ЛАБОРАТОРНАЯ РАБОТА 3

АНАЛИЗ СТРУКТУРЫ СЕТЕВОГО ТРАФИКА С ПОМОЩЬЮ ПРОГРАММ *WIRESHARK И OSTINATO*

Содержание

Лабораторная работа составлена по материалам книги *Computer Networking: A Top-Down Approach, 6th ed.,* J.F. Kurose and K.W. Ross.

Часть 1. Исследование структуры сетевых пакетов с помощью анализатора трафика Wireshark

Постановка задачи

В соответствии с заданием требуется проанализировать трафик, захваченный программой *Wireshark,* а именно:

1) рассмотреть структуру пакета, указав назначение каждого заголовка;
2) пояснить механизм инкапсуляции протоколов.

В отчете привести скриншоты, иллюстрирующие ответы на поставленные в задании вопросы (также пакет можно распечатать прямо из программы *Wireshark*). Необходимо иметь с собой на flash-носителе сохраненную версию захваченного трафика (так называемый дамп трафика) в формате pcap (это стандартный формат сохранения трафика в Wireshark).

Во всех вариантах задания необходимо выполнить следующие этапы исследования.

Протокол IP

1) запустить *Wireshark;*

2) запустить процесс захвата трафика;

3) в командной строке:

   tracert конечный_узел

   например, tracert wireshark.org

   в качестве конечного узла использовать URL, в котором по очереди встречаются инициалы фамилии и имени студента в латинской транскрипции (например, для имени Пётр Иванов подойдут адреса сайтов http://pictures.com или http://nopix.ru/;

4) остановить захват трафика.

В информационном поле разверните строку, содержащую «Internet Protocol». Ответьте на следующие вопросы.

1. Проанализируйте первый пакет ICMP Echo Request, отправленный вашим компьютером: укажите ваш IP-адрес.
2. Приведите значение поля, определяющее протокол верхнего уровня.
3. Сколько байт содержится в заголовке IP? Сколько байт в поле данных?
4. Укажите значение TTL. Как изменяется это поле в разных ICMP Echo Request?
5. Какое значение содержится в поле «Identification»? Для чего используется это поле?

Фрагментация пакетов

1) запустить *Wireshark;*
2) запустить процесс захвата трафика;
3) в командной строке:
4) ping –l 2000 конечный_узел (ключ -l позволяет указать загрузку поля «Data» пакета в байтах)

   например, ping –l 2000 wireshark.org

   в качестве конечного узла использовать URL, в котором присутствуют любые три буквы из фамилии студента в латинской транскрипции;

5) остановить захват трафика.

Ответьте на следующие вопросы.

1. Проанализируйте пакет ICMP Echo Request: имеет ли место фрагментация исходного пакета, какое поле на это указывает?
2. Проанализируйте фрагменты IP-дейтаграммы: какая информация указывает, является ли фрагмент пакета последним или промежуточным?
3. Укажите количество фрагментов исходного пакета.

На этом общая часть задания заканчивается. Описание вариативной части приведено в следующем параграфе. Номер варианта выдает преподаватель.

Описание программы Wireshark

Для выполнения лабораторной работы необходимо установить на компьютер программу-анализатор сетевых пакетов Wireshark, скачав ее с официального сайта http://wireshark.org. На рис. 1 представлено главное окно *Wireshark.*

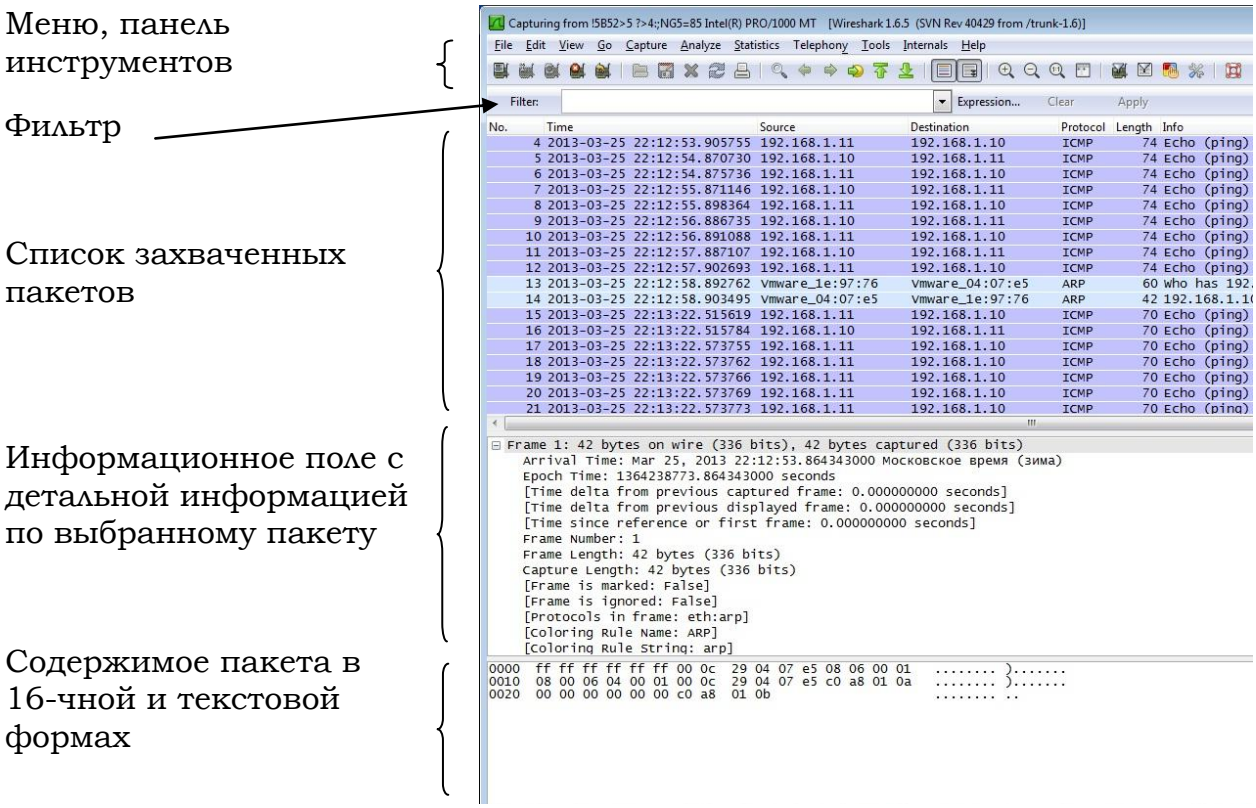

Рис. 1. Wireshark GUI

Начать работу с Wireshark следует следующим образом:

1) открыть браузер;
2) запустить *Wireshark*:
   a) установить параметры для захвата трафика; в качестве интерфейса, используемого для захвата трафика, выбрать физический адаптер, тип адаптера — Local (рис. 2);
   b) запустить процесс захвата трафика (кнопка *Start*);
3) в браузере открыть любой сайт (например, http://www.wireshark.org/docs/wsug_html_chunked/);
4) установить значение фильтра, равным http;

