Лабораторная работа: изучение кадров Ethernet с помощью программы Wireshark

Топология

Задачи

Часть 1. Изучение полей заголовков в кадре Ethernet II

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

Исходные данные/сценарий

При взаимодействии протоколов верхнего уровня данные проходят уровни взаимодействия открытых систем (OSI) и инкапсулируются в кадры 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 локальной среды.

При изучении концепций уровня 2 полезно анализировать 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 удалённого трафика с помощью программы Wireshark.

Необходимые ресурсы

- Один ПК (Windows 7, Vista или XP с выходом в Интернет и установленной программой Wireshark)

Часть 1: Изучение полей заголовков в кадре Ethernet II

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

Шаг 1: Просмотрите длины и описания полей заголовков Ethernet II.

Преамбула	Адрес назначения	Адрес источника	Тип кадра	Данные	Контрольная последовательность кадра (Frame Check Sequence-FCS)
8 байт	6 байт	6 байт	2 байта	от 46 до 1500 байт	4 байта

Шаг 2: Изучите конфигурацию сети ПК.

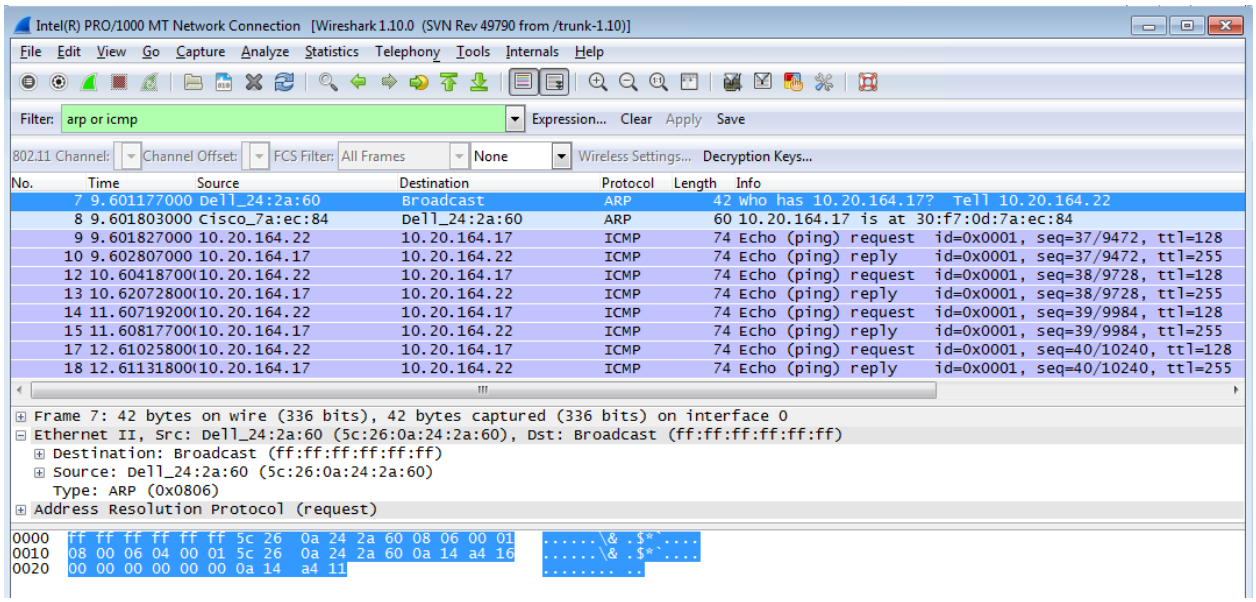
IP-адрес узла ПК — 10.20.164.22, IP-адрес шлюза по умолчанию — 10.20.164.17.

```
Ethernet adapter Подключение по локальной сети:

   DNS-суффикс подключения . . . . . : cisco.com
   Локальный IPv6-адрес канала . . . : fe80::b875:731b:3c7b:c0b1%10
   IPv4-адрес. . . . . . . . . . . . : 10.20.164.22
   Маска подсети . . . . . . . . . . : 255.255.255.240
   Основной шлюз. . . . . . . . . . : 10.20.164.17
```

Шаг 3: Изучите кадры Ethernet в данных, захваченных программой Wireshark.

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



Шаг 4: Изучите содержание заголовков Ethernet II в ARP-запросе.

