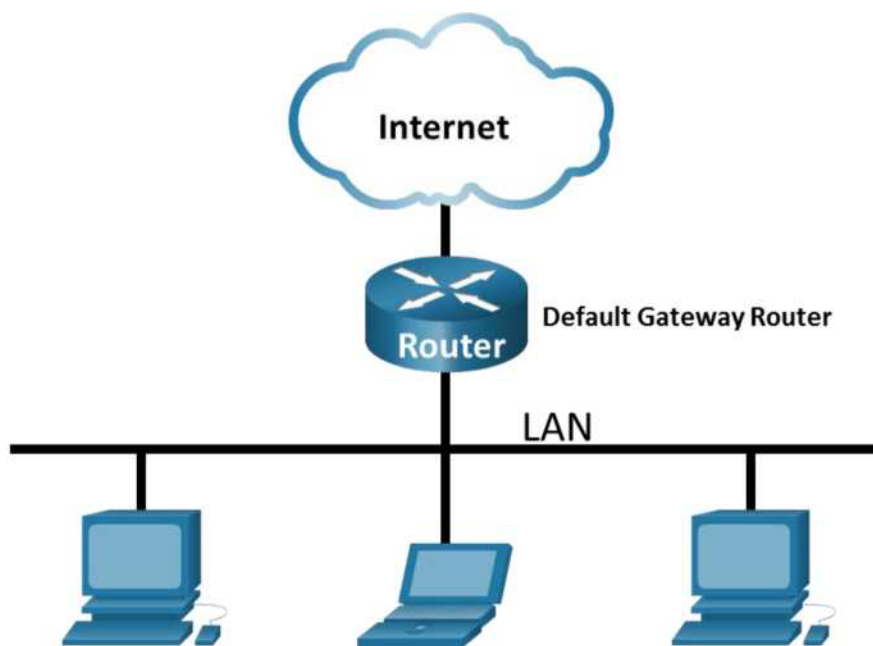


Лабораторная работа

Анализ кадров Ethernet и просмотр сетевого трафика с помощью программы Wireshark

Топология



Задачи

Часть 1. Изучение полей кадра Ethernet II

Часть 2. Захват и анализ данных протокола ICMP в локальной сети с помощью программы Wireshark

Часть 3. Захват и анализ данных протокола ICMP для удаленных узлов с помощью программы Wireshark

Общие сведения

При взаимодействии устройств по сети, данные приложений проходя уровни модели взаимодействия открытых систем (OSI), инкапсулируются в единицы данных протокола (PDU) канального уровня (кадры). Структура кадра зависит от типа среды передачи данных и метода доступа к ней. При изучении процесса функционирования канального уровня будет полезно проанализировать данные полей кадров. В первой части лабораторной работы необходимо изучить поля кадра Ethernet II. Во второй и третьей части требуется перехватить и проанализировать поля кадра Ethernet II для локального и удаленного трафика ICMP с помощью программы Wireshark.

Wireshark — это полезный инструмент для анализа трафика (анализатор кадров), который используется для поиска неполадок в сети, анализа, разработки программного обеспечения и протоколов, а также обучения. При передаче данных по среде передачи, Wireshark захватывает каждый кадр канального уровня и декодирует его содержимое согласно

документам **RFC** или другим спецификациям.

Необходимые ресурсы

- Компьютер с ОС **Windows**, доступом в Интернет и установленной программой **Wireshark**
- Дополнительный компьютер (оконечное устройство) в той же локальной сети.

Часть 1. Изучение полей в кадре Ethernet II

В этой части необходимо изучить поля кадра **Ethernet II**, перехваченного программой **Wireshark**, их размер и назначение.

