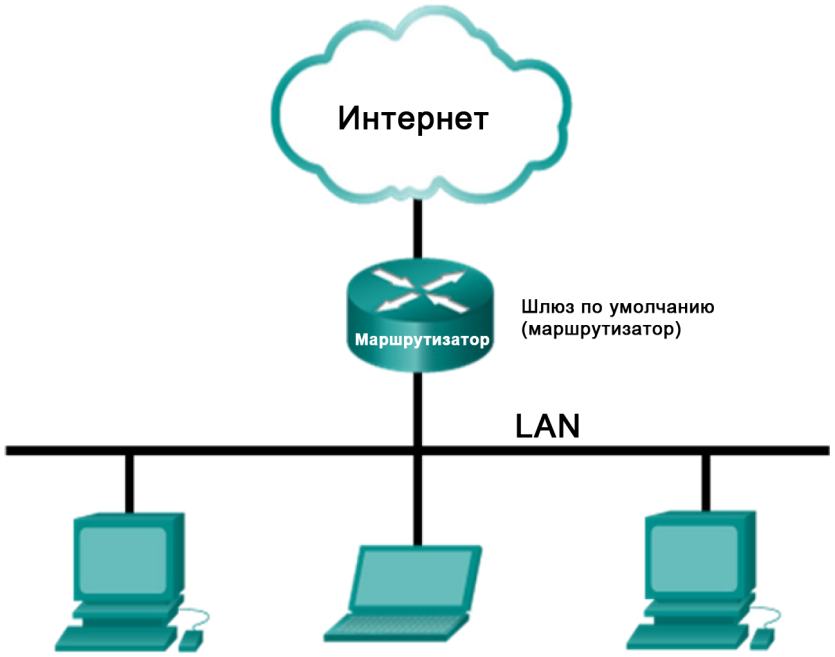
Лабораторная работа. Использование программы Wireshark для просмотра сетевого трафика

Топология



Задачи

Часть 1. Сбор и анализ данных протокола ICMP в программе Wireshark при передаче данных в локальной сети

Часть 2. Сбор и анализ данных протокола ICMP в программе Wireshark при передаче данных в удаленную сеть

Общие сведения/сценарий

Wireshark — это программа для анализа протоколов (анализатор пакетов), которая используется для поиска и устранения неполадок в сети, анализа, разработки программного обеспечения и протоколов, а также обучения. По мере движения потоков данных по сети анализатор «захватывает» каждую единицу данных протокола (PDU), после чего расшифровывает или анализирует ее содержание согласно соответствующему документу RFC или другим спецификациям.

Wireshark — полезный инструмент для всех, кто работает с сетями. Его можно использовать для анализа данных, а также для поиска и устранения неполадок при выполнении большинства лабораторных работ в рамках курсов CCNA. В ходе лабораторной работы вы научитесь пользоваться программой Wireshark для захвата IP-адресов пакетов данных ICMP и MAC-адресов Ethernet-кадров.

Необходимые ресурсы

- Один ПК (Windows 7 или 8 с доступом в Интернет)

- Дополнительные ПК в локальной сети будут использоваться для ответов на эхо-запросы (с помощью команды ping).

Часть 1: Сбор и анализ данных протокола ICMP в программе Wireshark при передаче данных в локальной сети

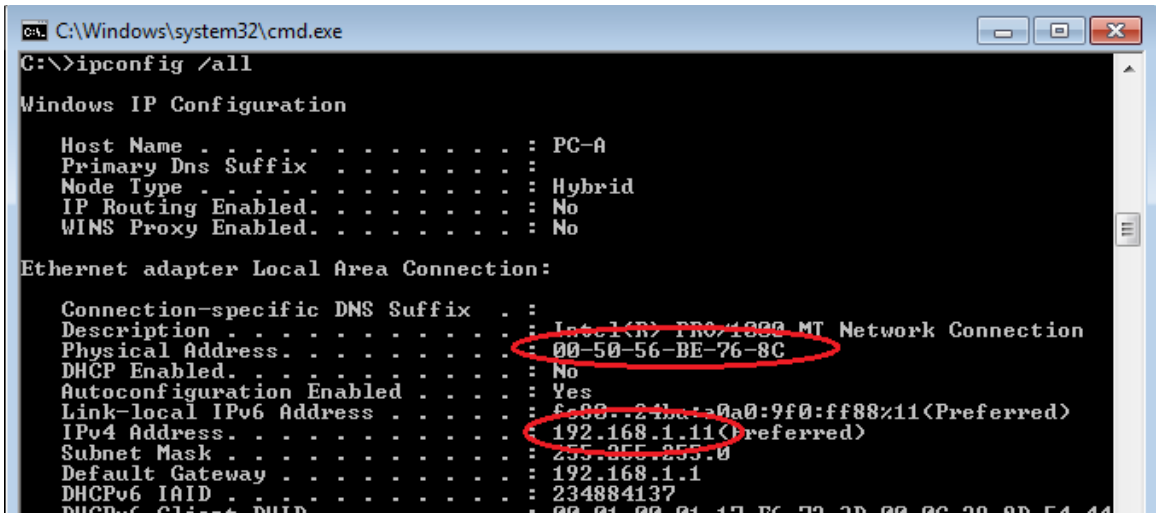
В части 1 этой лабораторной работы вы должны отправить эхо-запрос с помощью команды ping на другой ПК в локальной сети и перехватить ICMP-запросы и отклики в программе Wireshark. Кроме того, вам нужно найти необходимую информацию в собранных кадрах. Этот анализ поможет понять, как заголовки пакетов позволяют доставлять данные адресатам.

Шаг 1: Определите адреса интерфейсов вашего ПК.

В данной лабораторной работе вам необходимо узнать IP-адрес компьютера и физический адрес сетевой платы, который называется MAC-адресом.

a. Откройте окно командной строки, введите команду **ipconfig /all** и нажмите клавишу ввода.

b. Запишите IP-адрес интерфейса ПК и MAC-адрес (физический адрес).

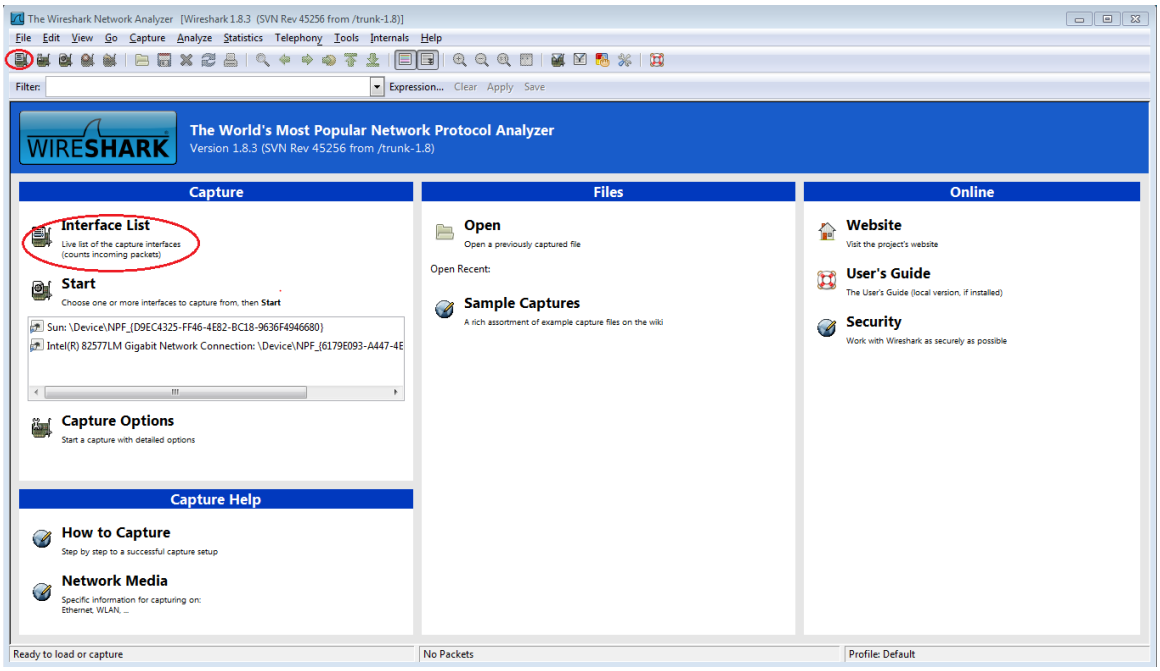


c. Обменяйтесь IP-адресами ПК с другими учащимися, но пока что не сообщайте им свой MAC-адрес.

Шаг 2: Запустите программу Wireshark и начните сбор данных.