В приведённой 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 аппаратным обеспечением сетевого адаптера.
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 номеров обозначают производителя сетевого адаптера, а последние — серийный номер устройства. Адрес назначения может быть широковещательным (состоящим только из единиц), либо индивидуальным. Адрес источника всегда индивидуальный.
Адрес источника	Dell_24:2a:60 (5c:26:0a:24:2a:60)	
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	ARP	Содержит инкапсулированный протокол верхнего уровня. Поле данных в диапазоне от 46 до 1500 байт.
Контрольная последовательность кадра (Frame Check Sequence-FCS)	Не показано в захвате данных	Контрольная последовательность кадра, используемая сетевым адаптером 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 с помощью команды ping ПК отправляет широковещательную рассылку ARP?

Назовите MAC-адрес источника в первом кадре.

Назовите идентификатор производителя (OUI) сетевого адаптера источника.

Какая часть MAC-адреса соответствует OUI?

Назовите серийный номер сетевого адаптера источника.

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

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

Шаг 1: Определите IP-адрес шлюза по умолчанию на своём ПК.

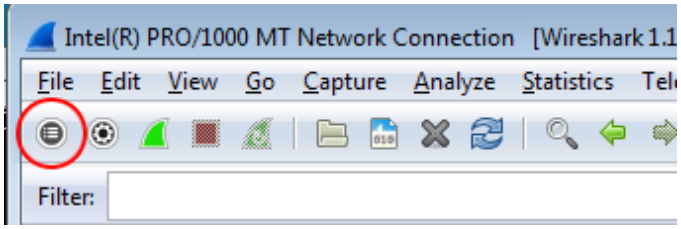
Откройте окно командной строки и введите**ipconfig**.

Назовите IP-адрес шлюза ПК по умолчанию.

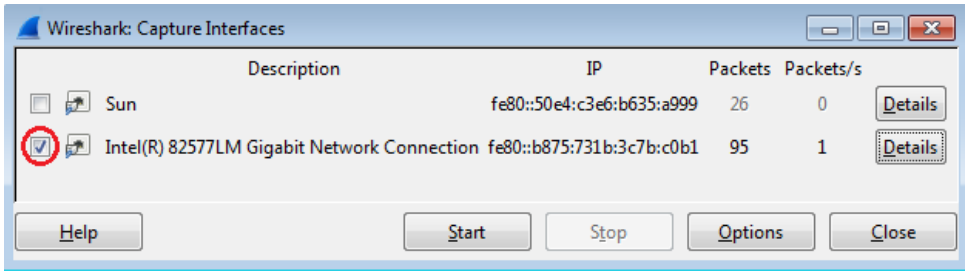
Шаг 2: Начните захват трафика на сетевом адаптере своего ПК.

a. Откройте Wireshark.

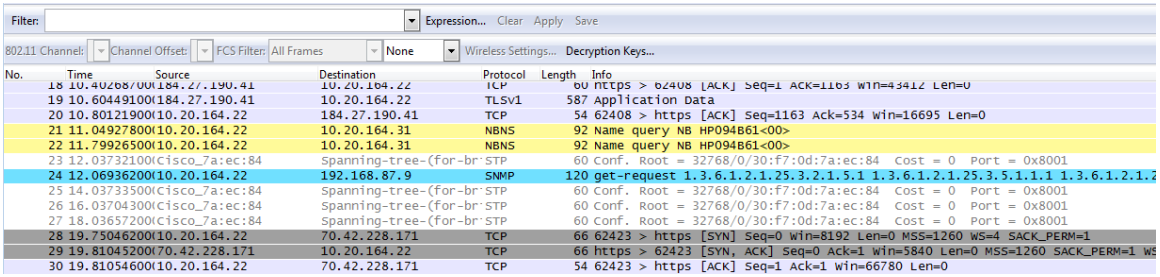
b. На панели инструментов анализатора сети Wireshark нажмите на значок **Interface List** (Список интерфейсов).



c. В окне Wireshark: Capture Interfaces (Захват интерфейсов) выберите интерфейс, в котором нужно начать захват трафика, установив соответствующий флажок, и нажмите кнопку **Start** (Пуск). Если вы не знаете, какой интерфейс выбрать, нажмите кнопку **Details** (Сведения), чтобы открыть подробную информацию о каждом из указанных интерфейсов.