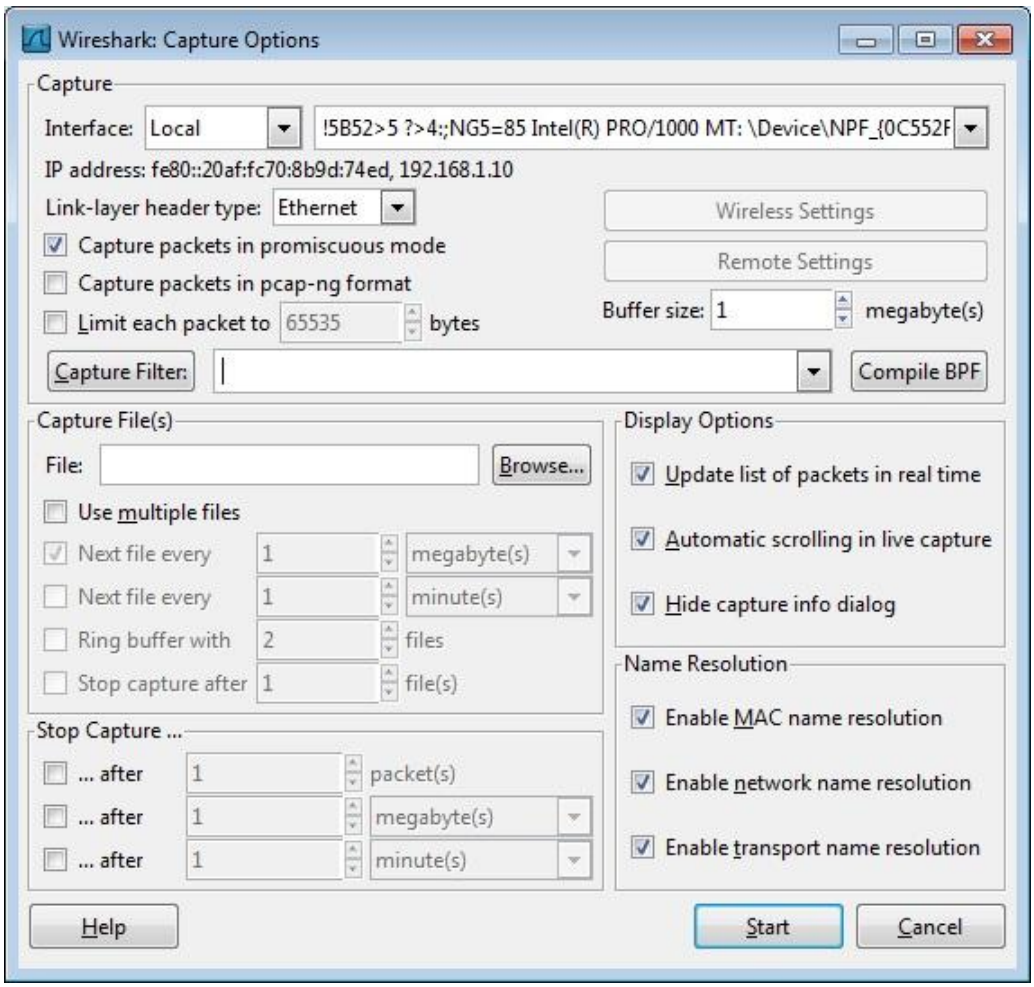

Рис. 2. Параметры захвата трафика

5) выбрать первое http сообщение в списке пакетов — это будет сообщение HTTP GET, отправленное на указанный хост (например, www.wireshark.org); в информационном поле отображена детальная информация по заголовкам пакета.

Варианты задания

Вариант 1. HTTP: Basic HTTP GET/response

1) запустить *Wireshark;*
2) настроить фильтр (http);
3) запустить процесс захвата трафика;
4) URL: например, http://wiki.wireshark.org/;

   в URL должны присутствовать любые три буквы из фамилии студента в латинской транскрипции;

5) остановить захват трафика.

Прим.: Не принимать во внимание HTTP запрос и ответ для favicon.ico. Появление ссылки на данный файл означает, что браузер автоматически

запрашивает сервер о наличии маленького значка веб-сайта, т. н. «Favicon» (отображается браузером в адресной строке перед URL страницы, а также в качестве картинки рядом с закладкой, во вкладках и в других элементах интерфейса).

В списке захваченных пакетов найдите пару HTTP сообщений (запрос-ответ): GET сообщение и ответ сервера.
В информационном поле разверните строку, содержащую HTTP, и отметьте указанную ниже информацию.

1. Версия HTTP.
2. Принимаемые браузером языки.
3. IP-адреса вашего компьютера и сервера.
4. Код состояния HTTP. Что он означает?
5. Длина тела сообщения. (Содержимое поля заголовка объекта Content-Length указывает длину тела сообщения в октетах (десятичное число), или в случае метода HEAD, размер тела объекта, который мог бы быть послан при запросе GET.)
6. Протокол транспортного уровня, который использует HTTP.

Вариант 2. HTTP: HTTP CONDITIONAL GET/response (Условный GET[1])

1) очистить кэш браузера;
2) открыть браузер;
3) запустить *Wireshark;*
4) запустить процесс захвата трафика;
5) URL: например, http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html

   в URL должны присутствовать любые три буквы из фамилии студента в латинской транскрипции;
6) быстро обновить страницу в браузере;
7) остановить захват трафика;
8) настроить фильтр (http).

[1] Кроме обычного метода GET, различают ещё условный GET и частичный GET. Условные запросы GET содержат заголовки If-Modified-Since, If-Match, If-Range и подобные. Метод GET изменяется на «условный GET», если сообщение запроса включает в себя поле заголовка «If-Modified-Since». В ответ на условный GET, тело запрашиваемого ресурса передается только, если он изменялся после даты, указанной в заголовке «If-Modified-Since». Алгоритм определения этого включает в себя следующие случаи:

- Если код статуса ответа на запрос будет отличаться от «200 OK», или дата, указанная в поле заголовка «If-Modified-Since» некорректна, ответ будет идентичен ответу на обычный запрос GET.
- Если после указанной даты ресурс изменялся, ответ будет также идентичен ответу на обычный запрос GET.
- Если ресурс не изменялся после указанной даты, сервер вернет код статуса «304 Not Modified».

Использование метода условный GET направлено на разгрузку сети, так как он позволяет не передавать по сети избыточную информацию.

Прим.: Не принимать во внимание HTTP запрос и ответ для favicon.ico. Появление ссылки на данный файл означает, что браузер автоматически запрашивает сервер о наличии маленького значка веб-сайта, т. н. «Favicon» (отображается браузером в адресной строке перед URL страницы, а также в качестве картинки рядом с закладкой, во вкладках и в других элементах интерфейса).