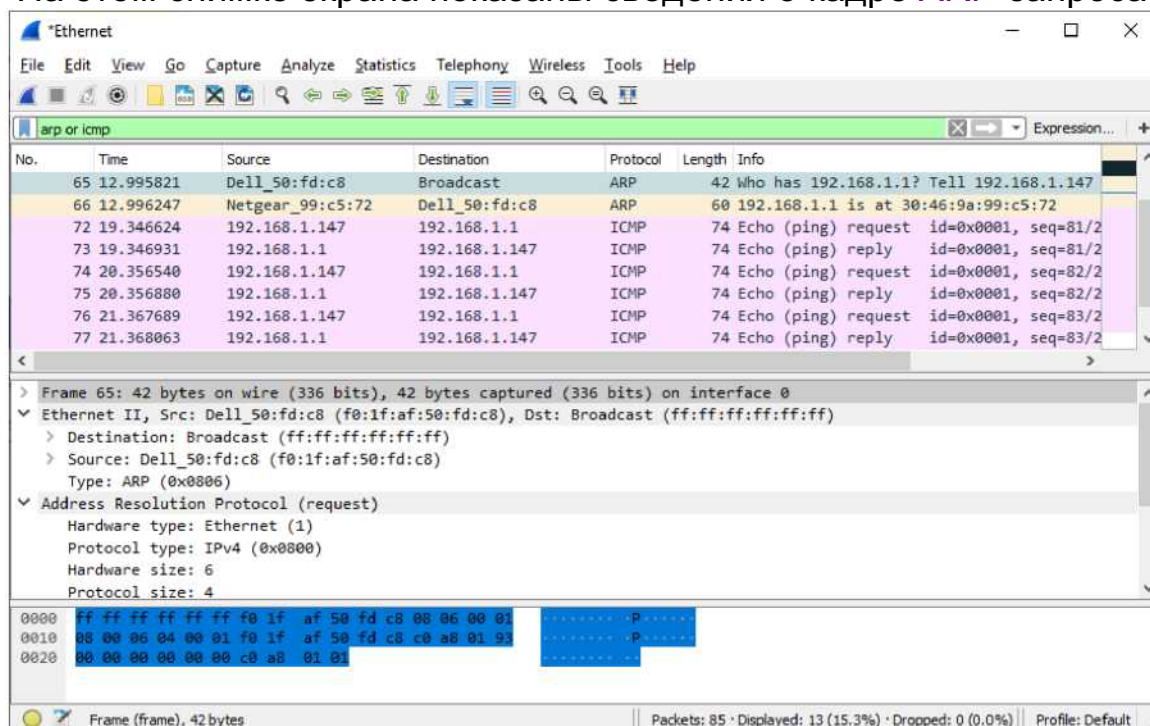
Шаг 1. Изучите размер и назначение полей кадров Ethernet II.

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

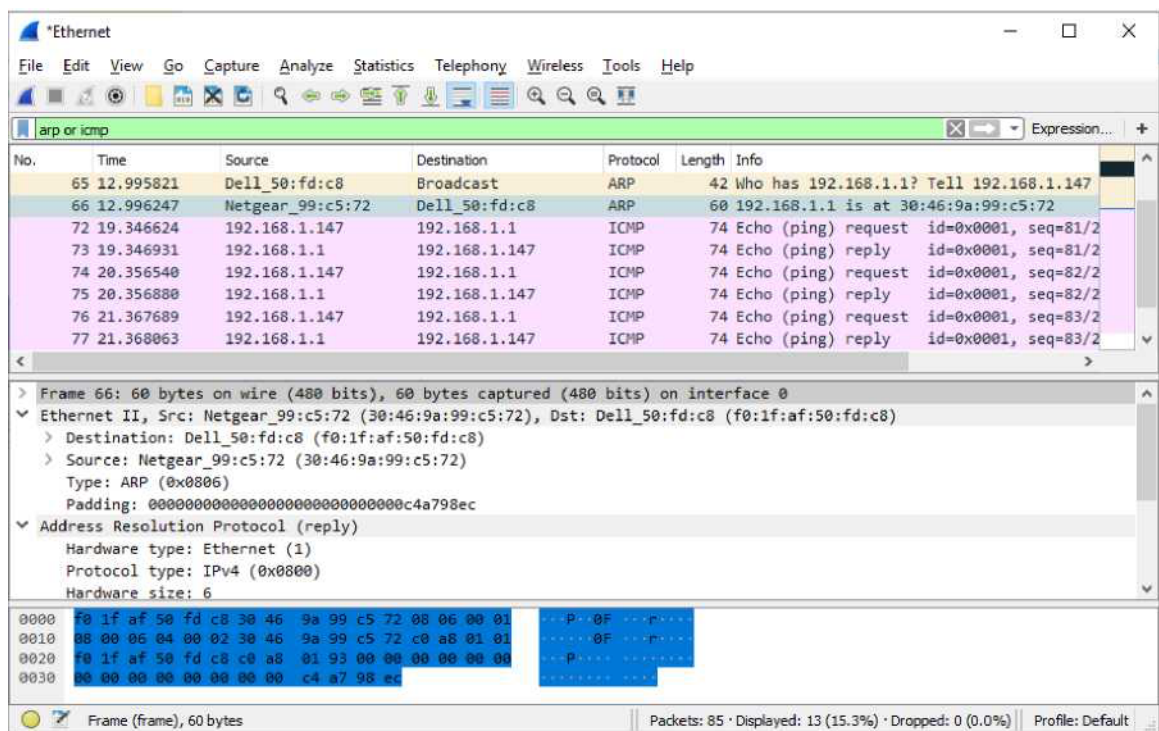
Шаг 2. Изучите кадры Ethernet, перехваченные программой Wireshark.

