

# Теория лабораторной работы №9

## Команды HTTP

Get - позволяет получить инф-ю, связанную с запраш-ым ресурсом.

Если идентификатор запрашиваемого ресурса указывает на документ, то сервер возвращает содержимое этого документа.

Если запрашиваемый ресурс является приложением, формирующим в процессе своей работы некоторые данные, то в теле сообщения ответа возвращаются эти данные.

Если идентификатор запрашиваемого ресурса указывает на директорию, то, в зависимости от настроек сервера, может быть возвращено либо содержимое директории, либо содержимое одного из файлов, находящегося в этой директории.

Вариантными командами GET являются условный GET (conditional) и частичный GET (partial). Условный запрашивает передачу объекта, только если он удовлетворяет условиям, описанным в приведенных заголовках. Частичный запрашивает передачу только части объекта.

HEAD - идентична команде GET, но не возвращает в ответе тело сообщения.

OPTIONS - запрос инф-и об опциях соединения, которые поддерживает сервер для запрашиваемого ресурса.

Если идентификатор ресурса - звездочка, то он обращен ко всему серверу.

POST - тело сообщения, которое передается в запросе, сохраняется на сервере, причем идентификатор запрашиваемого ресурса будет идентификатор сохраняемого объекта.

DELETE - запрос на удаление ресурса, имеющего запрашиваемый идентификатор.

TRACE - используется для тестирования или диагностики.

## Основные типы ответов

После получения и интерпретации сообщения запроса, сервер отвечает сообщением HTTP ответа.

Первая строка ответа - это строка состояния (Status-line):

<Версия HTTP>

<Код состояния> - целочисленный трехразрядный код результата понимания и удовлетворения запроса

<Поясняющая фраза>

Первая цифра кода состояния определяет тип ответа:

1

- 1xx - информационные коды
- 2xx - успешные коды
- 3xx - коды перенаправления
- 4xx - коды ошибок клиента
- 5xx - коды ошибок сервера

## Заголовки referer, host и keep-alive

Заголовок запроса referer содержит URL исходной страницы, с которой был осуществлен переход на текущую страницу. Сервер может анализировать эти данные, записывать их в лог или оптимизировать процесс кодирования.

Заголовок Host содержит имя домена, для которого предназначен запрос и, опционально, номер порта.

Если порт не указан, используется условный порт протокола сервиса (80 для HTTP, 443 для HTTPS и др.).

Каждый HTTP/1.1 запрос должен содержать 1 заголовок Host, в ином случае ответ будет с кодом статуса 400 Bad Request.

Keep-alive заголовок позволяет избежать накрутки, так, как соединение может быть использовано для установки тайм-аута и максимального количества запросов.

## Команды FTP

Команда	Описание	Код
ABOR	отменяет выполнение предыдущей команды	426, 226
DELE	удалить файл	250
RMD	удалить директорию	250
CWD	перейти в директорию	250
MKD	создать директорию	257
PWD	узнать текущую директорию	257
QUIT	закончить работу	221
TYPE	установить тип передачи	200
PORT	перейти в активный режим	200
PASV	перейти в пассивный режим	227
LIST	Получить содержимое каталога	150, 226
RETR	Скачать файл	150, 226
STOR	Загрузить файл	150, 226
RNFR	Выбрать файл для переименования	350
RNTO	Переименовать файл	250

## Устройство NAT

NAT (Network Address Translation) - это такой механизм, который позволяет определить какие серверы находятся за роутером и вернуть данные обратно из интернета, чтобы пользователи могли ими пользоваться.

СВМН М.А. 139



Сети обычно проектируются с использованием публичных IP-адресов. Такие адреса используются, чтобы позволить устройствам общаться локально. Чтобы позволить устройству с приватным IP-адресом обратиться к устройству и ресурсам за пределами локальной сети, приватный адрес сначала нужно перевести на публичный адрес. Этот NAT и занимается - переводит приватный адрес в публичный.

Если необходимо доставить пакет из публичного сегмента X в публичный сегмент Y, то преобразование NAT для сегмента X encapsулирует пакет в IP-заголовок с адресом получателя, установленной в публичном адресе устройства, выполняющего NAT для сегмента X. Когда преобразование для сегмента Y получает пакет с адресом получателя, NAT decapsулирует IP-заголовок и перенаправляет пакет во внутреннюю сеть.

## Проблемы клиента FTP за устройством NAT в активном режиме

FTP-протокол передает файлы по сети.

FTP-клиент может указать серверу использование активного режима, посылает команду "PORT", которая сообщает серверу, что нужно поднимать сервер FTP и порт клиента, и начать отправку данных.

Проблема 1. Сервер должен сам поднять на клиент IP-адрес. Если на пути будет какой-то брандмауэр, блокирующий все входящие подключения, сессия FTP не состоится.

Решение. Клиент FTP должен быть настроен на использование пассивного режима.

Проблема 2. Клиент использует внутренний IP-адрес. Сообщив адрес серверу, клиент обрекает его на невозможность подключения.

Решение. Настройка NAT за активным соединением FTP.

В зависимости от способа установки соединения для передачи данных работают активный и пассивный режимы работы FTP. В активном режиме сервер сам устанавливает соединение передачи данных клиенту в порт сервера.

## Проблема у FTP SSH проблема реализации записи активного соединения

FTP SSH возникает и проблема туннелирования обычной FTP-сессии через SSH-соединение. Поскольку FTP использует несколько TCP-соединений, туннелирование через SSH особенно затруднительно. Когда много клиентов пытаются установить туннель для канала управления, записей будет только одна; при передаче данных произойдет обрывание FTP на любом канале, установленном после первого соединения, которые обходят SSH-соединение и тем самым нарушают целостность записи.

Решение №1. А. 439-4

## URL. URI. URN

Uniform Resource Locator - URI, который позволяет идентифицировать ресурс, предоставляя инфу о его местонахождении.

URI Uniform Resource Identifier - единообразный идентификатор ресурса, представляющий собой короткую последовательность символов, идентифицирующую абстрактный/физический ресурс.

URN Uniform Resource Name - URI, который идентифицирует ресурс в определенном пространстве имен.

## Проблемы FTP

Проблема вспомогательного соединения в том, что существует идентификация РТА протокола не предусматривается никакого метода проверки того, кто клиент/сервер, который установлен. Соед. это именно тот, кто запросил это соединение в управляющем соединении. Многие ОС назначают TCP порты последовательно в порядке возрастания, в результате в FTP протоколе создаются условия, позволяющие атакующей стороне перехватить данные.

Исключается проверка ~~адресов~~ IP-адресов соединений, идентифицированных именами. Это значит, что передача в пассивном режиме данных происходит по обычной TCP-соединению.

## Samba ( smb )

Samba - пакет прог, который позволяет обращаться к сетевым дискам и принтерам на разных ОС по протоколу SMB.

SMB-протокол, если на тех-же клиент-сервер, который предоставляет клиент-или-принтер-или-просто-способ для чтения и записи файлов, а также запроса услуг у серверных программ в разл-ых типах сетевого окруж-ия. Серверы предоставляют файловые системы и другие ресурсы для общего доступа в сети.

Решит М.А. 439-4