Ответьте на следующие вопросы.

1. Укажите версию HTTP и принимаемые браузером языки.
2. Укажите IP-адреса вашего компьютера и сервера.
3. Есть ли в первом запросе HTTP GET строка «IF-MODIFIED-SINCE»?
4. Проанализируйте ответ сервера на первый запрос: передал ли сервер явным образом содержимое запрашиваемого ресурса?
5. Теперь просмотрите содержимое второго запроса HTTP GET: есть ли там строка «IF-MODIFIED-SINCE» (какую информацию содержит)?
6. Что означает код состояния в ответе сервера на второй запрос HTTP GET? Передал ли сервер явным образом содержимое запрашиваемого ресурса?

Вариант 3. DNS

1) очистить кэш DNS с помощью *ipconfig* (в командной строке)*:*

   ipconfig /flushdns

2) очистить кэш браузера;

3) запустить *Wireshark;*

4) настроить фильтр: ip.addr == ваш_IP_адрес;

5) запустить процесс захвата трафика;

6) URL: например, http://www.ietf.org/;

   в URL должны присутствовать любые три буквы из фамилии студента в латинской транскрипции;

7) остановить захват трафика.

Ответьте на следующие вопросы.

1. Найдите DNS-запрос и ответ. Поверх какого протокола транспортного уровня работает DNS?
2. Укажите порты источника/назначения для DNS-запроса и DNS-ответа.
3. На какой IP-адрес отправлен DNS-запрос? Совпадает ли этот адрес с адресом вашего DNS-сервера?
4. Укажите тип DNS-запроса.
5. Что содержится в поле «Answers» DNS-ответа?
6. Проверьте, какой IP-адрес содержится в последующем пакете TCP SYN, который был отправлен вашим компьютером.
7. Формирует ли ваш компьютер новые DNS-запросы для получения содержащихся на сайте изображений?

Вариант 4. DNS

nslookup — утилита, предоставляющая пользователю интерфейс командной строки для обращения к системе DNS (проще говоря, DNS-клиент). Позволяет задавать различные типы запросов и запрашивать произвольно указываемые сервера.

Использование *nslookup:*

```
nslookup [-opt ...]
  # интерактивный режим с использованием сервера по умолчанию
nslookup [-opt ...] - server
  # интерактивный режим с использованием сервера "server"
nslookup [-opt ...] host
  # поиск узла "host" с использованием сервера по умолчанию
nslookup [-opt ...] host server
  # поиск узла "host" с использованием сервера "server"
```

1) запустить *Wireshark;*
2) настроить фильтр: ip.addr == ваш_IP_адрес;
3) запустить процесс захвата трафика;
4) в командной строке:

   nslookup host

   например, nslookup ifmo.ru

   в качестве узла (host) использовать URL, в котором присутствуют любые три буквы из фамилии студента в латинской транскрипции;
5) остановить захват трафика.

Прим.: Всего *nslookup* отправил три DNS-запроса и получил три DNS-ответа. Для дальнейшего анализа использовать последние два пакета. (Первые два набора запросов/ответов не генерируются стандартными интернет-приложениями и специфичны для *nslookup*.)

Ответьте на следующие вопросы.

1. Найдите DNS-запрос и ответ. Поверх какого протокола транспортного уровня работает DNS?
2. Укажите порты источника/назначения для DNS-запроса и DNS-ответа.
3. На какой IP-адрес отправлен DNS-запрос? Совпадает ли этот адрес с адресом вашего DNS-сервера?
4. Укажите тип DNS-запроса.
5. Что содержится в поле «Answers» DNS-ответа?

Повторите предыдущий эксперимент, но в командной строке введите команду:

nslookup -type=NS host

например, nslookup -type=NS ifmo.ru

в качестве узла (host) использовать URL, в котором присутствуют любые три буквы из фамилии студента в латинской транскрипции;

Ответьте на следующие вопросы.

1. Укажите порты источника/назначения для DNS-запроса и DNS-ответа.
2. На какой IP-адрес отправлен DNS-запрос? Совпадает ли этот адрес с адресом вашего DNS-сервера?
3. Укажите тип DNS-запроса.
4. Проанализируйте DNS-ответ: укажите имена серверов, возвращающих авторитативный[2] отклик.

Вариант 5. ICMP

1) запустить *Wireshark;*

2) настроить фильтр (icmp);

3) запустить процесс захвата трафика;

4) в командной строке:

   ping –n 10 конечный_узел

   например, ping –n 10 wireshark.org

   в качестве конечного узла использовать URL, в котором присутствуют любые три буквы из фамилии студента в латинской транскрипции;

5) остановить захват трафика.

Ответьте на следующие вопросы.

1. Сколько всего пакетов захватила программа? Почему?
2. Какой IP-адрес вашего компьютера, адрес назначения?
3. Проанализируйте ping request, отправленный с вашего компьютера: укажите тип и код ICMP. Какие еще поля содержит ICMP пакет? Сколько байт занимают поля «Checksum», «Sequence number», «Identifier»?
4. Проанализируйте ping reply: укажите тип и код ICMP. Какие еще поля содержит ICMP пакет? Сколько байт занимают поля «Checksum», «Sequence number», «Identifier»?

6) запустить *Wireshark;*

7) настроить фильтр (icmp);

8) запустить процесс захвата трафика;

[2] Под авторитативным (autorative) сервером зоны понимается такой DNS сервер, который официально поддерживает описание зоны. При обращении к такому серверу с запросом по поводу информации о поддерживаемой им (сервером) официально зоне клиент (resolver) получает авторитативный отклик.

9) в командной строке:

   tracert конечный_узел

   например, tracert wireshark.org

   в качестве конечного узла использовать URL, в котором присутствуют любые три буквы из фамилии студента в латинской транскрипции;

10) остановить захват трафика.

Ответьте на следующие вопросы.

1. Какой IP-адрес вашего компьютера, адрес назначения?
2. Проанализируйте пакет ICMP echo: отличаются ли эти пакеты от пакетов в первой части эксперимента? Чем?
3. Проанализируйте пакет ICMP error: какие поля в нем содержатся?
4. Чем отличаются пакеты ICMP reply (полученные) и ICMP error?

Вариант 6. DHCP

1) в командной строке:

   ipconfig /release (IP-адрес станет 0.0.0.0)

2) запустить *Wireshark;*

3) настроить фильтр (bootp);

4) запустить процесс захвата трафика;

5) в командной строке:

   ipconfig /renew (получение нового IP-адреса)

   и еще раз:

   ipconfig /release

   ipconfig /renew

6) остановить захват трафика.

Ответьте на следующие вопросы.

1. Поверх какого протокола транспортного уровня работает DHCP?
2. Нарисуйте временную диаграмму, иллюстрирующую последовательность обмена первыми четырьмя пакетами Discover/Offer/Request/ACK. Укажите для каждого пакета номера портов источника, назначения.
3. Какими значениями отличаются пакеты DHCP Discover и DHCP Request?
4. Укажите значения поля «Transaction-ID» для всех пакетов (Discover/Offer/Request/ACK), что это поле означает?
5. Укажите IP-адреса источника, назначения для всех пакетов.