Приведенный ниже пример перехвата данных программой **Wireshark** отображает кадры, содержащие эхо-запросы, которые были созданы с помощью команды **ping**, и отправлены с компьютера на **основной шлюз (шлюз по умолчанию)**. В программе **Wireshark** установлен фильтр для просмотра только трафика протоколов **ARP** и **ICMP**. Протокол разрешения адресов (**ARP**), используется для сопоставления **MAC**-адреса с **IP**-адресом. Передача начинается с **ARP**-запроса **MAC**-адреса основного шлюза, за которым следуют четыре эхо-запроса и ответа.

На этом снимке экрана показаны сведения о кадре **ARP**-запроса.



На этом снимке экрана показаны сведения о кадре **ARP**-ответа.



Шаг 3. Изучите содержимое полей кадра Ethernet II.

В приведенной ниже таблице выбран кадр 65 из примера выше, перехваченный программой **Wireshark**, и приведены данные в полях этого кадра **Ethernet II**.

Поле	Значение	Описание
Преамбула	Не отображается при перехвате данных	В этом поле содержатся биты синхронизации, обработанные сетевой платой.
Адрес назначения	Адрес широковещательной рассылки (FF:FF:FF:FF:FF:FF)	Адреса канального уровня (физический адрес). Длина каждого адреса составляет 48 бит (6 октетов), представленных 12 шестнадцатеричными цифрами: 0-9, A-F. Обычный формат записи — 12:34:56:78:90:AB.
Адрес источника	Netgear_99:C5:72 (30:46:9A:99:C5:72)	Первые 6 шестнадцатеричных цифр определяют производителя сетевой платы, а последние — ее серийный номер. Адрес назначения может быть адресом широковещательной или одноадресной рассылки. Адрес источника всегда является адресом одноадресной рассылки.
Тип кадра	0x0806	Это поле содержит шестнадцатеричное значение, которое указывает данные какого протокола верхнего уровня содержатся в поле Данные кадра Ethernet II . Ethernet II поддерживает множество протоколов верхнего уровня. Наиболее распространены следующие типы кадров. Значение Описание 0x0800 IPv4 Protocol 0x0806 Address Resolution Protocol (ARP)
Данные	ARP	Содержит инкапсулированную PDU протокола верхнего уровня. Поле данных имеет размер в диапазоне от 46 до 1500 байт.

FCS	Не отображается при перехвате данных	Контрольная последовательность кадра (FCS), которая используется сетевой платой для обнаружения ошибок при передаче данных. Значение поля вычисляется устройством-отправителем и проверяется устройством-получателем.
-----	--------------------------------------	---

Что можно сказать о данных, содержащихся в поле **Адрес назначения** приведенного примера?

Почему перед первым эхо-запросом компьютер отправляет широковещательную рассылку **ARP**?

