Лабораторная работа. Анализ кадров Ethernet с помощью программы Wireshark

1. Топология



1. Задачи

Часть 1. Изучение полей заголовков в кадре Ethernet II

Часть 2. Захват и анализ кадров Ethernet с помощью программы Wireshark

1. Общие сведения/сценарий

При взаимодействии протоколов верхнего уровня данные проходят уровни модели взаимодействия открытых систем (OSI) и инкапсулируются в кадре уровня 2. Структура кадра зависит от типа доступа к среде передачи данных. Например, если в качестве протоколов верхнего уровня используются TCP и IP, а тип доступа к среде передачи — Ethernet, то инкапсуляция кадров уровня 2 происходит через Ethernet II. Это типично для среды локальных сетей.

При изучении концепций уровня 2 будет полезно проанализировать данные заголовков кадров. В первой части этой лабораторной работы вы сможете посмотреть поля в кадре Ethernet II. Во второй части вам предстоит захватить и проанализировать поля заголовков кадра Ethernet II для локального и удаленного трафика с помощью программы Wireshark.

1. Необходимые ресурсы

* Один ПК (под управлением Windows 7, 8 или 10 с доступом к Интернету и установленной программой Wireshark)

1. Изучение полей заголовков в кадре Ethernet II

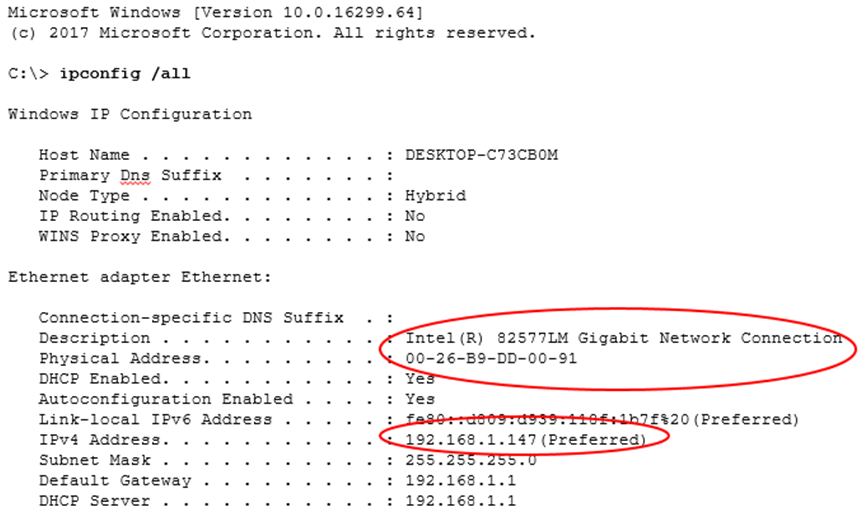
В части 1 вы изучите поля и содержание заголовков в кадре Ethernet II. Для этого будет использован захват данных программой Wireshark.

* 1. Просмотрите длины и описания полей заголовков Ethernet II.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Преамбула | Адрес назначения | Адрес источника | Тип кадра | Данные | FCS |
| 8 байт | 6 байт | 6 байт | 2 байта | от 46 до 1500 байт | 4 байта |

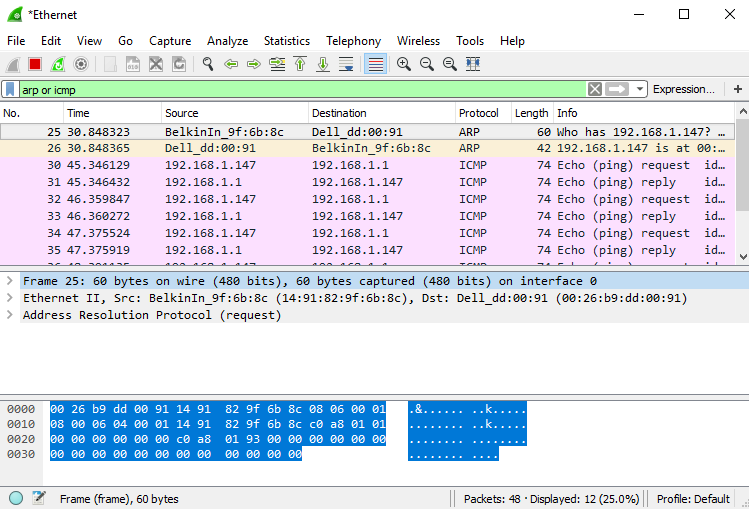
* 1. Изучите конфигурацию сети ПК.