6. Укажите IP-адрес DHCP сервера.
7. Поясните назначение сообщения DHCP release.
8. Очистите фильтр. Появились ли пакеты ARP, отправленные или полученные в течение обмена DHCP пакетами? Почему?

Вариант 7. Ethernet и ARP

Ethernet

1) очистить кэш браузера;

2) запустить *Wireshark;*

3) запустить процесс захвата трафика;

4) URL: например, http://ru.wikipedia.org/wiki/Ethernet

   в URL должны присутствовать любые три буквы из фамилии студента в латинской транскрипции;

5) остановить захват трафика;

6) в меню «Analyze» → «Enabled Protocols» можно снять галочку IP:тогда в списке пакетов не будет отображаться информация по протоколам верхнего уровня (после IP) — необязательный пункт.

Выберите кадр Ethernet, содержащий сообщение HTTP GET.
Ответьте на следующие вопросы.
1. Укажите 48-битный Ethernet адрес вашего компьютера.
2. Укажите 48-битный Ethernet адрес назначения. Что это за адрес? (Адрес сервера?)
3. Укажите 16-чное значение двухбайтового поля «Type»: какому протоколу верхнего уровня оно соответствует?

Выберите кадр Ethernet, содержащий ответ HTTP.
Ответьте на следующие вопросы.
1. Укажите значение Ethernet адреса источника. Какое устройство имеет такой адрес?
2. Укажите Ethernet адрес назначения: это адрес вашего компьютера?
3. Укажите 16-чное значение двухбайтового поля «Type»: какому протоколу верхнего уровня оно соответствует?

ARP

1) очистить ARP кэш:

   «Пуск» → «Выполнить»: netsh interface ip delete arpcache
   Вывести на экран ARP-таблицу можно с помощью команды: arp –a

2) очистить кэш браузера;

3) запустить *Wireshark;*

4) запустить процесс захвата трафика;

5) URL: например, http://ru.wikipedia.org/wiki/Ethernet

   в URL должны присутствовать любые три буквы из фамилии студента в латинской транскрипции;

6) остановить захват трафика;

7) в меню «Analyze» → «Enabled Protocols» снять галочку IP: в списке пакетов теперь не будет отображаться информация по протоколам верхнего уровня (после IP) — необязательный пункт.

Ответьте на следующие вопросы.

1. Укажите 16-чные значения адресов источника и назначения в пакете, содержащем ARP запрос (ARP ответ).
2. Укажите 16-чное значение двухбайтового поля «Type»: какому протоколу верхнего уровня оно соответствует (для ARP запроса/ARP ответа)?
3. Укажите значение поля «opcode» (для ARP запроса/ARP ответа).
4. Содержит ли ARP запрос IP-адрес источника (для ARP запроса/ARP ответа)?

Вариант 8. FTP

1) запустить *Wireshark;*

2) запустить процесс захвата трафика;

3) скачать файл с FTP-сервера (например, ftp://ftp.canon.ru/);

   в URL должны присутствовать любые три буквы из фамилии студента в латинской транскрипции;

4) остановить захват трафика;

5) настроить фильтр (ftp || ftp-data).

Ответьте на следующие вопросы.

1. Сколько байт данных содержится в пакете FTP-DATA?
2. Укажите IP-адреса FTP-сервера и вашего компьютера.
3. Укажите MAC-адрес FTP-сервера.
4. Укажите протокол транспортного уровня, который использует протокол FTP.
5. Укажите порт, который используется при передаче данных по протоколу FTP.
6. Поясните, чем отличаются пакеты FTP и FTP-DATA.

Вариант 9. UDP

1) запустить *Wireshark;*

2) настроить фильтр (udp);

3) запустить процесс захвата трафика;

4) создать сеанс связи с помощью программы *TeamViewer*;

5) остановить захват трафика.

Прим.: можно ничего не делать, просто запустить захват трафика — UDP пакеты все равно найдутся.

Ответьте на следующие вопросы.

1. Выберите один UDP пакет из списка пакетов. Сколько полей в UDP заголовке? Что это за поля?
2. Какова длина (в байтах) каждого поля заголовка?
3. Длина чего указана в поле «Length»?
4. Какова максимальная длина поля данных UDP?
5. Какой максимально возможный номер порта источника?
6. Укажите номер протокола для UDP (см. соответствующее поле IP-дейтаграммы) в 10-чном и 16-чном виде.
7. Найдите пару пакетов: первый UDP пакет, отправленный вашим компьютером, и ответ на него.

Часть 2. Исследование структуры сетевых пакетов с помощью генератора пакетов Ostinato

Постановка задачи

Это задание повышенной сложности. Его выполнение необходимо, чтобы получить оценку «отлично».

В соответствии с заданием варианта А или Б требуется сгенерировать и отправить в сеть трафик с заданными параметрами. Убедиться в том, что передача пакетов действительно происходит, можно с помощью *Wireshark.*

В отчете нужно привести структуру генерируемого пакета и параметры генерации (можно в виде скриншотов Wireshark или Ostinato). Во время защиты необходимо предоставить по требованию преподавателя pcap-файл с дампом сгенерированного трафика.

Описание программы Ostinato

Прим.: для работы с генератором *Ostinato* нужны права администратора.

1. Рабочая область (рис. 3) поделена на 3 части: список портов (*ports list*), список потоков (*streams list*), окно статистики (*statistics window*).
2. В списке портов вы увидите группу портов для «127.0.0.1» со статусом «присоединена» (*connected*) (зеленый цвет).
3. Выберите порт из группы портов.
4. В списке потоков создайте новый поток: правой кнопкой → *New stream*.
5. Для редактирования созданного потока дважды щелкните на иконке потока (или правой кнопкой → *Edit stream*).
6. В окне редактирования потока выберите протоколы, заполните поля, определите количество пакетов, скорость. Нажмите «OK».
7. **Важно!** Нажмите кнопку *Apply*, которая расположена сверху списка потоков.

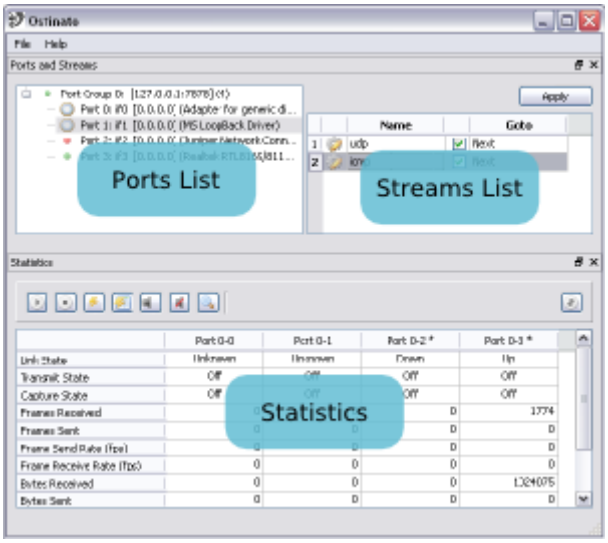

Рис. 3. Главное окно программы *Ostinato*

8. **Важно!** В окне статистики выберите тот же порт, для которого вы создавали поток (выделите весь столбец, щелкнув на заголовке порта).
9. Нажмите кнопку *Start Transmit*.