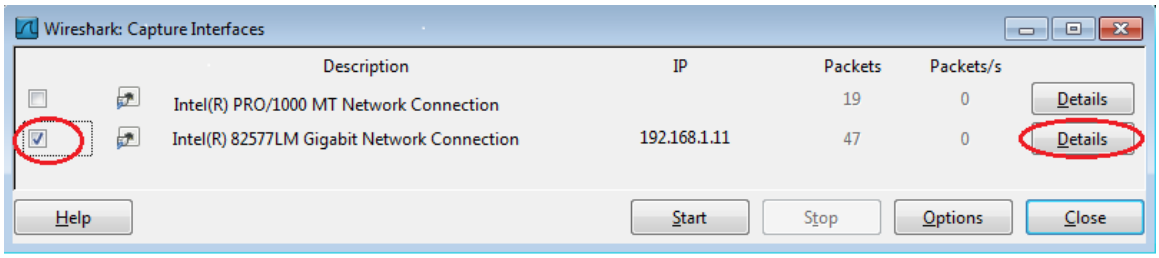
a. На своем ПК нажмите кнопку **Пуск** и найдите Wireshark в списке программ. Дважды нажмите на **Wireshark**.

b. После запуска программы Wireshark нажмите на **Interface List** (Список интерфейсов).

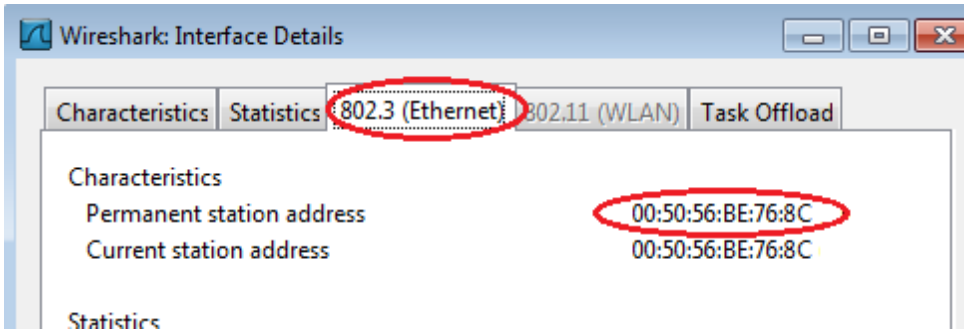


Примечание. Список интерфейсов можно также открыть, нажав на значок первого интерфейса в ряду значков.

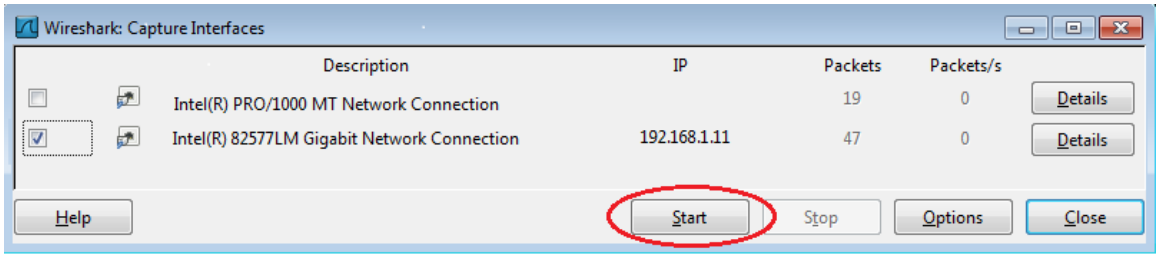
c. В окне Capture Interfaces (Захват интерфейсов) программы Wireshark установите флажок рядом с интерфейсом, подключенным к вашей локальной сети.



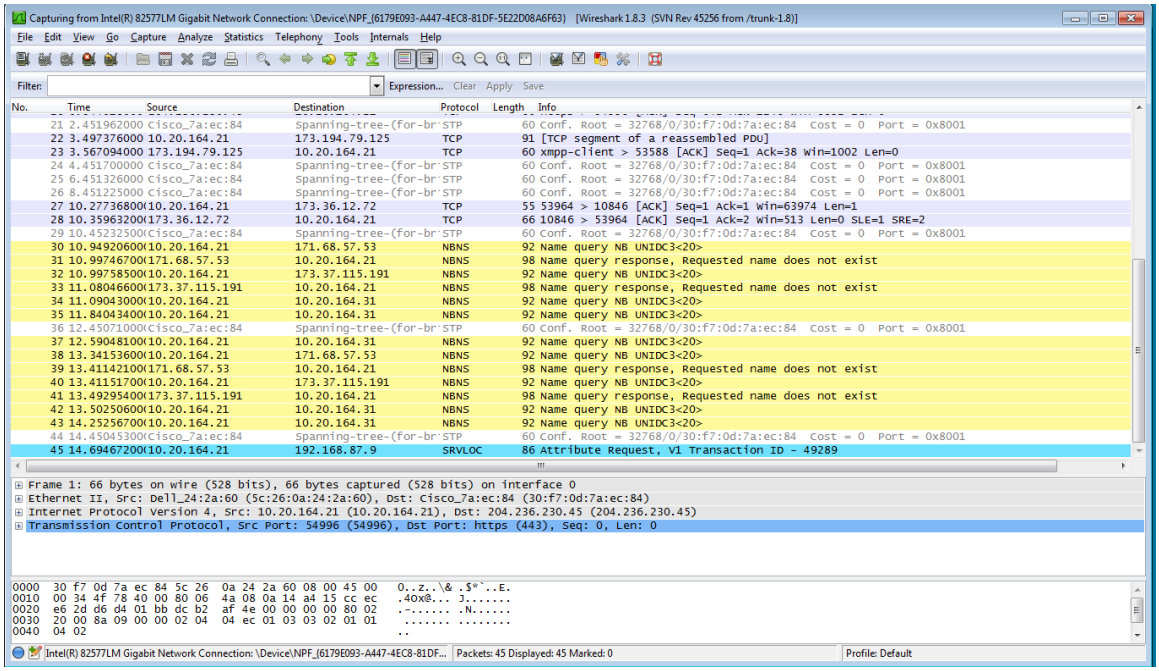
Примечание. Если перечислено несколько интерфейсов и вы не уверены в том, какой из них нужно выбрать, нажмите кнопку **Details** (Подробнее) и откройте вкладку **802.3 (Ethernet)**. Убедитесь в том, что MAC-адрес соответствует результату, который вы получили в шаге 1б. Убедившись в правильности интерфейса, закройте окно информации об интерфейсе.



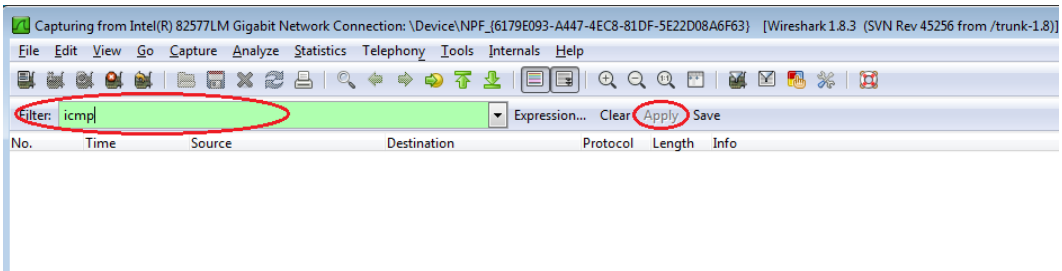
d. После этого нажмите кнопку **Start** (Начать), чтобы начать захват данных.



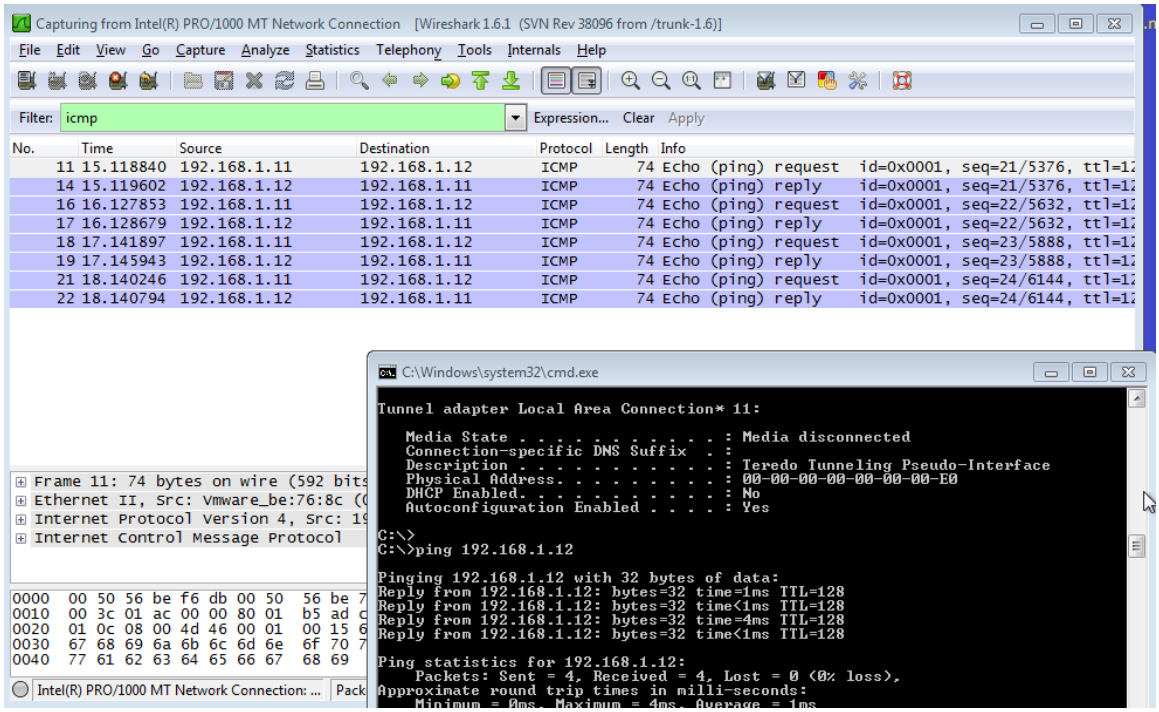
В верхней части окна программы Wireshark начнет прокручиваться информация. Строки данных выделяются различными цветами в зависимости от протокола.



e. Информация может прокручиваться очень быстро, это зависит от интенсивности взаимодействия ПК с локальной сетью. Чтобы облегчить просмотр и работу с данными, собранными программой Wireshark, можно применить фильтр. В этой лабораторной работе нас интересуют только единицы данных протокола (PDU) ICMP (эхо-запрос с помощью команды ping). Чтобы вывести на экран только единицы данных протокола ICMP (эхо-запрос с помощью команды ping), в поле фильтра в верхней части окна программы Wireshark введите **icmp** и нажмите клавишу ввода или кнопку **Apply** (Применить).