IP-адрес узла ПК — 192.168.1.147, IP-адрес шлюза по умолчанию — 192.168.1.1.



* 1. Изучите кадры Ethernet в данных, захваченных программой Wireshark.

Показанный ниже результат захвата данных в программе Wireshark отображает пакеты, которые были сгенерированы с помощью команды ping, отправленной с узла ПК на шлюз по умолчанию. В программе Wireshark включен фильтр для просмотра только ARP- и ICMP-протоколов. Сеанс начинается с ARP-запроса МАС-адреса маршрутизатора шлюза, за которым следуют четыре эхо-запроса и ответа.



* 1. Изучите содержание заголовков Ethernet II в ARP-запросе.

В приведенной ниже таблице выбран первый кадр из данных, захваченных программой Wireshark, и отображаются данные в полях заголовков Ethernet II.

|  |  |  |
| --- | --- | --- |
| Поле | Значение | Описание |
| Преамбула | Не показано в захвате данных | В этом поле содержатся синхронизированные биты, обработанные сетевой платой. |
| Адрес назначения | Широковещательная рассылка (ff:ff:ff:ff:ff:ff) | Адреса уровня 2 для кадра. Длина каждого адреса составляет 48 бит или 6 октетов, выраженных 12 шестнадцатеричными цифрами: 0-9,A-F. Общий формат — 12:34:56:78:9A:BC.  Первые шесть шестнадцатеричных чисел обозначают производителя сетевой платы, а последние — ее серийный номер.  Адрес назначения может быть адресом широковещательной рассылки (состоящим только из единиц) или одноадресной рассылки. Адрес источника всегда является адресом одноадресной рассылки. |
| Адрес источника | BelkinIn\_9f:6b:8c (14:91:82:9f:6b:8c) |
| Тип кадра | 0x0806 | В кадрах Ethernet II это поле содержит шестнадцатеричное значение, которое используется для указания типа протокола верхнего уровня в поле данных. Ethernet II поддерживает множество протоколов верхнего уровня. Наиболее распространены следующие два типа кадров.  Значение Описание  0x0800 Протокол IPv4  0x0806 Протокол разрешения адресов (ARP) |
| Данные | Протокол разрешения адресов (ARP) | Содержит инкапсулированный протокол верхнего уровня. Поле данных в диапазоне от 46 до 1500 байт. |
| FCS | Не показано в захвате данных | Контрольная последовательность кадра (FCS), используемая сетевой платой для выявления ошибок при передаче данных. Значение вычисляется компьютером отправителя, включает адреса, тип и поле данных кадра и проверяется получателем. |

Какова особенность содержания поля адреса назначения?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Почему перед первым эхо-запросом ПК отправляет широковещательную рассылку ARP?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Назовите MAC-адрес источника в первом кадре. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Назовите идентификатор поставщика (OUI) сетевой интерфейсной платы (NIC) источника. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Какая часть МАС-адреса соответствует OUI?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Назовите серийный номер сетевой интерфейсной платы (NIC) источника. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Захват и анализ кадров Ethernet с помощью программы Wireshark

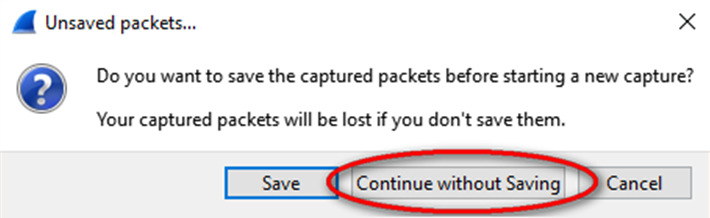
В части 2 вы воспользуетесь программой Wireshark для захвата локальных и удаленных кадров Ethernet. Затем вы изучите сведения, содержащиеся в полях заголовков кадров.