Клиент-серверная архитектура

Генератор имеет клиент-серверную архитектуру. Запущенный на одном компьютере клиент (*ostinato*) соединен с одним (или несколькими) компьютером-сервером (*drone*). Клиент имеет доступ ко всем портам всех присоединенных серверов и осуществляет управление ими. В один момент времени сервер может быть соединен только с одним клиентом. Клиент и сервер могут быть запущены на разных ОС (например, клиент Windows может быть соединен как с сервером Windows, так и Linux). Режим по умолчанию — клиент и сервер запущены на одном компьютере. Локальный сервер представлен loopback IP-адресом 127.0.0.1.

Важно! Клиент отправляет серверу конфигурационную информацию по потоку, только если была нажата кнопка *Apply*. Поэтому если вы добавляете/редактируете/удаляете потоки, не забывайте нажимать *Apply*, иначе изменения не будут сохранены.

Список портов (Ports List)

Список портов (рис. 4) отображает все порты, которые можно контролировать. Порты объединены в следующие группы портов. Группа портов это компьютер или устройство (локальное или удаленное), запущенное на серверном компоненте (*drone*). Ниже перечислены статусы группы портов:

●	Клиент не соединен с группой портов

	Клиент пытается соединиться с группой портов
	Клиент соединен с группой портов
	Клиентом обнаружена ошибка при попытке соединения с группой портов

Статусы портов. Порты могут иметь следующие статусы:

	Текущий статус порта неизвестен
	Порт не присоединен
	Порт присоединен

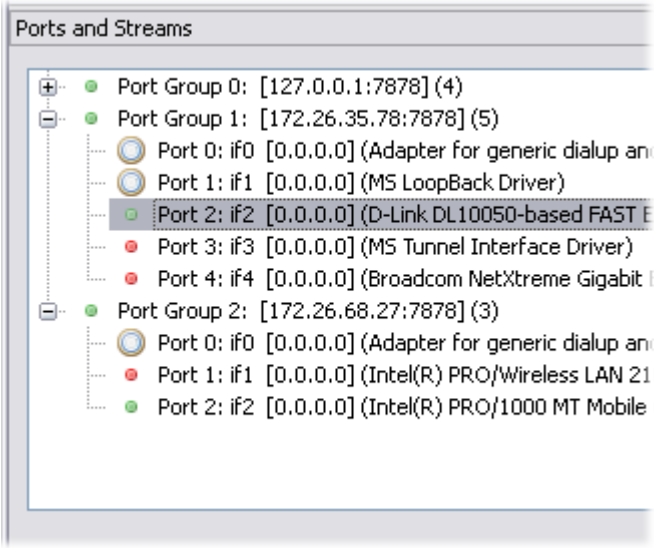

Рис. 4. Список портов

Прим.: Если доступ к порту запрещен администратором, порт может не отображаться. Если в списке нет ни одного порта, проверьте, запущен ли серверный компонент (*drone*) с правами администратора.

Действия над группами портов

Значок	Действие	Описание
	New Port Group	Добавить новый удаленный компьютер к списку и произвести соединение. Нужно указать IP-адрес и дополнительно (необязательно) номер порта.
	Delete Port Group	Удалить удаленный компьютер из списка

	Connect Port Group	Произвести попытку переподключения к удаленному компьютеру
	Disconnect Port Group	Отсоединить удаленный компьютер (он не будет удален из списка, при необходимости можно присоединить его снова)
	Exclusive Port Control	Для предотвращения использования порта операционной системой можно установить полный контроль над портом
	Port Configuration	Конфигурирование свойств порта

Контроль нескольких компьютеров

1. На удаленном компьютере, за которым вы хотите осуществлять контроль, запустите серверный компонент (*drone*).
2. В клиенте *Ostinato* выберите *File → New Port Group* и введите IP-адрес.
3. Удаленный компьютер появится как новая группа портов в списке портов.

Вы можете присоединить любое количество удаленных компьютеров.

Конфигурирование портов

Режим передачи (Transmit Mode)

Sequential Streams: потоки отправляются один за другим последовательно. Все пакеты одного потока будут отправлены после окончания передачи пакетов предшествующего потока.

Пример. Есть 2 потока: TCP и UDP. TCP поток сконфигурирован следующим образом: 100 пакетов, скорость передачи 10 пакетов/с. UDP поток сконфигурирован следующим образом: 500 пакетов, скорость передачи 5 пакетов/с. В данном режиме сначала будут отправлены 100 пакетов TCP со скоростью 10 пакетов/с, а затем — 500 пакетов UDP со скоростью 5 пакетов/с.

Interleaved Streams: потоки отправляются в зависимости от их скорости (packet/burst rate). Пакеты всех потоков будут отправлены в чередующемся режиме. Это непрерывный режим — вы можете указать скорость передачи (packet/burst rate), но не количество пакетов.

Пример. Есть 2 потока: TCP и UDP. TCP поток сконфигурирован следующим образом: скорость передачи 10 пакетов/с. UDP поток сконфигурирован следующим образом: скорость передачи 5 пакетов/с. В данном режиме за секунду будут отправлены 15 пакетов, из которых 10 пакетов — пакеты TCP, а 5 — UDP.

Создание, редактирование и удаление потоков

Чтобы создать поток, сначала выберите соответствующий порт в списке портов, далее — *File → New Stream* (или правой кнопкой в контекстном меню).

Для того чтобы вставить поток между двумя существующими потоками, выберите нижний поток и затем создайте новый (он будет создан перед выделенным). Дважды щелкните на ячейке *Name* и присвойте потоку нужное имя. Поток можно запретить/разрешить, сняв/поставив галочку. Столбец *Goto* позволяет задать способ передачи потоков: по умолчанию *Next* — после завершения передачи потока генератор *Ostinato* переходит к отправке следующего по списку.

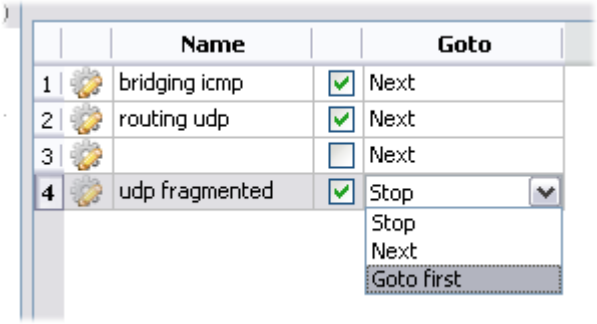

Рис. 5. Список потоков

Для удаления потока выберите поток, затем *File → Delete Stream* (или правой кнопкой в контекстном меню).