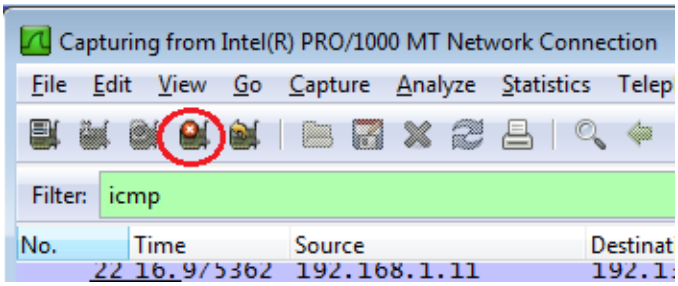


f. После этого все данные в верхнем окне исчезнут, однако захват трафика в интерфейсе продолжится. Откройте окно командной строки, которое вы открывали ранее, и отправьте эхо-запрос с помощью команды ping на IP-адрес, полученный от другого учащегося. Обратите внимание на то, что в верхней части окна программы Wireshark снова появятся данные.



Примечание. Если компьютеры других учащихся не отвечают на ваши эхо-запросы, это может быть вызвано тем, что межсетевые экраны их компьютеров блокируют эти запросы. Информацию о том, как обеспечить пропуск трафика ICMP через межсетевой экран на ПК с ОС Windows 7 см. в Ошибка: источник перекрёстной ссылки не найден.

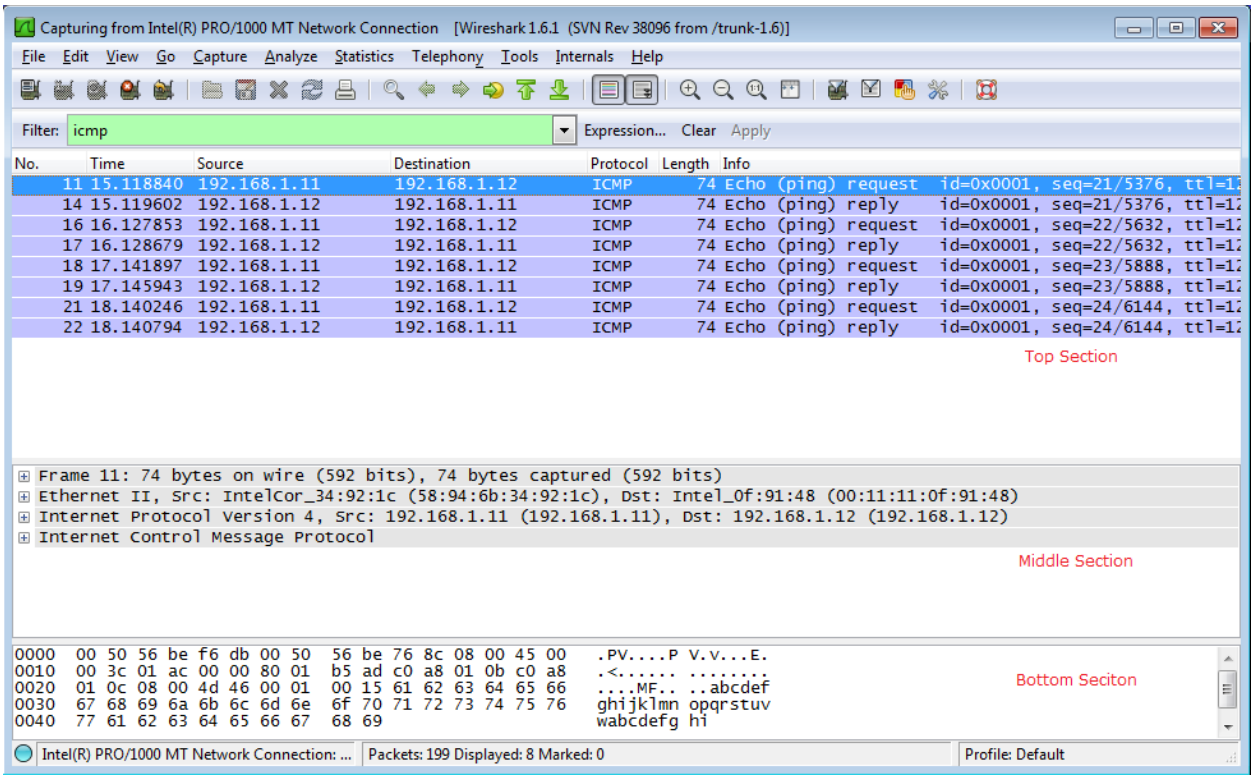
g. Остановите захват данных, нажав на значок **Stop Capture** (Остановить захват).



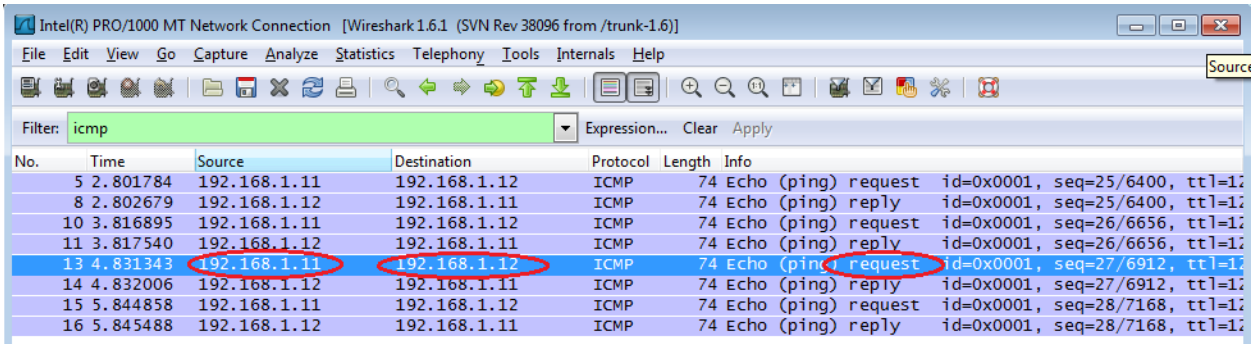
Шаг 3: Изучите полученные данные.

В шаге 3 необходимо проверить данные, сформированные эхо-запросами с помощью команды ping на ПК других учащихся. Программа Wireshark отображает данные в трех разделах: 1) в верхнем разделе отображается список полученных кадров PDU со сводной информацией об IP-пакетах; 2) в среднем разделе приводится информация о PDU для кадра, выбранного в верхней части экрана, а также разделение перехваченного кадра PDU по уровням