* 1. Определите IP-адрес шлюза по умолчанию на своем ПК.

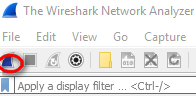
Откройте окно командной строки и введите **ipconfig** .

Назовите IP-адрес шлюза ПК по умолчанию. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

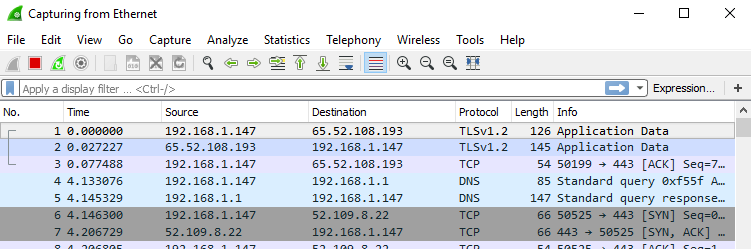
* 1. Начните захват трафика на сетевой интерфейсной плате своего ПК.
     1. Закройте программу Wireshark. Не нужно сохранять собранные данные.



* + 1. Откройте программу Wireshark и начните захват данных.



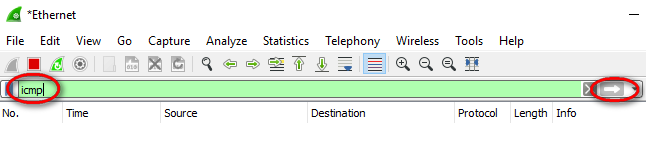
* + 1. Понаблюдайте за трафиком в окне списка пакетов.



* 1. С помощью фильтров программы Wireshark отобразите на экране только трафик ICMP.

Чтобы скрыть ненужный трафик, установите соответствующий фильтр Wireshark. Фильтр не блокирует захват ненужных данных, а лишь отбирает то, что нужно показывать на экране. На данный момент разрешено отображение только трафика ICMP.

В поле **Filter** (Фильтр) программы Wireshark введите **icmp**. При правильной настройке фильтра поле должно стать зеленым. Если поле стало зеленым, нажмите кнопку **Apply** (Применить) (кнопка со стрелкой вправо), чтобы применить фильтр.

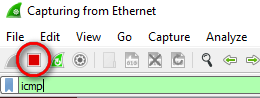


* 1. Из окна командной строки отправьте эхо-запрос на шлюз ПК по умолчанию.

Из окна командной строки отправьте эхо-запрос на шлюз по умолчанию, используя IP-адрес, записанный в шаге 1.

