине невнимательности администратора, например) может получиться так, что в Интернете оказывается доступен передающий SMTP-сервер, который не требует авторизации. Спамеры довольно быстро обнаруживают и начинают использовать такой сервер. Кроме того, не всегда достаточно явно указать в настройках почтового сервера запрет на пересылку сообщений от неизвестных пользователей. Злоумышленник может добиться несанкционированной пересылки и путем различных манипуляций с аргументами команд MAIL и RCPT.

Чаще всего современное программное обеспечение позволяет настроить почтовый узел безопасно. Так что в большинстве случаев серверы, доступные для использования спамерами, появляются из-за невнимательности администраторов. Но проблема действительно существует и называется open relay. Для борьбы со спамом, распространяющимся таким образом, существуют различные «черные списки» (black list), в которых скапливаются адреса SMTP-серверов, допускающих возможность пересылки без авторизации.