Открытие, сохранение потоков

Чтобы открыть файл, содержащий пакеты, выберите соответствующий порт в списке портов, затем *File → Open Streams* (или правой кнопкой в контекстном меню). Чтобы сохранить сконфигурированные пакеты, выберите соответствующий порт в списке портов, затем *File → Save Streams* (или правой кнопкой в контекстном меню). Форматы файлов: PCAP, PDML, собственный формат[3].

Конфигурирование потоков

Выберите *File → Edit Stream:*

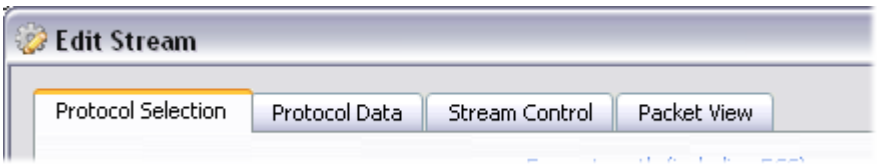

Рис. 6. Окно редактирования потока

[3] Binary format using Google Protocol Buffers encoding. A filename for a Ostinato file does not have a special "extension" such as .ost (although a user may use one if he desires). For identification as an Ostinato file, a fixed size magic field is used.

Выбор протокола

Длина кадра

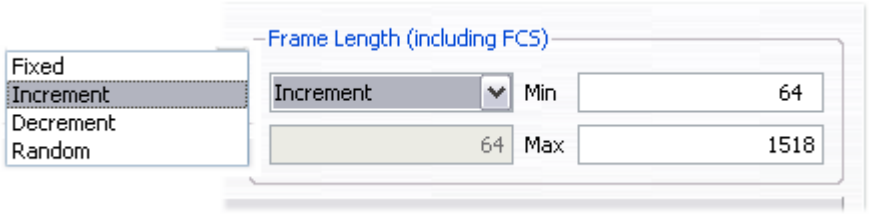

Рис. 7. Фрагмент окна редактирования потока: выбор длины кадра

Вы можете установить фиксированное значение *(fixed)* длины кадра или одно из трех других: инкрементированное *(incrementing)*, декрементированное *(decrementing)*, случайное *(random)*.

Прим.: для нефиксированных значений следует конфигурировать поток из нескольких пакетов, иначе разница в длине кадра не будет заметна.

Прим.: значение длины кадра включает в себя 4 байта FCS.

Протоколы (простой режим)

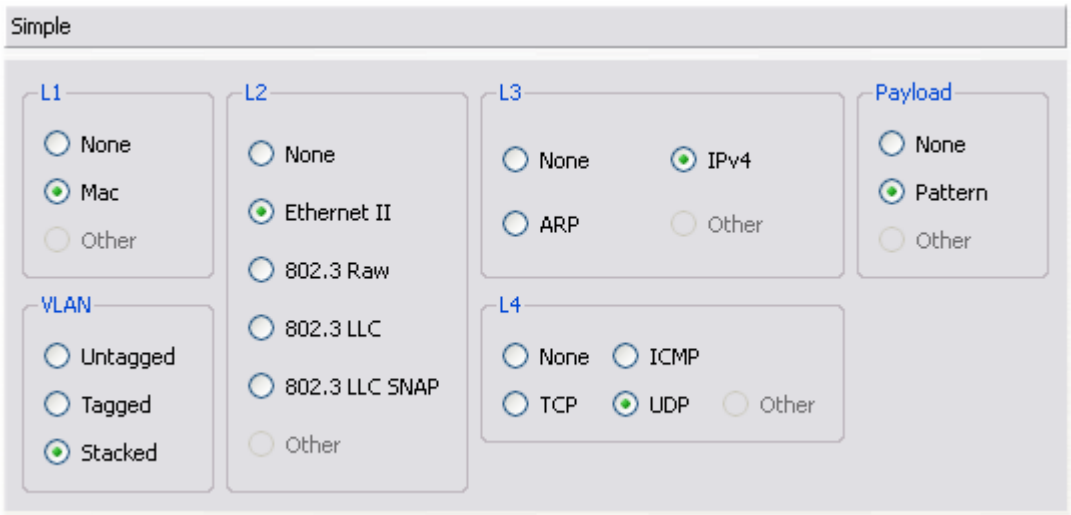

Рис. 8. Фрагмент окна редактирования потока: выбор протокола (простой режим)

Выбор из стандартных комбинаций различных протоколов осуществляется с помощью переключателей.

Для нестандартных комбинаций следует выбрать расширенный режим *(advanced mode)*.

Протоколы (расширенный режим)

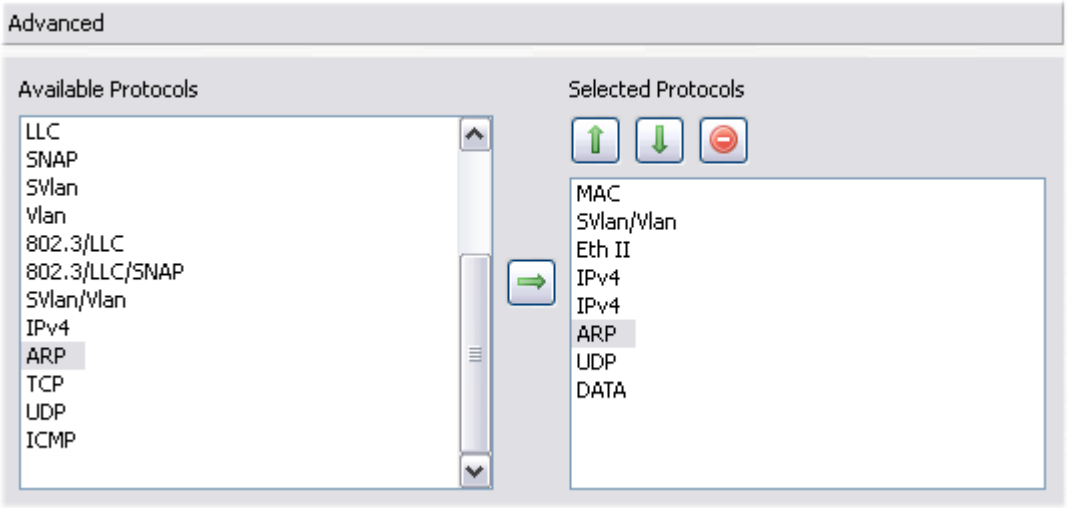

Рис. 9. Фрагмент окна редактирования потока: выбор протокола (расширенный режим)

В данном режиме протоколы можно «собирать» в любом порядке (например, TCP после ARP; IP над IP).

Слева на рис. 9 отображены все доступные протоколы, справа — выбранные из списка доступных.