Назовите физический адрес источника в приведенном для примера кадре.

Назовите идентификатор производителя (**OUI**) сетевой интерфейсной платы источника в ответе **ARP** (кадр 66 примера)?

Какая часть физического адреса соответствует идентификатору производителя?

Назовите серийный номер сетевой интерфейсной платы (**NIC**) источника (кадр 66 примера).

Часть 2. Захват и анализ данных протокола ICMP в локальной сети с помощью программы Wireshark

В этой части лабораторной работы необходимо осуществить перехват ICMP-запросов и ответов в локальной сети с помощью программы Wireshark. Кроме этого, требуется найти и проанализировать информацию в захваченных кадрах. Этот анализ позволит понять, как используются поля кадров при передаче данных по локальной сети.

Шаг 1. Определите параметры интерфейсов своего компьютера и IP-адрес основного шлюза.

В данном шаге необходимо узнать IP-адрес компьютера, физический адрес (MAC-адрес) сетевой интерфейсной платы (NIC) и IP-адрес основного шлюза.

а. В окне командной строки ОС Windows введите команду `ipconfig /all`

чтобы узнать IP-адрес интерфейса компьютера, его описание, физический адрес, а также IP-адрес основного шлюза.

```
Физический адрес. . . . . : 84-34-97-7B-F1-39
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::a037:4716:80af:f844%19(Основной)
IPv4-адрес. . . . . : 192.168.1.147(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена. . . . . : 3 августа 2022 г. 8:42:16
Срок аренды истекает. . . . . : 7 августа 2022 г. 0:13:19
Основной шлюз. . . . . : 192.168.1.1
DHCP-сервер. . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 327431319
DUID клиента DHCPv6 . . . . . : 00-01-00-01-2A-01-21-AF-C0-25-E9-16-EA-26
DNS-серверы. . . . . : 192.168.1.1
```

Назовите IP-адрес этого компьютера.

Назовите IP-адрес основного шлюза.

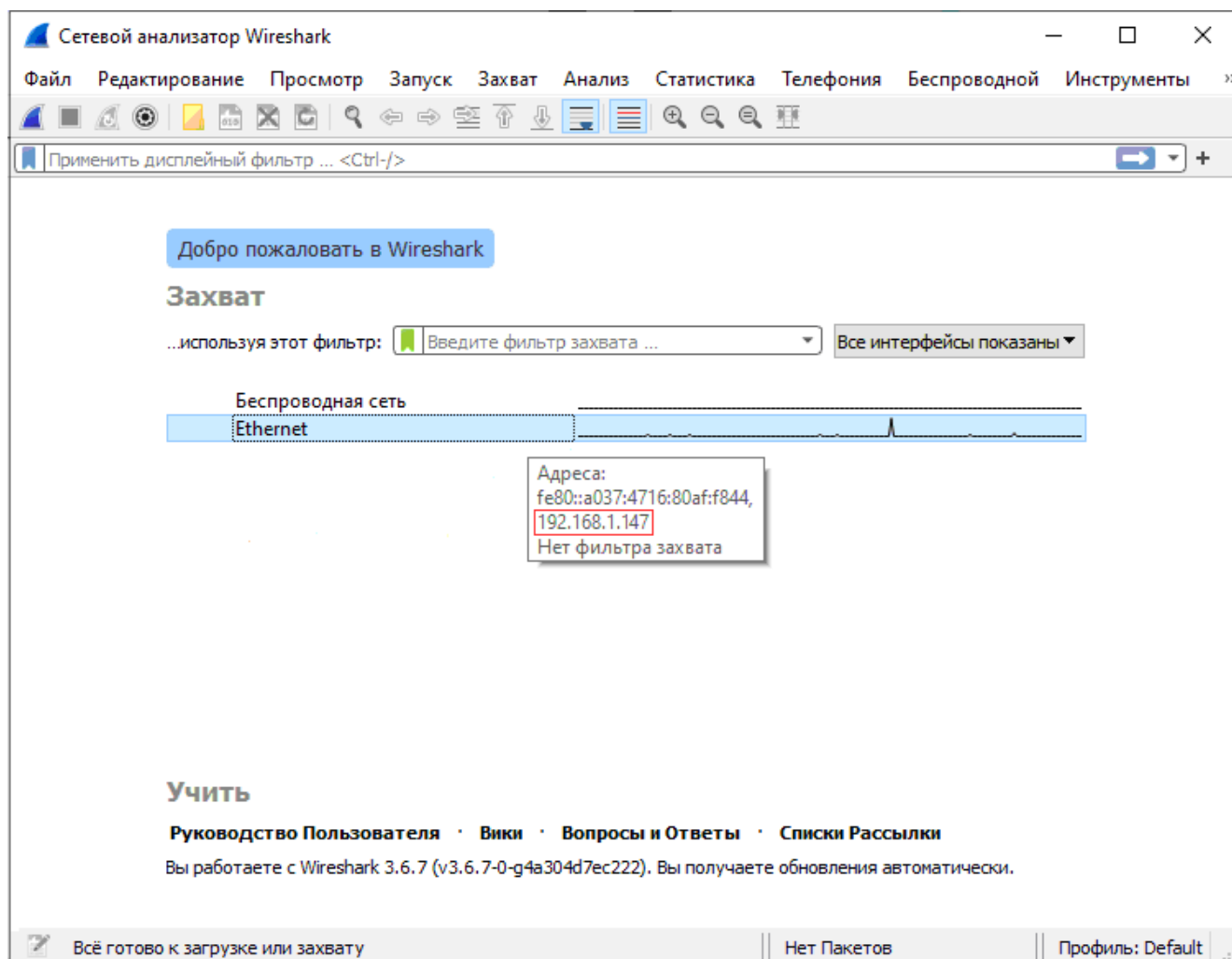
Назовите физический адрес сетевой интерфейсной платы этого компьютера.