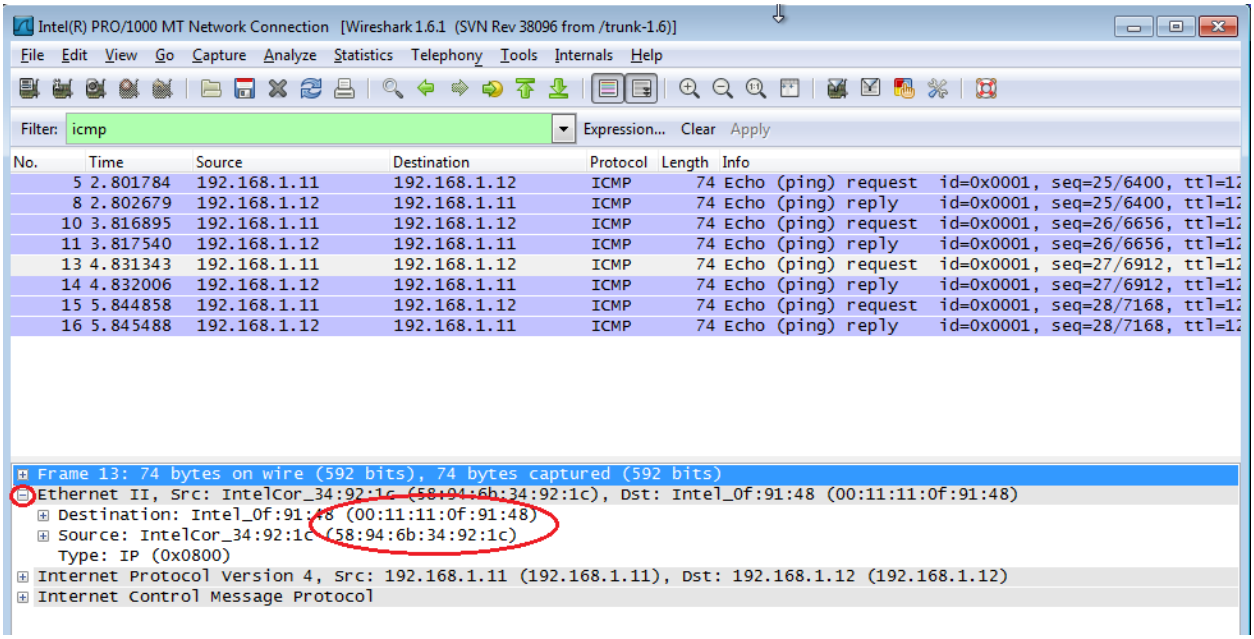
протоколов; 3) в нижнем разделе показываются необработанные данные каждого уровня. Необработанные данные отображаются как в шестнадцатеричном, так и в десятичном форматах.



a. Выберите кадры PDU первого запроса ICMP в верхнем разделе окна программы Wireshark. Обратите внимание на то, что в столбце Source (Источник) указывается IP-адрес вашего компьютера, а в столбце «Destination» (Назначение) — IP-адрес ПК другого участника, на который вы отправили эхо-запрос с помощью команды ping.



b. Не меняя выбор кадра PDU в верхнем разделе окна, перейдите в средний раздел. Нажмите на символ + слева от строки «Ethernet II», чтобы увидеть MAC-адреса источника и назначения.



Совпадает ли MAC-адрес источника с интерфейсом вашего компьютера? _____

Совпадает ли MAC-адрес назначения в программе Wireshark с MAC-адресом другого учащегося?

_____

Как ваш ПК определил MAC-адрес другого ПК, на который был отправлен эхо-запрос с помощью команды ping?

_____

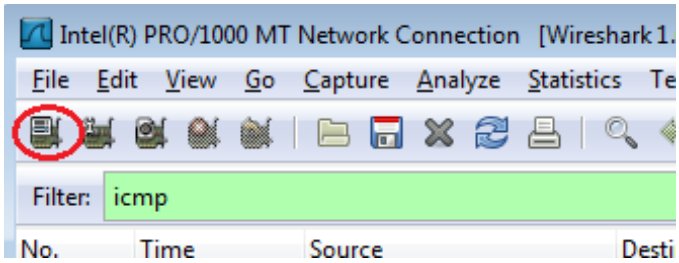
Примечание. В предыдущем примере захваченного ICMP-запроса данные протокола ICMP инкапсулируются внутри PDU пакета IPv4 (заголовка IPv4), который затем инкапсулируется в PDU кадра Ethernet II (заголовок Ethernet II) для передачи по локальной сети.

Часть 2: Сбор и анализ данных протокола ICMP в программе Wireshark при передаче данных в удаленную сеть

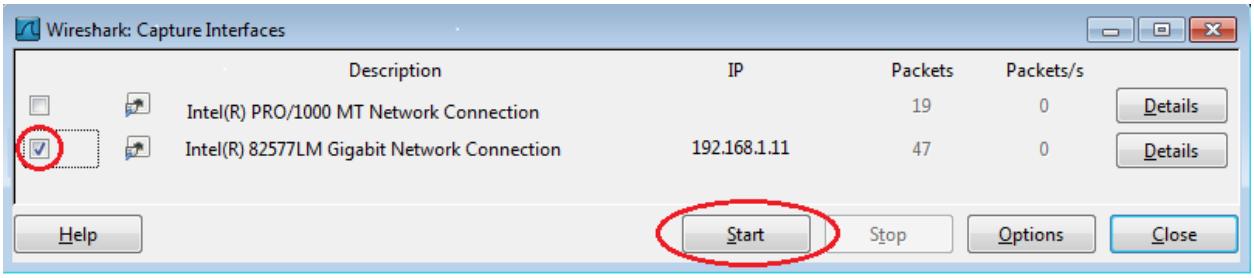
В части 2 вы должны будете отправить эхо-запросы с помощью команды ping на удаленные узлы (расположенные за пределами локальной сети) и изучить данные, сформированные этими запросами. Затем вам нужно будет определить различия между этими данными и данными, которые вы изучали в части 1.

Шаг 1: Запустите захват данных в интерфейсе.

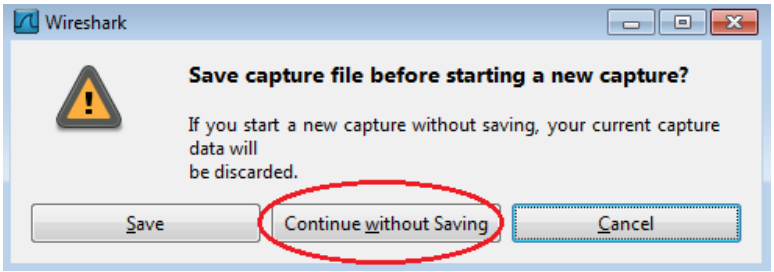
a. Нажмите на значок **Interface List** (Список интерфейсов), чтобы снова открыть список интерфейсов ПК.



b. Убедитесь, что напротив интерфейса локальной сети установлен флажок, и нажмите кнопку **Start** (Начать).



c. Появится окно с предложением сохранить полученные ранее данные перед началом нового захвата. Сохранять эти данные необязательно. Нажмите **Continue without Saving** (Продолжить без сохранения).

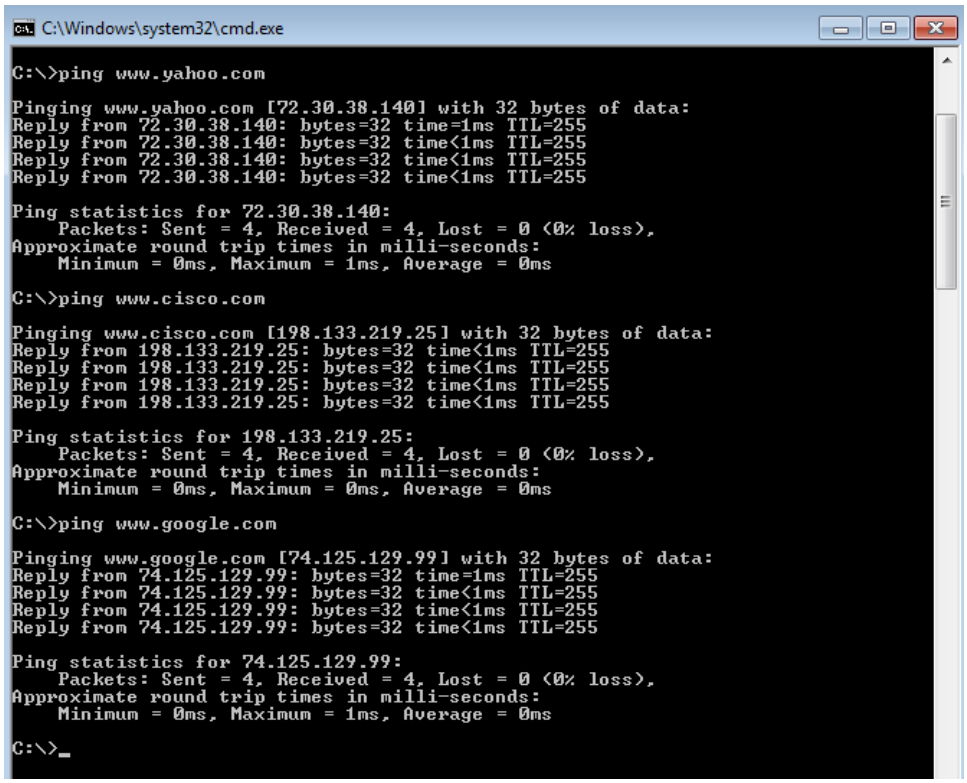


d. Активировав захват данных, отправьте эхо-запрос с помощью команды ping на следующие три URL-адреса веб-сайтов:

1) www.yahoo.com

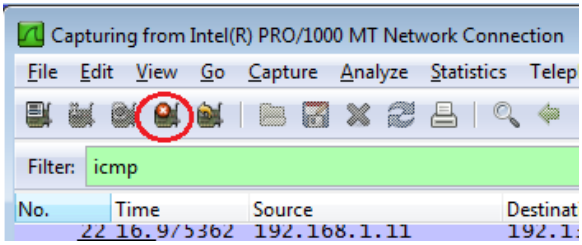
2) www.cisco.com

3) www.google.com



Примечание. При отправке эхо-запросов с помощью команды ping на указанные URL-адреса обратите внимание на то, что служба доменных имен (DNS) преобразует адрес URL в IP-адрес. Запишите IP-адреса, полученные для каждого URL-адреса.

e. Остановите захват данных, нажав на значок **Stop Capture** (Остановить захват).