	Добавить выбранный(ые) протокол(ы) из левого списка в правый
	Переместить выбранный протокол вниз
	Переместить выбранный протокол вверх
	Удалить выбранный протокол из правого списка

Поля протокола

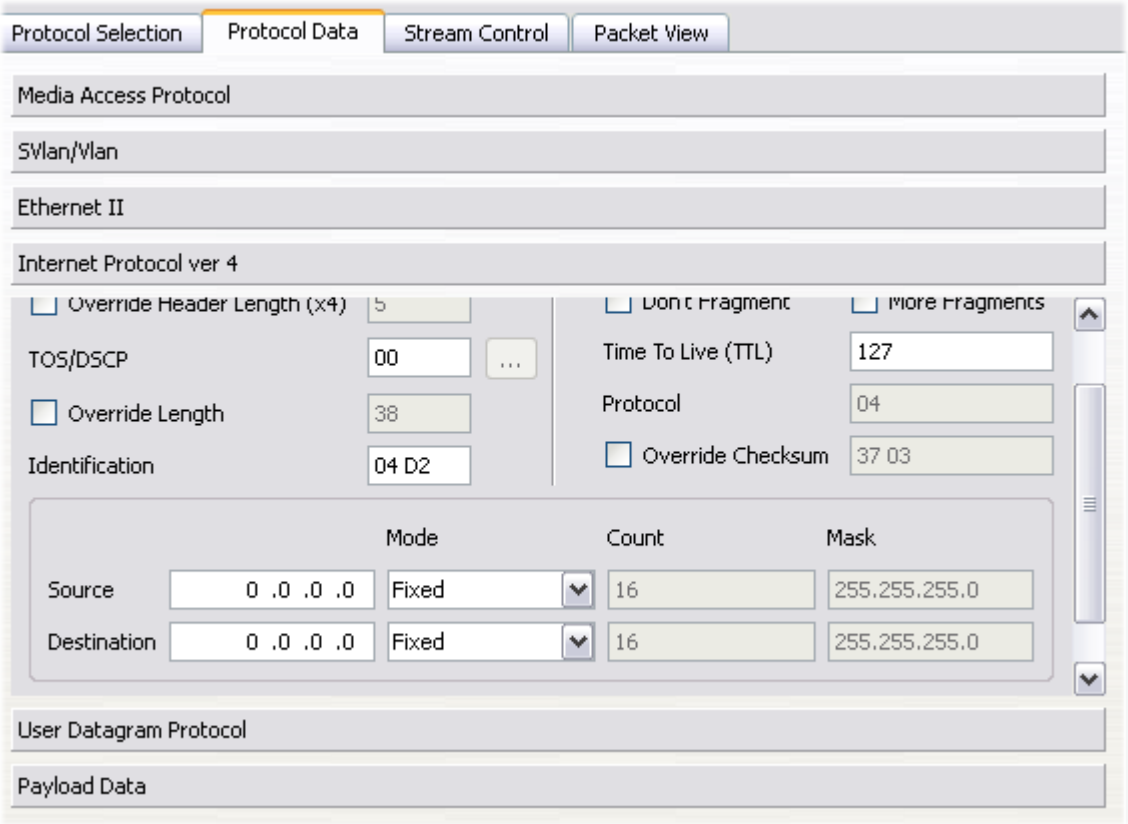

Рис. 10. Фрагмент окна редактирования потока: вкладка «Protocol Data»

Конфигурируйте поля каждого протокола.

Прим.: поля *Protocol Id* для поддерживаемых протоколов не редактируются (например, если после Ethernet идет IP, будет установлено значение 0x0800 без возможности его изменения).

Управление потоками

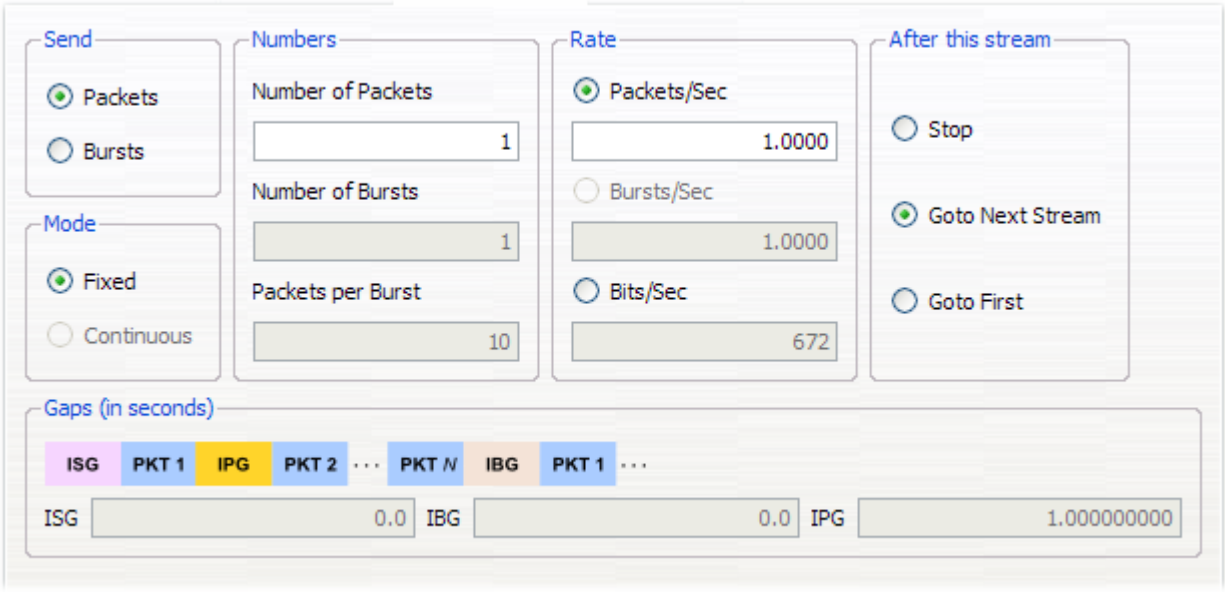

Рис. 11. Фрагмент окна редактирования потока: вкладка «Stream Control»

Варианты отправки:

1) отправлять пакеты (packets) — можно задавать их количество и скорость отправки (pkts/sec);
2) отправлять группы пакетов (bursts) — можно задавать их количество и скорость отправки (bursts/sec), дополнительно: количество пакетов в группе.

Также можно задать порядок передачи: *goto the next stream* (перейти к следующему в списке потоку), *goto first* (перейти к первому потоку в списке), *stop* (остановить передачу).

Прим.: в зависимости от режима отправки некоторые поля могут быть недоступны.

Важно! Генератор *Ostinato* не гарантирует отправку пакетов с заданной скоростью. Фактическая скорость зависит от компьютера (например, от его загрузки), на котором запущен серверный компонент (*drone*).