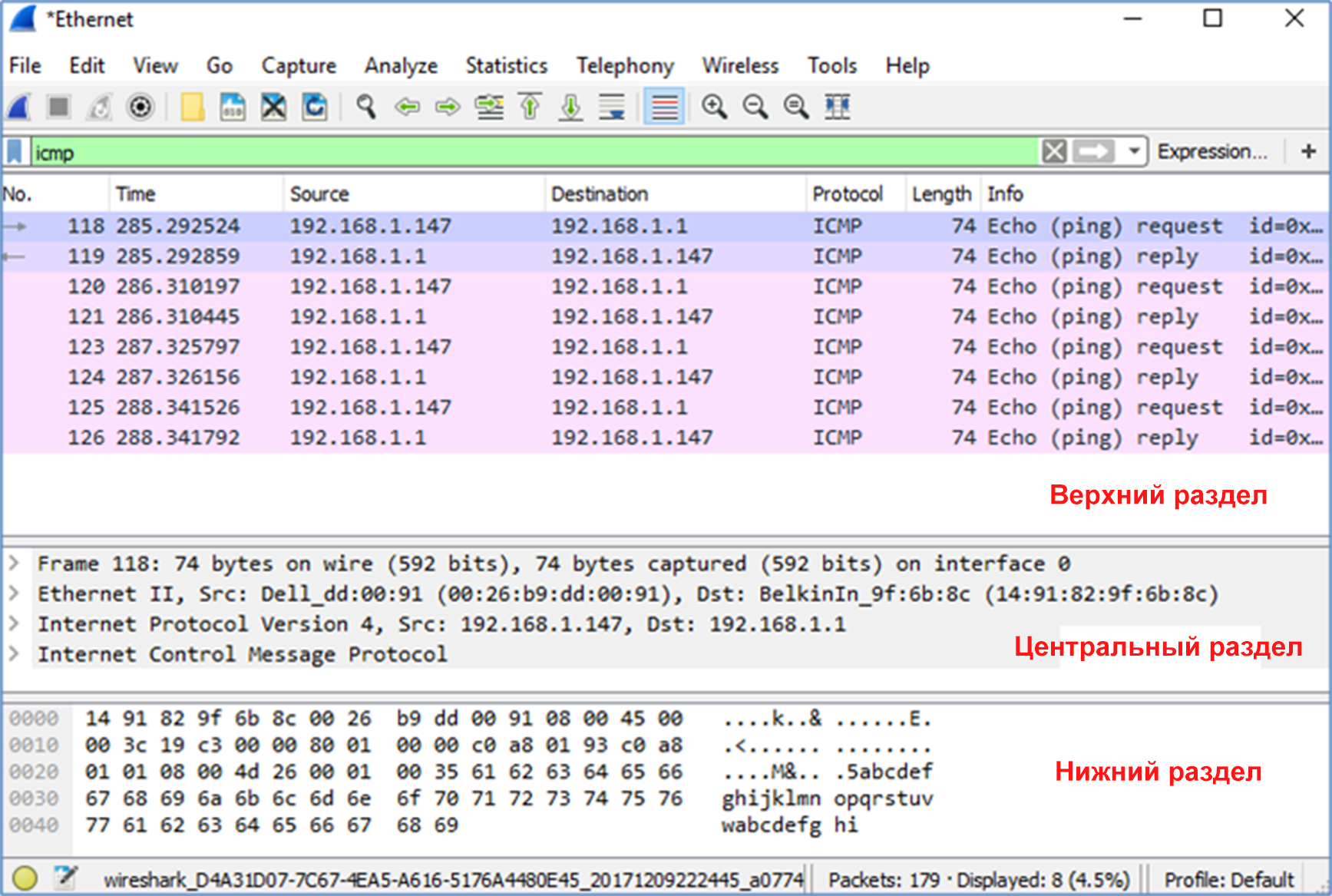
* 1. Остановите захват трафика на сетевой плате.

Нажмите значок **Stop Capture** (Остановить захват), чтобы остановить захват трафика.



* 1. Изучите первый эхо-запрос в программе Wireshark.

Главное окно программы Wireshark состоит из трех разделов: панель списка пакетов (вверху), панель **Packet Details** (Сведения о пакете) (посередине) и панель **Packet Bytes** (Последовательность байтов пакета) (внизу). Если вы правильно выбрали интерфейс для захвата пакетов на шаге 3, программа Wireshark отобразит данные протокола ICMP на панели списка пакетов, как показано в приведенном ниже примере.



* + 1. На панели списка пакетов (верхний раздел) выберите первый указанный кадр. В столбце **Info** (Информация) появится значение **Echo (ping) request** (Эхо-запрос с помощью команды ping). Строка станет синей.
    2. Изучите первую строку на панели сведений о пакете в средней части экрана. В этой строке указывается длина кадра (в данном примере — 74 байта).
    3. Вторая строка на панели сведений о пакете показывает, что это кадр Ethernet II. Также отображаются MAC-адреса источника и назначения.