б. Узнайте IP-адрес другого компьютера (устройства), находящегося в той же подсети.

Шаг 2. Запустите программу Wireshark и начните захват данных.

а. Запустите программу Wireshark.

б. В списке интерфейсов выберите необходимый интерфейс.




Примечание. Если указано несколько интерфейсов, убедитесь в том, что **IP**-адрес выбранного интерфейса **соответствует тому, что вы узнали в шаге 1a**.

В верхней части окна программы **Wireshark** должна выводиться информация. Цвет строк данных, выводимых **Wireshark** зависит от протокола, к которому они относятся.

Шаг 3. Применение фильтров программы Wireshark для отображения на экране только нужного трафика.

Информация на экране может выводиться очень быстро. Скорость вывода зависит от многих факторов. Чтобы облегчить поиск и анализ данных, захваченных программой **Wireshark**, применяют фильтры, скрывающие ненужный трафик. Фильтр лишь отображает нужный трафик на экране, но не блокирует захват других кадров. В этой лабораторной работе анализируются только единицы данных протокола **ICMP**, полученные с помощью команды **ping**.

a. В поле **Фильтр** в верхней части окна программы **Wireshark** введите **icmp**, чтобы на экран выводились только сведения о кадрах, содержащих единицы данных протокола **ICMP**. При правильном задании фильтра, указанное поле станет зеленым. После этого, нажмите клавишу **Ввод** или кнопку **Применить** , чтобы применить фильтр.

После этого верхняя часть окна программы **Wireshark** очистится от данных, однако захват трафика в интерфейсе продолжится.