Просмотр пакета

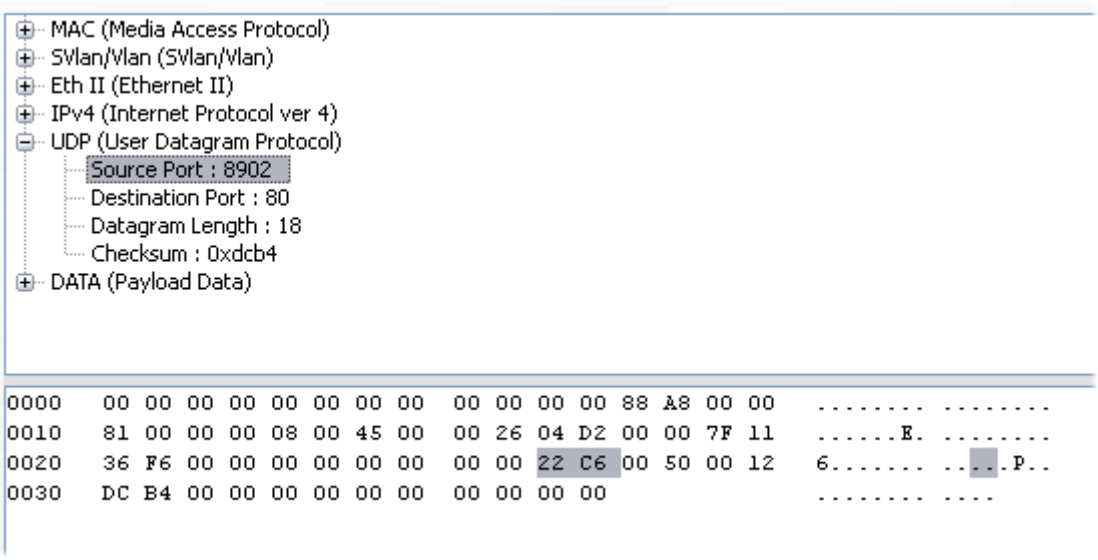

Рис. 12. Фрагмент окна редактирования потока: вкладка «Packet View»

Здесь полностью представлен сконфигурированный пакет: в виде дерева и в 16-чной форме.

Окно статистики

Все кнопки, расположенные в этом окне (кроме *Clear All Stats*), применимы к выбранному(ым) порту(ам) в самом окне (не в списке портов).

Порт выбран, если выделен весь столбец целиком, а не его часть.

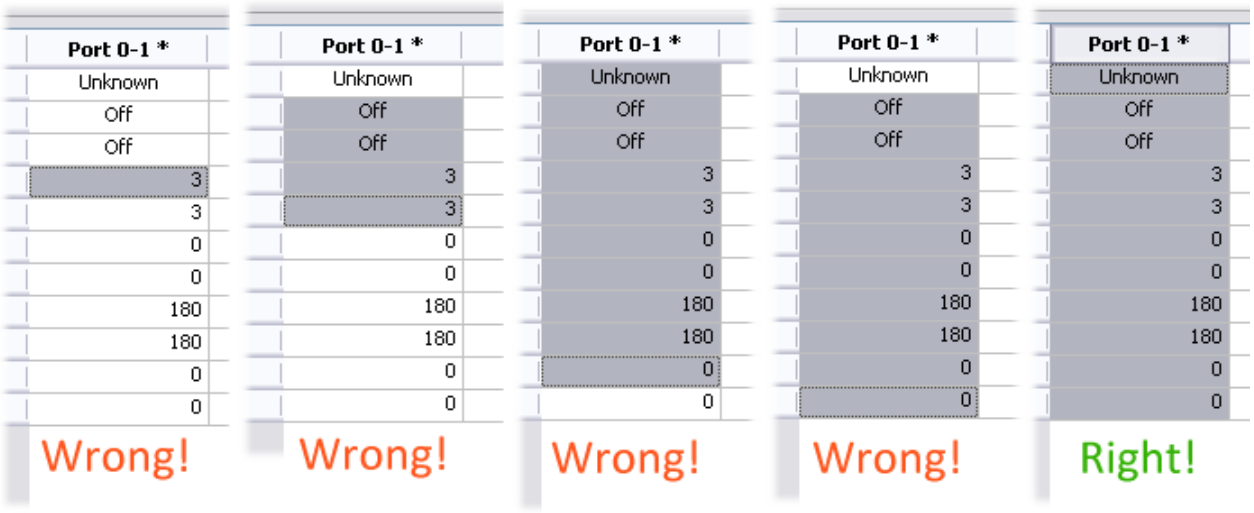

Рис. 13. Окно статистики

Действия

Значок	Действие	Описание
	Start Transmit	Начать передачу пакетов на выбранный(ые) порт(ы)
	Stop Transmit	Остановить передачу пакетов на выбранный(ые) порт(ы)
	Clear Stats	Очистить статистику выбранного(ых) порта(ов)
	Clear All Stats	Очистить статистику всех портов
	Start Capture	Начать захват пакетов с выбранного(ых) порта(ов)
	Stop Capture	Остановить захват пакетов с выбранного(ых) порта(ов)
	Configure View	Выбрать очередность отображения порта(ов) в окне статистики

Вариант А

Генерировать два потока пакетов в соответствии с таблицей 1. Цифра обозначает номер варианта. Например, для 1-го варианта: один поток ARP, второй Ethernet, т.к. цифра «1» находится на пересечении строки ARP и столбца Ethernet.

Таблица 1

	ARP	**Ethernet**	**ICMP**	**IP**	**TCP**	**UDP**
ARP		1	2	3	4	5
Ethernet			6	7	8	9
ICMP				10	11	12
IP					13	14
TCP						15
UDP						

Использовать два режима передачи:

1) *Sequential Streams* (см. в описании программы *Ostinato*);

2) *Interleaved Streams* (см. в описании программы *Ostinato*).

Таблица 2

Параметры						
Размер пакетов	Скорость передачи	Адреса отправителя, назначения	Порт источника, назначения	MAC-адрес	Фрагмен-тация	Количество пакетов
Любой	Любая	Фиксированные	В соответствии с протоколом	Фиксированный	Рассмотреть два варианта: без фрагментации и с фрагментацией	> 2

Вариант Б

Генерировать тот же тип пакетов, что и в первой части работы. Можно генерировать несколько потоков пакетов.

Использовать два режима передачи:

1) *Sequential Streams* (см. в описании программы *Ostinato*);

2) *Interleaved Streams* (см. в описании программы *Ostinato*).

Таблица 2

Параметры						
Размер пакетов	Скорость передачи	Адреса отправителя, назначения	Порт источника, назначения	MAC-адрес	Фрагментация	Количество пакетов
Любой	Любая	Фиксированные	В соответствии с протоколом	Фиксированный	Рассмотреть два варианта: без фрагментации и с фрагментацией	> 2

В отчете привести структуру генерируемого пакета и параметры генерации. Убедиться в том, что передача пакетов действительно происходит, можно с помощью *Wireshark.*