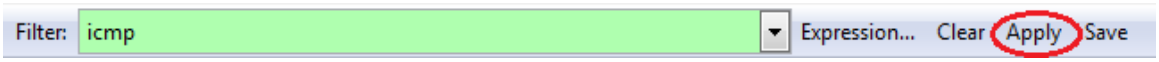
d. Понаблюдайте за трафиком в окне списка пакетов (Packet List).



Шаг 3: 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 ICMP-трафика.

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

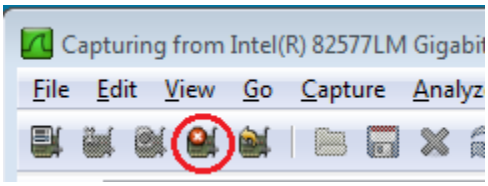


Шаг 4: Из окна командной строки отправьте эхо-запрос с помощью команды ping на шлюз ПК по умолчанию.

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

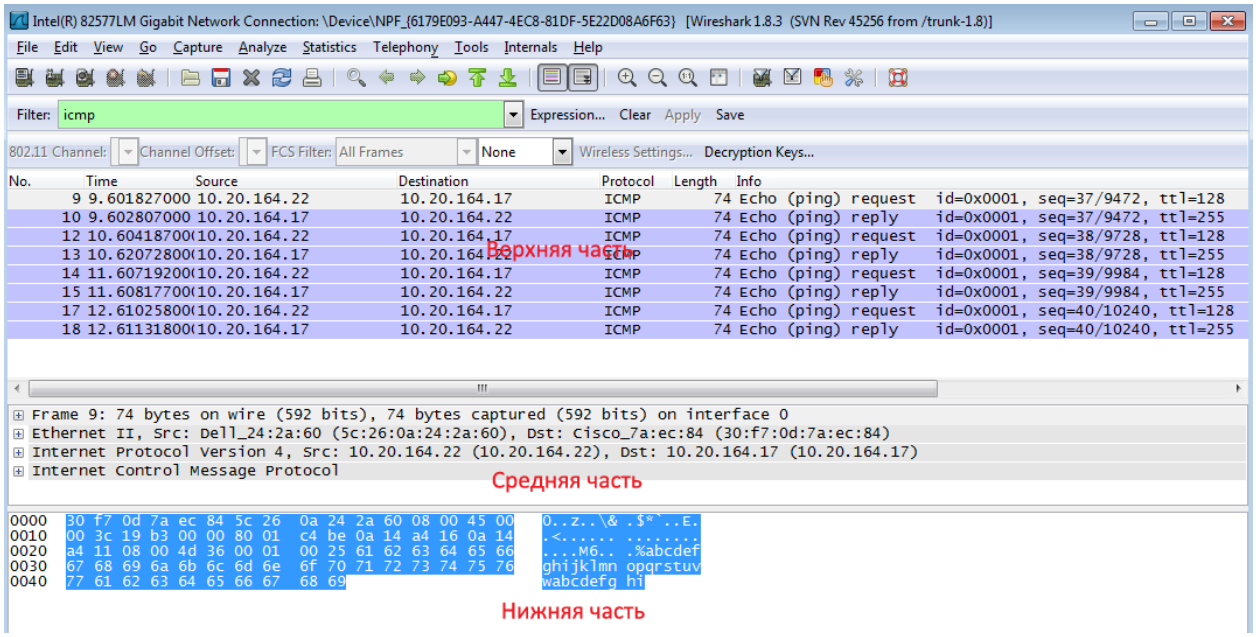
Шаг 5: Остановите захват трафика на сетевом адаптере.

Чтобы остановить захват трафика, нажмите на значок **Stop Capture** (Остановить захват).



Шаг 6: Изучите первый эхо-запрос с помощью команды ping в программе Wireshark.

Главное окно программы Wireshark состоит из трёх разделов: панель списка пакетов (вверху), панель сведений о пакете (посередине) и панель отображения пакета в виде последовательности байтов (внизу). Если вы правильно выбрали интерфейс для захвата пакетов в шаге 3, программа Wireshark отобразит данные протокола ICMP на панели списка пакетов, как показано в приведённом ниже примере.



a. 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.

b. Изучите первую строку в панели сведений о пакете в средней части экрана. В этой строке указывается длина кадра (в данном примере — 74 байта).

c. Вторая строка в панели Packet Details (Сведения о пакете) показывает, что это кадр Ethernet II. Также отображаются MAC-адреса источника и назначения.

