

Практика 4. Прикладной уровень (сдать до 19.03.2022)

1. Программирование сокетов: Прокси-сервер

Разработайте прокси-сервер для проксирования веб-страниц.

Запуск прокси-сервера

Запустите свой прокси-сервер из командной строки, а затем запросите веб-страницу с помощью вашего браузера. Направьте запросы на прокси-сервер, используя свой IP-адрес и номер порта.

Например,

`http://localhost:8888/www.google.com`

(*)Вы должны заменить стоящий здесь 8888 на номер порта, который вы использовали в серверном коде, то есть тот, на котором прокси-сервер слушает запросы.

Вы можете также настроить непосредственно веб-браузер на использование вашего прокси-сервера. В настройках браузера вам нужно будет указать адрес прокси-сервера и номер порта, который вы использовали при запуске прокси-сервера (опционально).

А. Прокси-сервер без кеширования (4 балла)

1. Разработайте свой прокси-сервер для проксирования http GET запросов от клиента веб-серверу с журналированием проксируемых HTTP-запросов. В файле журнала сохраняется краткая информация о проксируемых запросах (URL и код ответа). Кеширование в этом задании не требуется. (2 балла)
2. Добавьте в ваш прокси-сервер обработку ошибок. Отсутствие обработчика ошибок может вызвать проблемы. Особенно, когда клиент запрашивает объект, который не доступен, так как ответ 404 Not Found, как правило, не имеет тела, а прокси-сервер предполагает, что тело есть и пытается прочитать его. (1 балл)
3. Простой прокси-сервер поддерживает только метод GET протокола HTTP. Добавьте поддержку метода POST. В запросах теперь будет использоваться также тело запроса (body). Для вызова POST запросов вы можете использовать Postman. (1 балл)

Б. Прокси-сервер с кешированием (4 балла)

Когда прокси-сервер получает запрос, он проверяет, есть ли запрашиваемый объект в кэше, и, если да, то возвращает объект из кэша без соединения с веб-сервером. Если объекта в кэше нет, прокси-сервер извлекает его с веб-сервера обычным GET запросом, возвращает клиенту и кеширует копию для будущих запросов.

Для проверки того, прокис объект в кеше или нет, необходимо использовать условный GET запрос. В таком случае вам необходимо указывать в заголовке запроса значение для If-Modified-Since и If-None-Match. Подробности можно найти тут:

<https://ruturajv.wordpress.com/2005/12/27/conditional-get-request>

Будем считать, что кеш-память прокси-сервера хранится на его жестком диске. Ваш прокси-сервер должен уметь записывать ответы в кеш и извлекать данные из кэша (т.е. с диска) в случае попадания в кэш при запросе. Для этого необходимо реализовать некоторую внутреннюю структуру данных, чтобы отслеживать, какие объекты закешированы.

В. Черный список / Black list (2 балла)

Прокси-сервер отслеживает страницы и не пускает на те, которые попадают в black list. Вместо этого прокси-сервер отправляет предупреждение, что страница заблокирована. Список доменов и/или URL-адресов для блокировки по черному списку задается в конфигурационном файле

2. Wireshark. Работа с DNS

Для каждого задания в этой секции приложите скрин с подтверждением ваших ответов.

А. Утилита nslookup (1 балл)

- Выполните nslookup, чтобы получить IP-адрес какого-либо веб-сервера в Азии
- Выполните nslookup, чтобы определить авторитетные DNS-серверы для какого-либо университета в Европе
- Используя nslookup, найдите веб-сервер, имеющий несколько IP-адресов. Сколько IP-адресов имеет веб-сервер вашего учебного заведения?

Б. DNS-трассировка www.ietf.org (3 балла)

Предварительная подготовка:

1. Используйте ipconfig для очистки кэша DNS на вашем компьютере.
2. Откройте браузер и очистите его кэш (для Chrome можете использовать сочетание клавиш CTRL+Shift+Del).
3. Запустите Wireshark и введите ip.addr == ваш_IP_адрес в строке фильтра, где значение ваш_IP_адрес вы можете получить, используя утилиту ipconfig. Данный фильтр позволит нам отбросить все пакеты, не относящиеся к вашему хосту. Запустите процесс захвата пакетов в Wireshark.
4. Зайдите на страницу www.ietf.org в браузере.
5. Остановите захват пакетов.

Вопросы:

- Найдите DNS-запрос и ответ на него. С использованием какого транспортного протокола они отправлены?
- Какой порт назначения у запроса DNS?
- На какой IP-адрес отправлен DNS-запрос? Используйте ipconfig для определения IP-адреса вашего локального DNS-сервера. Одинаковы ли эти два адреса?
- Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?
- Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?
- Посмотрите на последующий TCP-пакет с флагом SYN, отправленный вашим компьютером. Соответствует ли IP-адрес назначения пакета с SYN одному из адресов, приведенных в ответном сообщении DNS?
- Веб-страница содержит изображения. Выполняет ли хост новые запросы DNS перед загрузкой этих изображений?

В. DNS-трассировка www.spbu.ru (2 балла)

Предварительная подготовка:

1. Запустите захват пакетов с тем же фильтром ip.addr == ваш_IP_адрес
2. Выполните команду nslookup для сервера www.spbu.ru.
3. Остановите захват
4. Вы увидите несколько пар запрос-ответ DNS. Найдите последнюю пару, все вопросы будут относиться к ней

Вопросы:

- Каков порт назначения в запросе DNS? Какой порт источника в DNS-ответе?
- На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNS-сервера, установленного по умолчанию?

- Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?
- Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?

Г. DNS-трассировка `nslookup -type=NS` (1 балл)

Повторите все шаги по предварительной подготовке из Задания В, но теперь для команды:

`nslookup -type=NS spbu.ru`

Вопросы:

- На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNS-сервера, установленного по умолчанию?
- Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?
- Проанализируйте ответное сообщение DNS. Имена каких DNS-серверов университета в нем содержатся? А есть ли их адреса в этом ответе?

Д. DNS-трассировка `nslookup www.spbu.ru ns2.pu.ru` (1 балл)

Снова повторите все шаги по предварительной подготовке из Задания В, но теперь для команды:

`nslookup www.spbu.ru ns2.pu.ru`

Вопросы:

- На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNS-сервера, установленного по умолчанию? Если нет, то какому хосту он принадлежит?
- Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?
- Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?

Е. Сервисы `whois` (2 балла)

- Что такое база данных `whois`?
- Используя различные сервисы `whois` в Интернете, получите имена любых двух DNS-серверов. Какие сервисы вы при этом использовали?
- Используйте команду `nslookup` на локальном хосте чтобы послать запросы трем серверам DNS: вашему локальному серверу DNS и двум DNS-серверам, найденным в предыдущей части.