b. Откройте окно командной строки ОС **Windows** на компьютере и

отправьте с помощью команды **ping** эхо-запрос на **IP**-адрес компьютера, полученный в шаге 1, пункт **б** (находящегося в той же подсети).

```
Командная строка

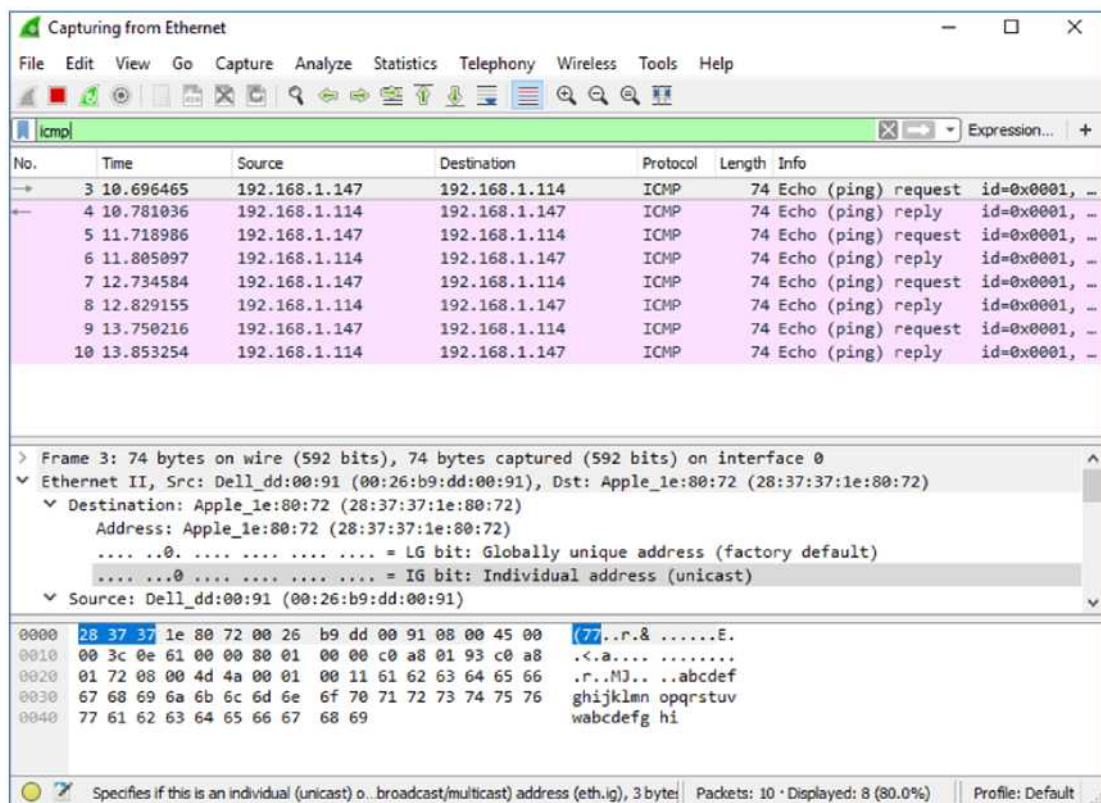
C:\>ping 192.168.1.114

Обмен пакетами с 192.168.1.114 по с 32 байтами данных:
Ответ от 192.168.1.114 число байт=32 время<1мс TTL=64
Ответ от 192.168.1.114 число байт=32 время<1мс TTL=64
Ответ от 192.168.1.114 число байт=32 время<1мс TTL=64
Ответ от 192.168.1.114 число байт=32 время<1мс TTL=64

Статистика Ping для 192.168.1.114:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
              (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

C:\>
```

с. В верхней части окна программы **Wireshark** должны снова появиться данные.



Примечание. Если компьютер из той же подсети не отвечает на эхо-запросы, то возможно, их блокирует межсетевой экран. Чтобы обеспечить пропуск трафика **ICMP** через межсетевой экран на компьютере с ОС **Windows**, воспользуйтесь **Приложением А**. Пропуск трафика **ICMP** через межсетевой экран.

d. Нажмите на значок **Остановить захват пакетов**  , чтобы остановить захват кадров.

Шаг 4. Проанализируйте полученные данные.

На шаге 4 необходимо изучить данные, сформированные эхо-запросами на компьютер в той же подсети. Окно программы **Wireshark**

состоит из трех частей:

в верхней части отображается список полученных кадров и общая информация о них;

в средней части приводится информация о кадре, **выбранном в верхней части экрана**;

в нижней части отображаются декодированные данные верхних уровней, как в шестнадцатеричном представлении, так и в кодировке **ASCII**.

a. Выделите кадр первого запроса **ICMP** в верхней части окна программы **Wireshark**. В столбце **Source** (Источник) должен быть указан **IP**-адрес вашего компьютера, а в столбце **Destination** (Назначение) — **IP**-адрес компьютера в той же подсети, на который вы отправили эхо-запрос.

b. Не меняя выделенный кадр в верхней части окна, перейдите в среднюю часть. Нажмите значок > слева от строки **Ethernet II**, чтобы просмотреть физические адреса источника и назначения.