Шаг 2: Изучите и проанализируйте данные, полученные от удаленных узлов.

a. Просмотрите собранные данные в программе Wireshark и изучите IP- и MAC-адреса трех веб-сайтов, на которые вы отправили эхо-запросы. Ниже в оставленном месте укажите IP- и MAC-адреса назначения для всех трех веб-сайтов.

1-й адрес: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

2-й адрес: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

3-й адрес: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

b. Какова существенная особенность этих данных?

_____

c. Как эта информация отличается от данных, полученных в результате эхо-запросов локальных узлов в части 1?

_____

_____

Вопросы для повторения

Почему программа Wireshark показывает фактические MAC-адреса локальных узлов, но не показывает фактические MAC-адреса удаленных узлов?

_____

_____

Лабораторная работа. Использование программы Wireshark для анализа кадров Ethernet

Топология

Задачи

Часть 1. Изучение полей заголовков в кадре Ethernet II

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

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 вышестоящих уровней используются TCP и IP, а тип доступа к среде передачи — Ethernet, то на 2 уровне кадры инкапсулируются по стандарту 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.

Необходимые ресурсы

- 1 ПК (Windows 7 или 8 с выходом в Интернет и программой Wireshark)

Часть 3: 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.

Шаг 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

Шаг 2: Изучите конфигурацию сети ПК.

IP-адрес узла ПК — 192.168.1.17, IP-адрес шлюза по умолчанию — 192.168.1.1.