   Назовите MAC-адрес сетевого адаптера этого ПК.

   Назовите MAC-адрес шлюза по умолчанию.

d. 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 («-»).

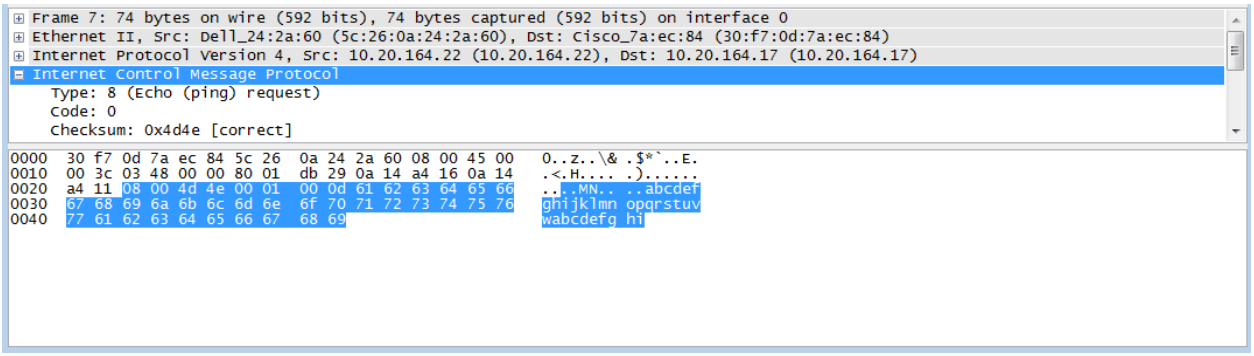
   Назовите показанный тип кадра.

e. 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.

f. Чтобы выделить эту часть кадра (в шестнадцатеричной системе и ASCII) в панели отображения пакета в виде последовательности байтов (нижний раздел) нажмите на любую строку в среднем разделе. Нажмите на строку **Internet Control Message Protocol** в среднем разделе и посмотрите, что будет выделено в панели отображения пакета в виде последовательности байтов.



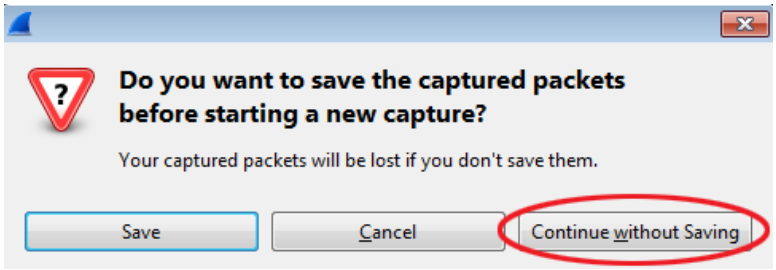
Какое слово образуют последние два выделенных октета?

g. Нажмите на следующий кадр в верхнем разделе и изучите кадр эхо-ответа. Обратите внимание на то, что MAC-адреса источника и назначения поменялись местами, поскольку маршрутизатор, который служит шлюзом по умолчанию, отправил этот кадр в ответ на первый эхо-запрос с помощью команды ping.

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

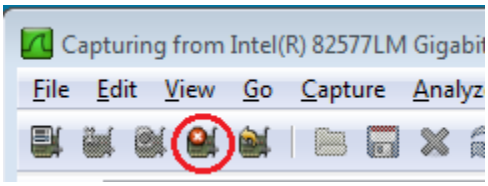
Шаг 7: Перезапустите захват пакетов в программе Wireshark.

Нажмите на 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 кнопку **Continue without Saving** (Продолжить без сохранения).



Шаг 8: Через окно командной строки отправьте эхо-запрос с помощью команды ping на веб-сайт www.cisco.com.

Шаг 9: Остановите захват пакетов.



Шаг 10: Изучите новые данные на панели списка пакетов в программе Wireshark.

Назовите MAC-адреса источника и назначения в первом кадре эхо-запроса с помощью команды ping.

Источник:

Назначение:

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

Источник:

Назначение:

Сравните эти адреса с адресами, полученными в шаге 7. Изменился только IP-адрес назначения. Почему IP-адрес назначения изменился, а MAC-адрес назначения остался прежним?

Вопросы на закрепление

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