Совпадает ли физический адрес источника с физическим адресом сетевого интерфейса вашего компьютера?

Совпадает ли физический адрес назначения с физическим адресом другого компьютера в той же подсети, на который вы отправили эхо-запрос?


Как ваш компьютер определил физический адрес другого компьютера в той же подсети, на который он отправил эхо-запрос с помощью команды **ping**?

Примечание. В показанном примере перехваченного кадра, данные протокола **ICMP** инкапсулируются в пакет **IPv4**, который затем инкапсулируется в кадр **Ethernet II** для передачи по локальной сети.

Шаг 5. Из окна командной строки компьютера отправьте эхо-запрос на основной шлюз.

Из окна командной строки ОС **Windows** компьютера отправьте с помощью команды **ping** эхо-запрос на основной шлюз, используя **IP**-адрес, записанный в шаге 1, пункт **a**.

Шаг 6. Остановите захват кадров программой Wireshark.

Нажмите значок **Остановить захват пакетов** , чтобы остановить захват кадров.

Шаг 7. Изучите первый эхо-запрос в программе Wireshark.

a. На панели списка кадров (верхняя часть) выделите необходимый кадр. В столбце **Info** должно быть указано **Echo (ping) request** (Эхо-запрос с помощью команды **ping**).

b. Изучите в панели сведений о кадре в средней части экрана первую строку. В этой строке показана длина кадра.

c. Вторая строка в панели сведений о кадре показывает, что это кадр

Ethernet II. Здесь же отображаются физические адреса источника и назначения.

Назовите физический адрес сетевой интерфейсной платы этого компьютера.

Назовите физический адрес основного шлюза.

d. Вы можете щелкнуть значок > в начале второй строки, чтобы получить развернутую информацию о кадре **Ethernet II**.

Назовите тип текущего кадра.

e. Последние две строки среднего раздела содержат информацию о поле данных кадра. В рассматриваемом примере, данные содержат **IPv4**-адреса источника и назначения.

Назовите **IP**-адрес источника.

Назовите **IP**-адрес назначения.

f. Для того, чтобы выделить часть кадра (в шестнадцатеричной системе и в кодировке **ASCII**) в нижней части окна программы **Wireshark**, необходимо щелкнуть по любой строке в средней части. Щелкните по строке **Internet Control Message Protocol** в средней части и посмотрите, что будет выделено в нижней части.

Какое слово образуют последние два выделенных октета?


g. Нажмите **следующий** кадр в верхней части и изучите кадр эхо-ответа. Физические адреса источника и назначения **поменялись местами**, т. к. основной шлюз, отправил этот кадр в ответ на первый эхо-запрос.

Какое устройство и какой физический адрес показаны в качестве адреса назначения?

Часть 3. Захват и анализ данных протокола ICMP для удаленных узлов с помощью программы Wireshark

В части 3 необходимо отправить с помощью команды **ping** эхо-запросы на удаленные узлы (расположенные за пределами локальной сети) и изучить данные, сформированные этими запросами. Затем необходимо определить различия между этими данными и данными, полученными в части 2.

Шаг 1. Запустите захват данных в программой Wireshark.


a. Нажмите значок **Перезапустить текущий захват** , чтобы начать новый перехват кадров в программе **Wireshark**. Откроется всплывающее окно с предложением сохранить перед началом нового перехвата предыдущие перехваченные кадры в файл. Сохранять данные необязательно. Нажмите **Продолжить без сохранения**.

b. Отправьте из командной строки ОС **Windows** с помощью команды **ping** эхо-запросы на следующие URL-адреса узлов:

- 1) www.yahoo.com
- 2) www.cisco.com
- 3) www.google.com

Примечание. При отправке эхо-запросов с помощью команды **ping** на указанные URL-адреса, служба доменных имен (**DNS**) сопоставляет адрес URL и IP-адрес.