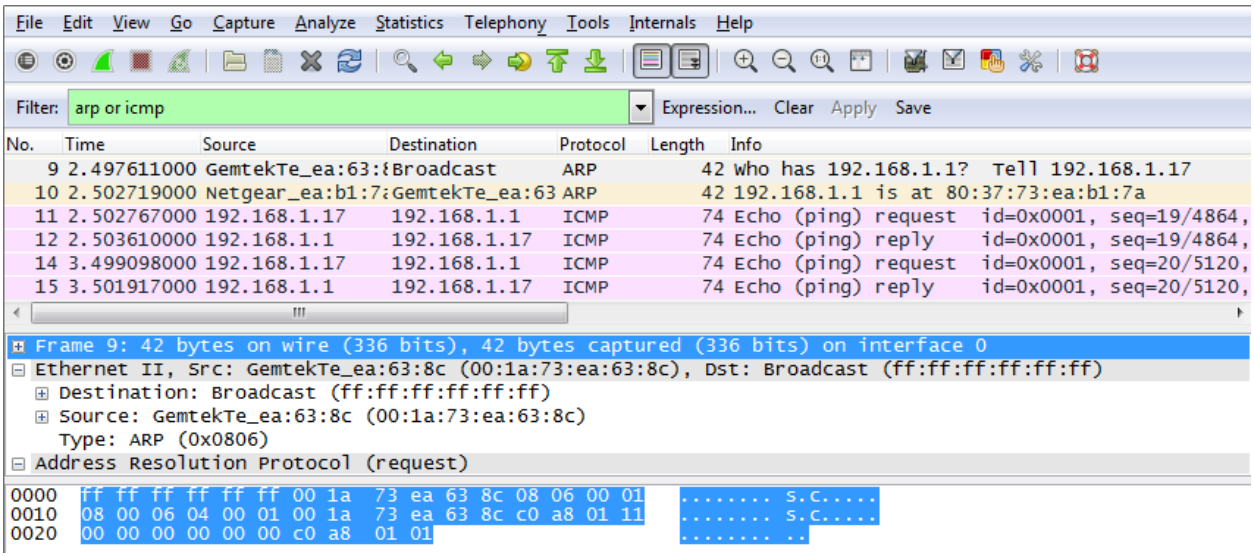
```
Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Broadcom 802.11a/b/g WLAN
   Physical Address. . . . . . . . . : 00-1A-73-EA-63-8C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a858:5f3e:35e2:d38f%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.17(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, June 16, 2015 6:59:54 AM
   Lease Expires . . . . . . . . . . : Wednesday, June 17, 2015 6:59:54 AM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 234887795
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1B-07-0A-E1-00-1E-EC-15-74-C2

   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Шаг 3: 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 MAC-адреса маршрутизатора шлюза, за которым следуют четыре эхо-запроса и ответа.



Шаг 4: 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 широковещательным (состоящим только из единиц) или индивидуальным (unicast). Адрес источника всегда должен быть индивидуальным адресом.
Адрес источника	GemtekTe_ea:63:8c (00:1a:73:ea:63:8c)	
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 производителя (OUI) сетевой платы источника. _____

Какая часть MAC-адреса соответствует OUI?

_____

Назовите серийный номер сетевой платы источника. _____

Часть 4: 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.

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

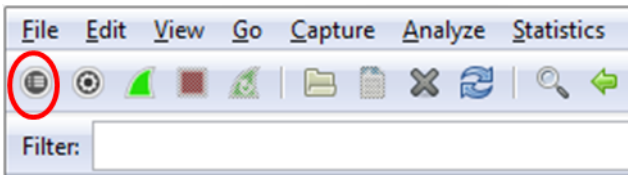
Откройте окно командной строки и введите **ipconfig** .

Назовите IP-адрес шлюза ПК по умолчанию. _____

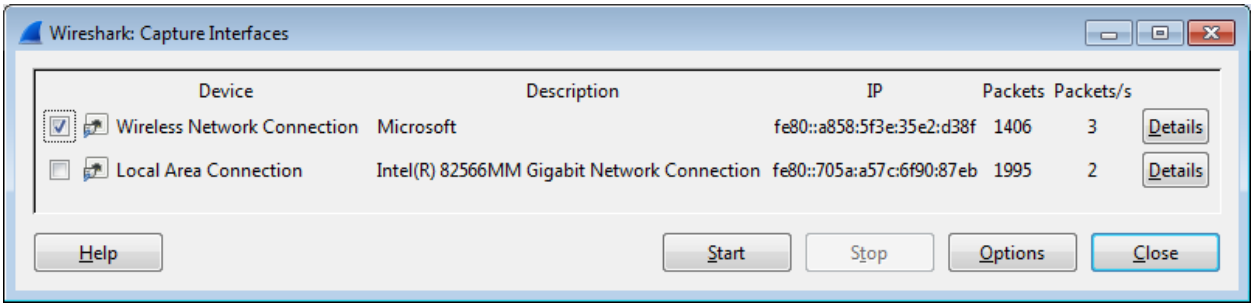
Шаг 2: Начните захват трафика на сетевой плате своего ПК.

a. Откройте Wireshark.

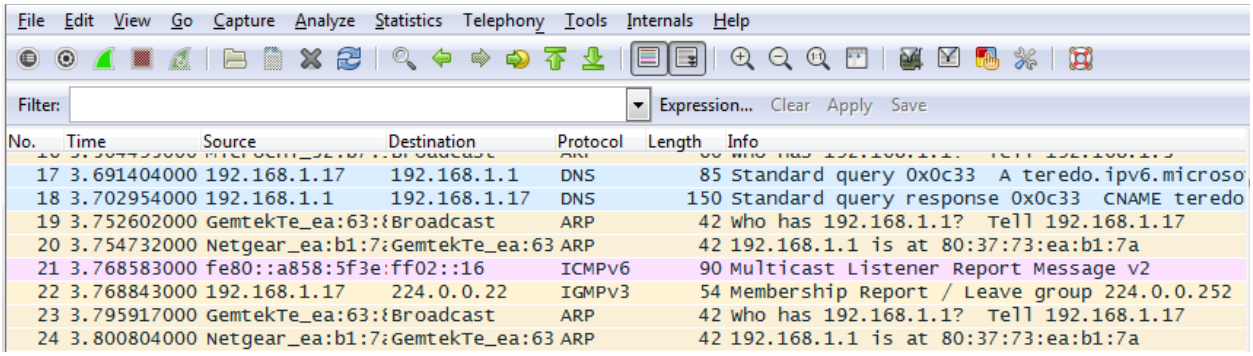
b. На панели анализатора сети Wireshark нажмите значок **Interface List** (Список интерфейсов).



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.



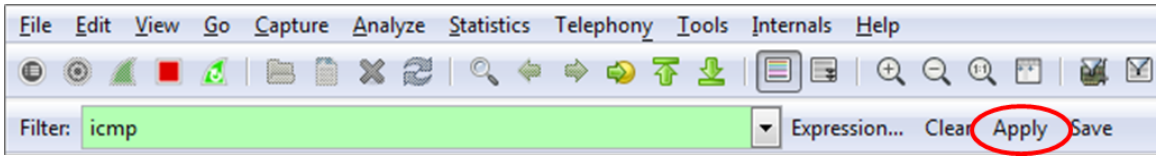
d. Понаблюдайте за трафиком в окне списка пакетов.



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 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), чтобы применить фильтр.

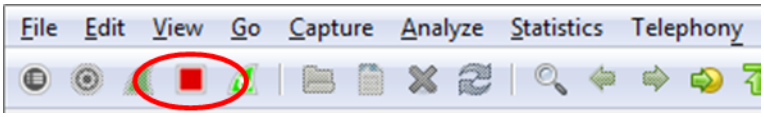


Шаг 4: Из окна командной строки отправьте эхо-запрос на шлюз ПК по умолчанию.

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

Шаг 5: Остановите захват трафика на сетевой плате.

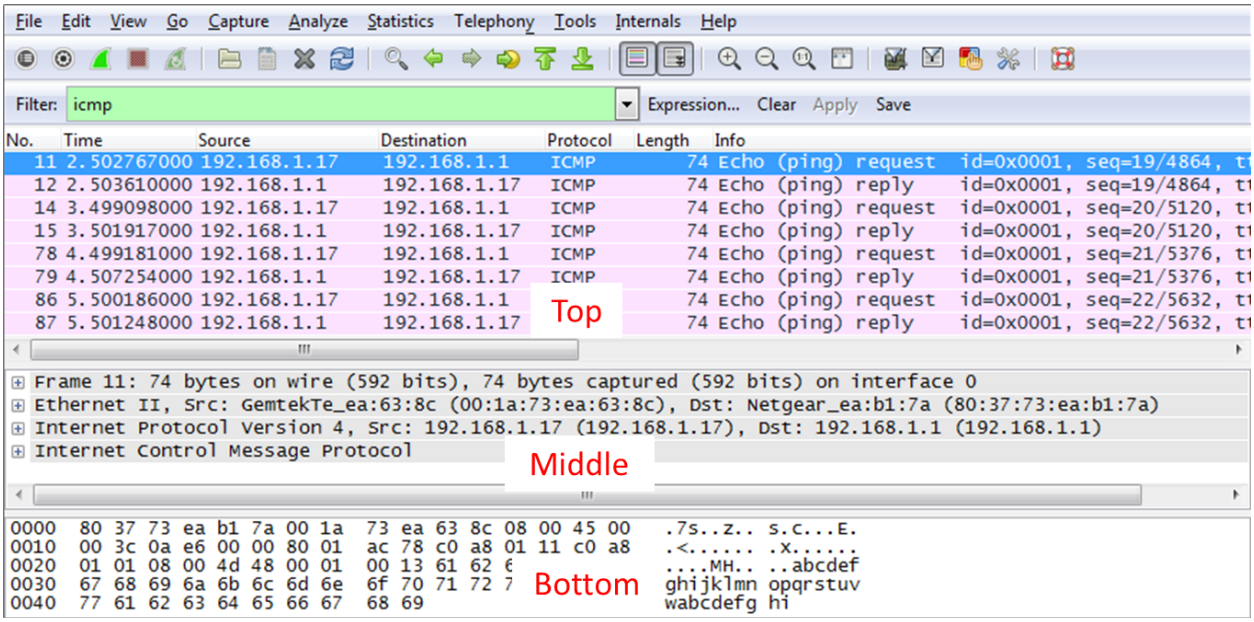
