НИУ ИТМО

Факультет программной инженерии и компьютерных технологий

Отчет по лабораторной работе №4

по дисциплине Компьютерные сети

|  |  |
| --- | --- |
| Студент группы № P33151 | Шипулин Павел Андреевич |
| Преподаватель | Тропченко Андрей Александрович |

Санкт-Петербург

2024

# ЭТАПЫ И ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

## Этап 1. Анализ трафика утилиты ping

Необходимо отследить и проанализировать трафик, создаваемый утилитой ping, запустив её следующим образом из командной строки:

* «ping -l размер\_пакета адрес\_сайта\_по\_варианту».
* Например, «ping -l 2000 wireshark.org» (без кавычек).

В качестве «размера\_пакета» необходимо поочерёдно использовать различные значения от 100 до 10000, самостоятельно выбрав шаг изменения. По результатам анализа собранной трассы, необходимо ответить на следующие вопросы и выполнить указанные задания.

1. Имеет ли место фрагментация исходного пакета, какое поле на это указывает?

Да. Поле More Fragments = 1.

1. Какая информация указывает, является ли фрагмент пакета последним или промежуточным?

Если поле More Fragments = 0, то пакет является последним.

1. Чему равно количество фрагментов при передаче ping-пакетов?

Зависит от количества передаваемой информации, которая будет разбита на пакеты, у которых есть максимальный размер поля данных, равный 1500 байт.

1. Построить график, в котором на оси абсцисс находится размер пакета (килобайт), а по оси ординат – количество фрагментов, на которое был разделён каждый ping-пакет.

Изображение выглядит как Параллельный, линия, прямоугольный, текст

Автоматически созданное описание

1. Как изменить поле TTL с помощью утилиты ping?

ping -i <число>

1. Что содержится в поле данных ping-пакета?

Байты передаваемой информации. При использовании ping – это будут последовательные символы английского алфавита и прочие символы кодировки.

## Этап 2. Анализ трафика утилиты tracert (traceroute)

Необходимо отследить и проанализировать трафик, создаваемый утилитой tracert (или traceroute в Linux), запустив её следующим образом из командной

строки:

* «tracert -d адрес\_сайта\_по\_варианту»
* Например, tracert wireshark.org.

По результатам анализа собранной трассы, ответьте на следующие вопросы.

1. Сколько байт содержится в заголовке IP? Сколько байт содержится в поле данных?

20 байт. 64 байт.

1. Как и почему изменяется поле TTL в следующих друг за другом ICMP пакетах tracert? Для ответа на этот вопрос нужно проследить изменение TTL при передаче по маршруту, состоящему из более чем двух хопов.

Команда увеличивает TTL на 1 пока не будет получен ответ от следующего узла в маршруте.

1. Чем отличаются ICMP-пакеты, генерируемые утилитой tracert, от ICMP пакетов, генерируемых утилитой ping (см. предыдущее задание).

Поле данных пакетов ICMP заполнено нулевыми байтами.

1. Чем отличаются полученные пакеты «ICMP reply» от «ICMP error» и зачем нужны оба этих типа ответов?

Reply – ответ от узла. Error – произошла ошибка, например истекло время TTL.

1. Что изменится в работе tracert, если убрать ключ «-d»? Какой дополнительный трафик при этом будет генерироваться?

Вместо доменов будут отображаться адреса.

## Этап 3. Анализ HTTP-трафика

Необходимо отследить и проанализировать HTTP-трафик, создаваемый браузером при посещении Интернет-сайта, заданного по варианту. В списке захваченных пакетов необходимо проанализировать следующую пару HTTP сообщений (запрос-ответ):

* GET-сообщение от клиента (браузера);
* ответ сервера.

Для этого в поле с детальной информацией о пакете нужно развернуть строку «HTTP». Затем необходимо обновить страницу в браузере так, чтобы вместо «HTTP GET» был сгенерирован «HTTP CONDITIONAL GET» (так называемый «условный GET»). Условные запросы GET содержат поля IfModified-Since, If-Match, If-Range и подобные, которые позволяют при повторном запросе не передавать редко изменяемые данные. В ответ на условный GET тело запрашиваемого ресурса передается только в том случае, если этот ресурс изменялся после даты «If-Modified-Since». Если ресурс не изменялся, сервер вернет код статуса «304 Not Modified».

По результатам анализа собранной трассы покажите, каким образом протокол HTTP передавал содержимое страницы при первичном посещении страницы и при вторичном запросе-обновлении от браузера (т. е. при различных видах GET-запросов).

## Этап 4. Анализ DNS-трафика

Необходимо отследить и проанализировать трафик протокола DNS, сгенерированный в результате выполнения следующих действий:

* настроить Wireshark-фильтр: «ip.addr == ваш\_IP\_адрес»;
* очистить кэш DNS с помощью команды ipconfig в командной строке: ipconfig /flushdns
* очистить кэш браузера;
* зайти на Интернет-сайт, заданный по варианту.