Запишите IP-адреса, сопоставленные службой доменных имен каждому URL-адресу.

c. Остановите захват кадров, нажав на значок **Остановить захват пакетов** .


Шаг 2. Проанализируйте данные, полученные от удаленных узлов.

Просмотрите перехваченные кадры в программе **Wireshark**. Укажите IP- и физические адреса назначения для всех узлов.


IP-адрес для www.yahoo.com: 

Физический адрес для www.yahoo.com: 

IP-адрес для www.cisco.com: 

Физический адрес для www.cisco.com: 

IP-адрес для www.google.com: 

Физический адрес для www.google.com: 

Проанализируйте IP- и физические адреса узлов, на которые были отправлены эхо-запросы. Какова существенная особенность этих данных?

Почему IP-адрес назначения изменяется, а физический адрес назначения остается прежним?

Как эти данные отличаются от данных, полученных в результате эхо-запросов, отправленных на локальные узлы в части 2?

Вопросы для повторения

Почему программа **Wireshark** показывает фактические физические адреса локальных узлов, но не показывает фактические физические адреса удаленных узлов?

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

Приложение А. Пропуск трафика протокола ICMP через межсетевой экран

Если эхо-запросы, отправленные с помощью команды **ping** с других компьютеров не достигают вашего компьютера, возможно, их блокирует межсетевой экран. В этом приложении объясняется, как обеспечить прохождение эхо-запросов через межсетевой экран, а также как отменить это по завершении лабораторной работы.

Часть 1. Создание нового правила, разрешающего прохождение трафика ICMP через межсетевой экран.

a. Перейдите в **Панель управления** и выберите параметр **Система и безопасность** в представлении **Категория**.

b. В окне **System and Security** (Система и информационная безопасность) выберите **Windows Defender Firewall** или **Windows Firewall**.

c. В левой части окна **Windows Firewall** или **Windows Defender Firewall** выберите **Advanced settings** (Дополнительные параметры).

d. В окне **Advanced Security** (Расширенные функции безопасности) выберите параметр **Inbound Rules** (Правила для входящих подключений) на левой боковой панели, а затем щелкните **New Rule...** (Создать правило...) на правой боковой панели.

e. Откроется Мастер создания новых правил для входящих подключений. На экране **Rule Type** (Тип правила) нажмите селективную кнопку **Custom** (Настраиваемые) и нажмите **Next** (Далее).

f. На левой панели щелкните параметр **Protocol and Ports** (Протокол и порты) и выберите **ICMPv4** из раскрывающегося меню **Protocol Type** (Тип протокола), затем щелкните **Next** (Далее).

g. Убедитесь, что выбран любой IP-адрес для локальных и удаленных IP-адресов. Для продолжения нажмите кнопку **Next** (Далее).

h. Выберите **Разрешить подключение**. Для продолжения нажмите кнопку **Next** (Далее).

i. По умолчанию это правило применяется ко всем профилям. Для продолжения нажмите кнопку **Next** (Далее).

j. Назовите правило **Разрешить запросы ICMP**. Нажмите **Готово**, чтобы продолжить. Созданное правило позволит другим устройствам сети получать эхо-отклики с вашего компьютера.

Часть 2. Отключение или удаление нового правила.

По завершении лабораторной работы отключите или удалите правило, созданное в части 1, пункт j.

a. В левой части окна **Advanced Security** (Расширенные функции безопасности) выберите **Inbound Rules** и найдите правило, созданное ранее в части 1, пункт j.

b. Щелкните правой кнопкой мыши правило **ICMP** и выберите пункт **Отключить правило** или **Удалить**. Выбор пункта **Отключить правило**

позволит снова включить его, если это снова станет необходимо. Выбор пункта **Удалить** позволит навсегда удалить правило для входящих подключений из списка. Если после этого снова потребуется разрешить запросы **ICMP**, правило нужно будет создавать заново.