Нажмите значок **Stop Capture** (Остановить захват), чтобы остановить захват трафика.



Шаг 6: Изучите первый эхо-запрос в программе Wireshark.

Главное окно программы Wireshark состоит из трех 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 приведенном 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 на панели сведений о пакете в средней части экрана. В этой строке указывается длина кадра (в данном примере — 74 байта).

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

Назовите MAC-адрес сетевой платы 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 («-»).

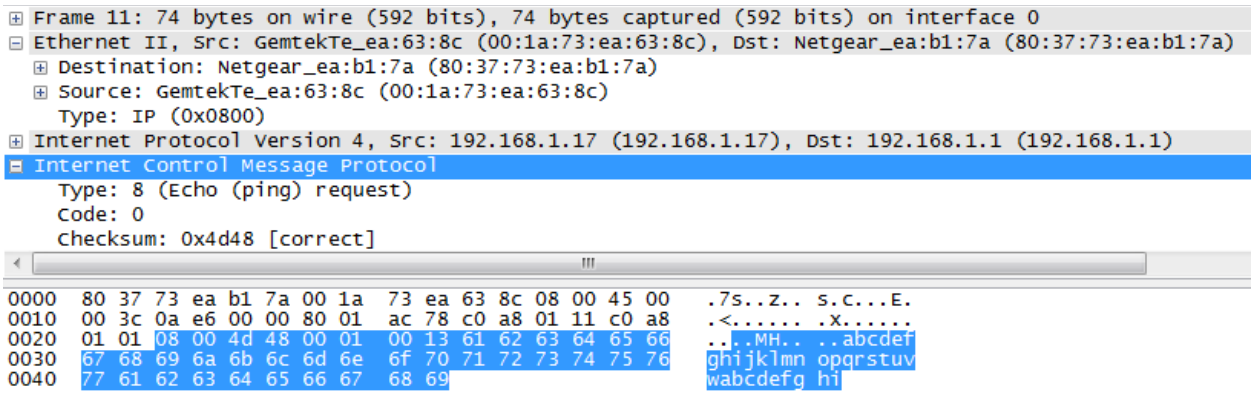
Назовите отображающийся тип кадра. _____

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) на панели отображения пакета в виде последовательности байтов (нижний раздел), нажмите на любую строку в среднем разделе. Нажмите строку **Internet Control Message Protocol** в среднем разделе и посмотрите, что будет выделено на панели отображения пакета в виде последовательности байтов.



Какое слово образуют последние два выделенных октета? _____

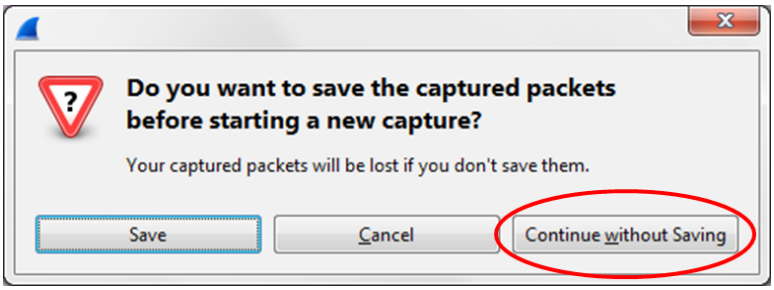
g. Нажмите на следующий кадр в верхнем разделе и изучите кадр эхо-ответа. Обратите внимание на то, что MAC-адреса источника и назначения поменялись местами, поскольку маршрутизатор, который служит шлюзом по умолчанию, отправил этот кадр в ответ на первый эхо-запрос.

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

_____

Шаг 7: 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).



Шаг 8: Через окно командной строки отправьте эхо-запрос 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.

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?

_____

_____

_____

_____

Вопросы для повторения

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

_____

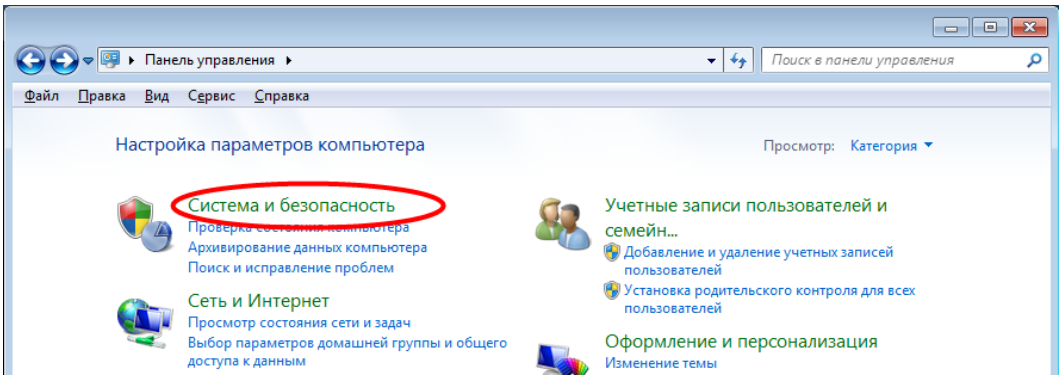
_____

Приложение A. Пропуск трафика ICMP через межсетевой экран

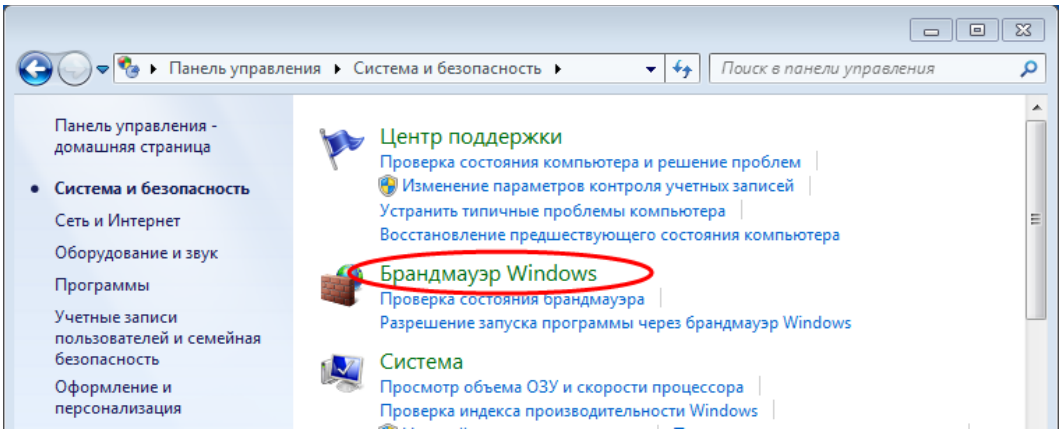
Если эхо-запросы с помощью команды ping с других компьютеров не проходят на ваш ПК, возможно, их блокирует межсетевой экран. В этом приложении объясняется, как обеспечить пропуск эхо-запросов через межсетевой экран, а также как отменить новое правило ICMP по завершении лабораторной работы.

1 Создайте новое правило, разрешающее прохождение ICMP-трафика через межсетевой экран.