Назовите MAC-адрес сетевой интерфейсной платы этого ПК. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Назовите MAC-адрес шлюза по умолчанию. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Чтобы получить больше информации о кадре Ethernet II, нажмите на значок плюса («+») в начале второй строки. Обратите внимание на то, что значок плюса при этом изменится на значок минуса («-»).

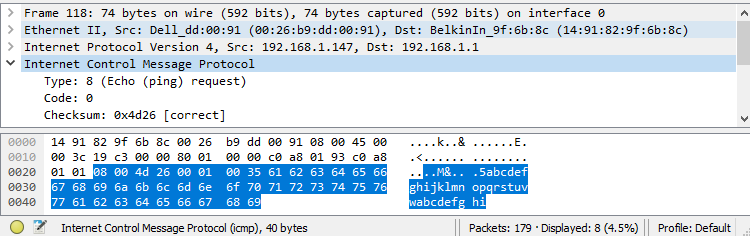
Назовите отображающийся тип кадра. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Последние две строки среднего раздела содержат информацию о поле данных кадра. Обратите внимание на то, что данные содержат IPv4-адреса источника и назначения.

Назовите IP-адрес источника. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Назовите IP-адрес назначения. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Для того чтобы выделить эту часть кадра (в шестнадцатеричной системе и в кодировке ASCII) на панели **Packet Bytes** (Последовательность байтов пакета) (нижний раздел), щелкните по любой строке в среднем разделе. Щелкните по строке **Internet Control Message Protocol** (Протокол ICMP) в среднем разделе и посмотрите, что будет выделено на панели **Packet Bytes** (Последовательность байтов пакета).



Какое слово образуют последние два выделенных октета? \_\_\_\_\_\_

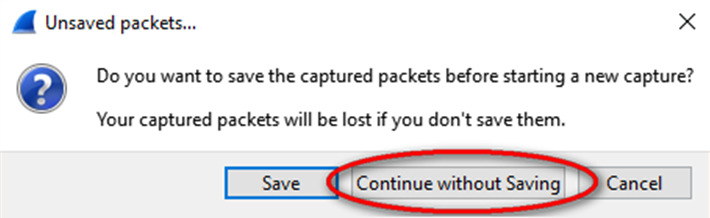
* + 1. Нажмите на следующий кадр в верхнем разделе и изучите кадр эхо-ответа. Обратите внимание на то, что МАС-адреса источника и назначения поменялись местами, поскольку маршрутизатор, который служит шлюзом по умолчанию, отправил этот кадр в ответ на первый эхо-запрос.

Какое устройство и MAC-адрес отображаются в качестве адреса назначения?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Перезапустите захват пакетов в программе Wireshark.

Нажмите значок **Start Capture** (Начать захват), чтобы начать новый захват данных в программе Wireshark. Откроется всплывающее окно с предложением сохранить предыдущие захваченные пакеты в файл перед началом нового захвата. Нажмите **Continue without Saving** (Продолжить без сохранения).



* 1. Через окно командной строки отправьте эхо-запрос на веб-сайт [www.cisco.com](http://www.cisco.com).
  2. Остановите захват пакетов.
  3. Изучите новые данные на панели packet list (список пакетов) в программе Wireshark.

Назовите МАС-адреса источника и назначения в первом кадре эхо-запроса.

**Источник**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Назначение**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Назовите IP-адреса источника и назначения в поле данных кадра.

**Источник**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Назначение**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Сравните эти адреса с адресами, полученными в шаге 6. Изменился только IP-адрес назначения. Почему IP-адрес назначения изменился, а MAC-адрес назначения остался прежним?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Вопросы для повторения

Программа Wireshark не отображает поле преамбулы заголовка кадра. Что содержит преамбула?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_