По результатам анализа собранной трассы, ответьте на следующие вопросы.

1. Почему адрес, на который отправлен DNS-запрос, не совпадает с адресом посещаемого сайта?

Потому что компьютер не имеет достаточно информации про необходимый ресурс, и чтобы узнать о нём – обращается к маршрутизатору.

1. Какие бывают типы DNS-запросов?

* Прямой – получить адрес по имени
* Обратный – получить имя по адресу
* Итеративный – ??
* Рекурсивный – выполняется DNS сервером, чтобы найти домен.

1. В какой ситуации нужно выполнять независимые DNS-запросы для получения содержащихся на сайте изображений?

Если эти изображения хранятся на другом ресурсе.

## Этап 5. Анализ ARP-трафика

Необходимо отследить и проанализировать трафик протокола ARP, сгенерированный в результате выполнения следующих действий:

* очистить ARP-таблицу командой «netsh interface ip delete arpcache» (проверить очистилась ли таблица можно с помощью команды команды «arp -a», выводящей таблицу на экран);
* очистить кэш браузера;
* зайти на Интернет-сайт, заданный по варианту.

По результатам анализа собранной трассы, ответьте на следующие вопросы.

1. Какие МАС-адреса присутствуют в захваченных пакетах ARP протокола? Что означают эти адреса? Какие устройства они идентифицируют?
2. Какие МАС-адреса присутствуют в захваченных HTTP-пакетах и что означают эти адреса? Что означают эти адреса? Какие устройства они идентифицируют?
3. Для чего ARP-запрос содержит IP-адрес источника?

## Этап 6. Анализ трафика утилиты nslookup

Это задание является необязательным, его необходимо выполнить только для желающих получить оценку «хорошо» или «отлично». Необходимо отследить и проанализировать трафик протокола DNS, сгенерированный в результате выполнения следующих действий:

1. Настроить Wireshark-фильтр: «ip.addr == ваш\_IP\_адрес».
2. Запустить в командной строке команду «nslookup адрес\_сайта\_по\_варианту».
3. Дождаться отправки трёх DNS-запросов и трёх DNS-ответов (в работе нужно использовать только последние из них, т.к. первые два набора запросов/ответов специфичны для nslookup и не генерируются другими сетевыми приложениями).
4. Повторить предыдущие два шага, используя команду:

«nslookup -type=NS имя\_сайта\_по\_варианту».

По результатам анализа собранной трассы, ответьте на следующие вопросы.

1. Чем различается трасса трафика в п.2 и п.4, указанных выше?
2. Что содержится в поле «Answers» DNS-ответа?
3. Каковы имена серверов, возвращающих авторитативный (authoritative) отклик?

## Этап 7. Анализ FTP-трафика

Это задание является необязательным, его необходимо выполнить только для желающих получить оценку «хорошо» или «отлично». Необходимо отследить и проанализировать трафик протокола FTP, сгенерированный в результате выполнения следующих действий:

* настроить Wireshark-фильтр «ftp || ftp-data»;
* скачать в браузере небольшой файл с соответствующего варианту FTP сервера в Интернете.

В адресной строке путь к скачиваемому файлу должен начинаться с «ftp://». Адрес сайта нужно выбрать, руководствуясь правилами, указанными в пункте 3.

По результатам анализа собранной трассы, ответьте на следующие вопросы.

1. Сколько байт данных содержится в пакете FTP-DATA?
2. Как выбирается порт транспортного уровня, который используется для передачи FTP-пакетов?
3. Чем отличаются пакеты FTP от FTP-DATA?

## Этап 8. Анализ DHCP-трафика

Это задание является необязательным, его необходимо выполнить для желающих получить оценку «отлично». Необходимо отследить и проанализировать трафик протокола DHCP, сгенерированный в результате выполнения следующих действий:

1. Убедиться, что для назначения IP-адреса на компьютере был использован DHCP и что компьютеру был назначен IP-адрес.
2. Настроить Wireshark-фильтр «bootp» (во время защиты УИР следует объяснить, почему именно такой фильтр используется для анализа DHCP-трафика).
3. Сбросить текущий IP-адрес, выданный накануне перед этим DHCPсервером, с помощью команды:

«ipconfig /release».

1. Запросить новый IP-адрес с помощью команды:

«ipconfig /renew».

1. Повторить п.3 и п.4.

Нарисуйте временную диаграмму, иллюстрирующую последовательность обмена первыми четырьмя DHCP-пакетами Discover/Offer/Request/ACK. Укажите для каждого пакета номера портов источника и назначения. По результатам анализа собранной трассы, ответьте на следующие вопросы.

1. Чем различаются пакеты «DHCP Discover» и «DHCP Request»?
2. Как и почему менялись MAC- и IP-адреса источника и назначения в переданных DHCP-пакетах.
3. Каков IP-адрес DHCP-сервера?
4. Что произойдёт, если очистить использованный фильтр «bootp»?