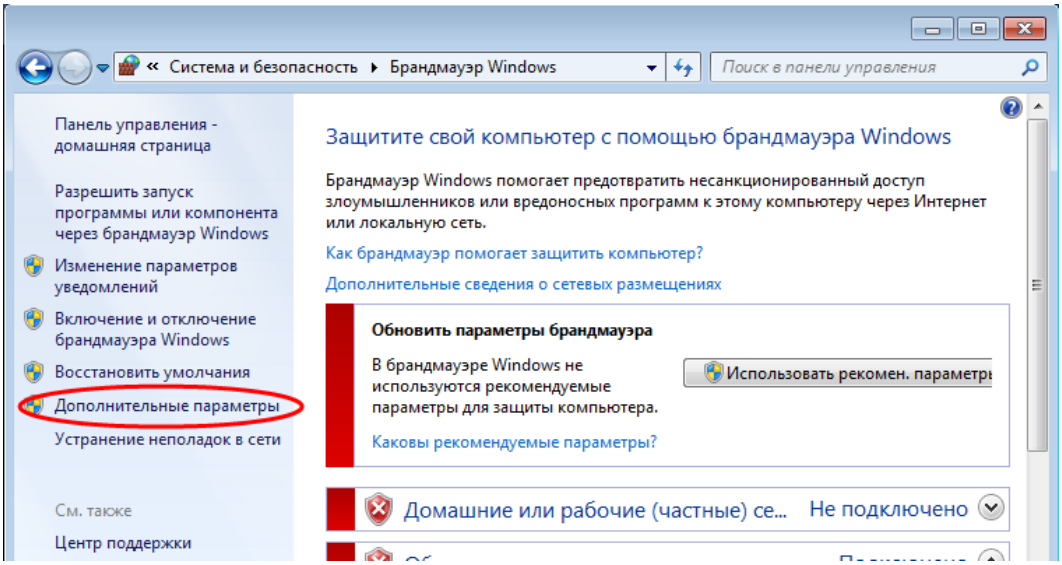
a На Панели управления выберите пункт **Система и безопасность**.



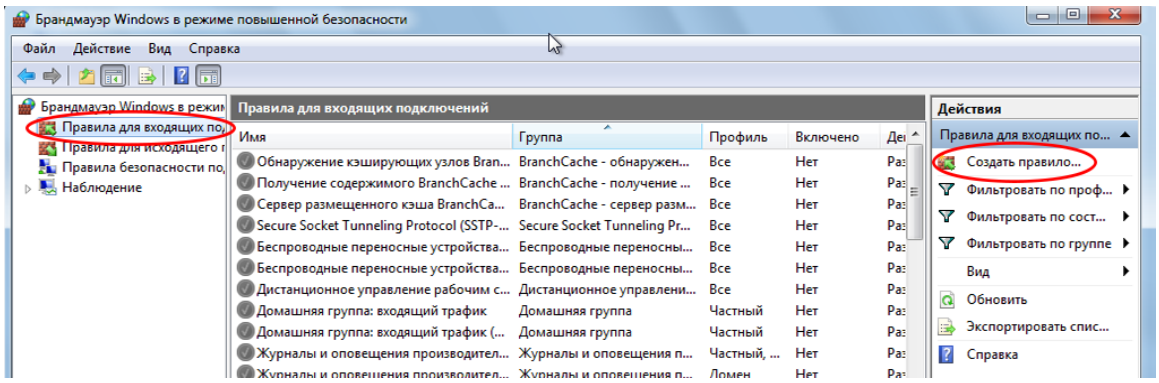
a. В окне «Система и безопасность» выберите **Брандмауэр Windows**.



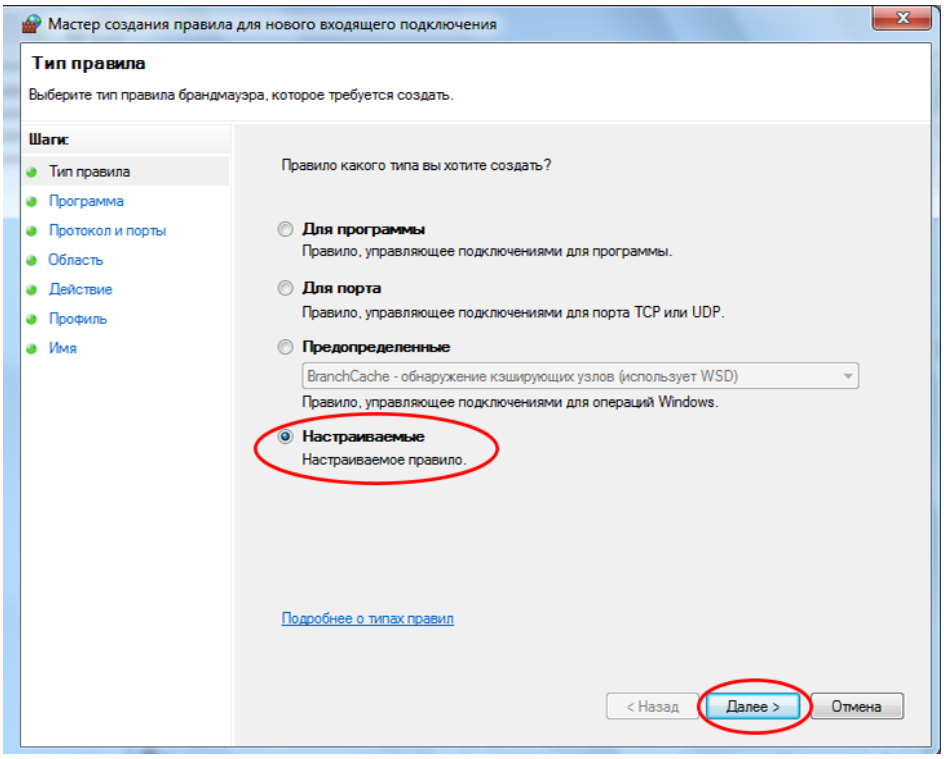
b. В левой части окна «Брандмауэр Windows» выберите **Дополнительные параметры**.



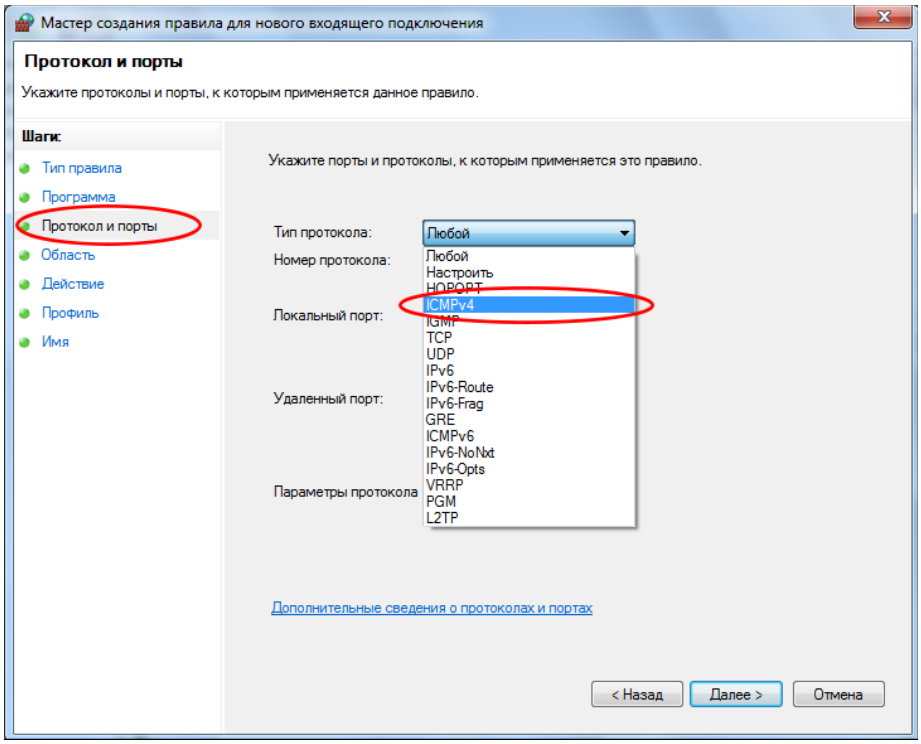
c. В окне «Дополнительные настройки безопасности» выберите в левой боковой панели **Правила для входящих подключений**, а затем **Создать правило...** в правой боковой панели.



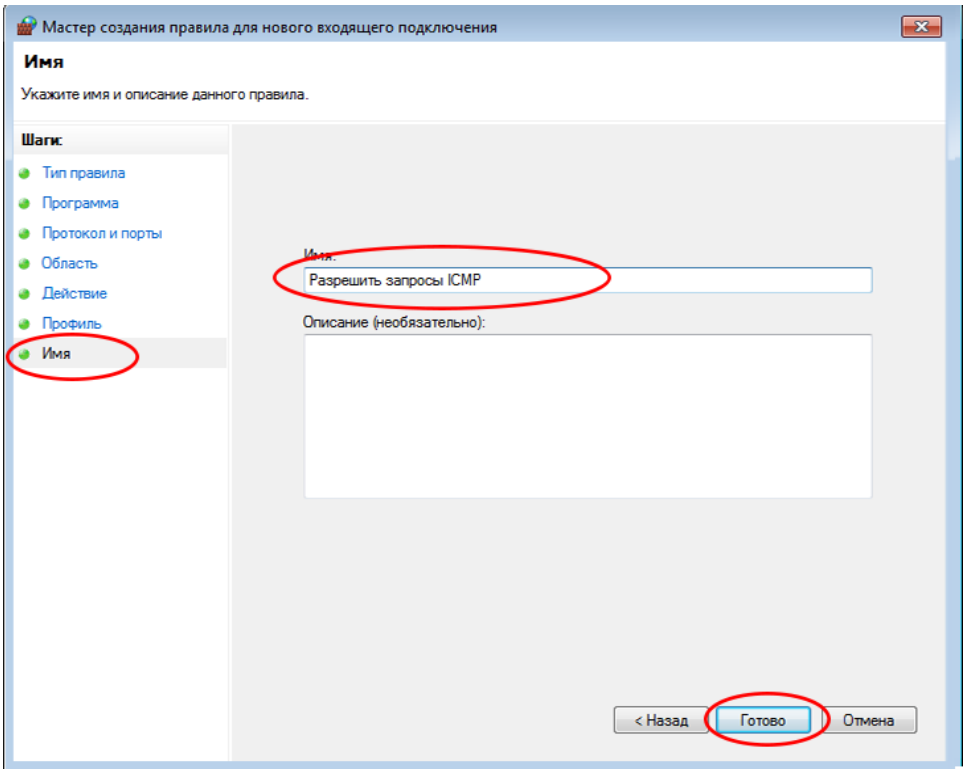
d. Откроется мастер создания новых правил для входящих подключений. В окне «Тип правила» установите переключатель **Настраиваемые** и нажмите кнопку **Далее**.



e. В левой панели выберите **Протокол и порты**, затем в раскрывающемся меню типов протокола выберите пункт **ICMPv4**. После этого нажмите кнопку **Далее**.



f. В левой панели выберите **Имя** и в соответствующее поле введите **Allow ICMP Requests** (Разрешить запросы ICMP). Нажмите **Готово**.

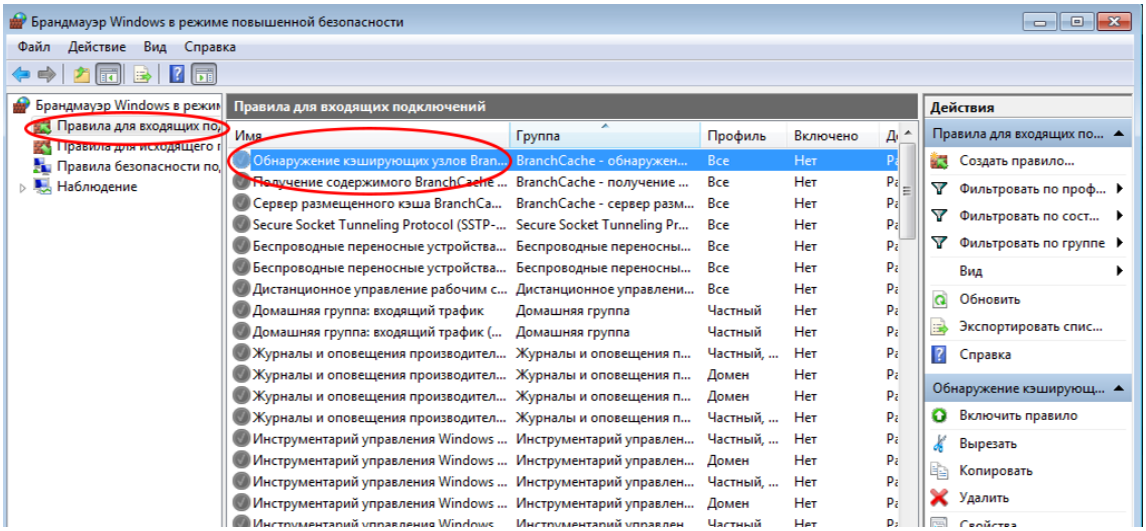


Созданное правило позволит другим учащимся получать эхо-отклики с вашего ПК.

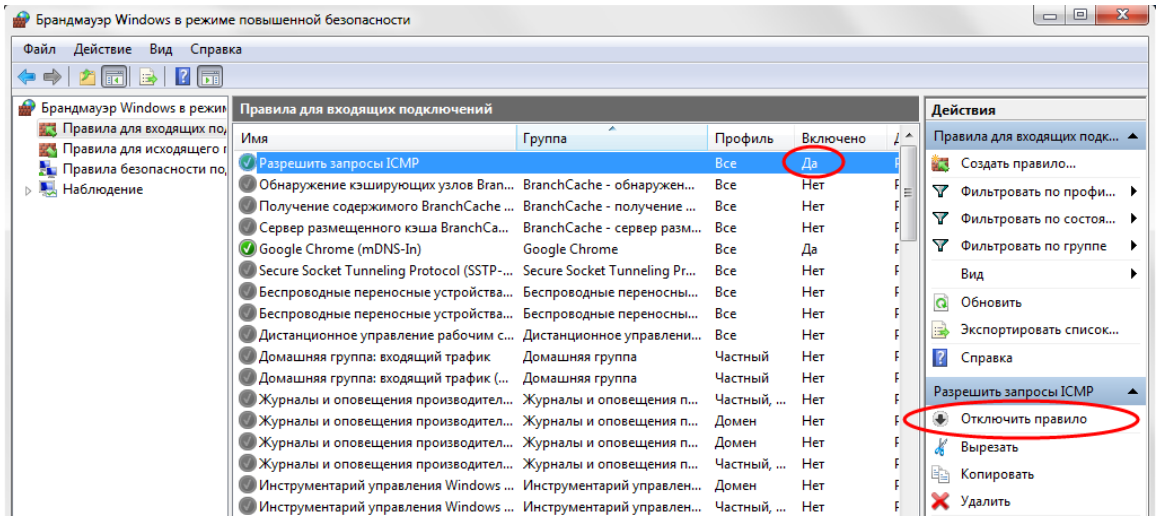
2 Отключите и удалите новое правило ICMP.

По завершении лабораторной работы необходимо отключить или удалить новое правило, созданное в шаге 1. Опция **Отключить правило** позволяет снова включить его при необходимости. Полное удаление правила навсегда удалит его из списка правил для входящих подключений.

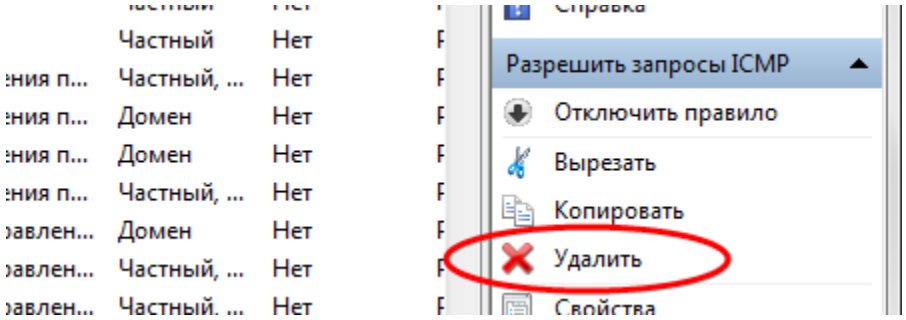
g. В левой части окна «Дополнительные настройки безопасности» выберите **Правила для входящих подключений** и найдите правило, созданное в шаге 1.



h. Чтобы отключить правило, выберите опцию **Отключить правило**. После этого название опции изменится на **Включить правило**. Правило можно включать и отключать поочередно. Состояние правила также отображается в столбце «Включено» списка правил для входящих подключений.



i. Чтобы удалить правило ICMP навсегда, нажмите **Удалить**. Если после этого потребуется разрешить запросы ICMP, правило нужно будет создать заново.



Приложение B. Требования к отчету

В отчете по контрольной работе должны содержаться:

- Задания (что делаем?)
- Результаты (снимки экрана)
- Ответы на содержащиеся в задании вопросы