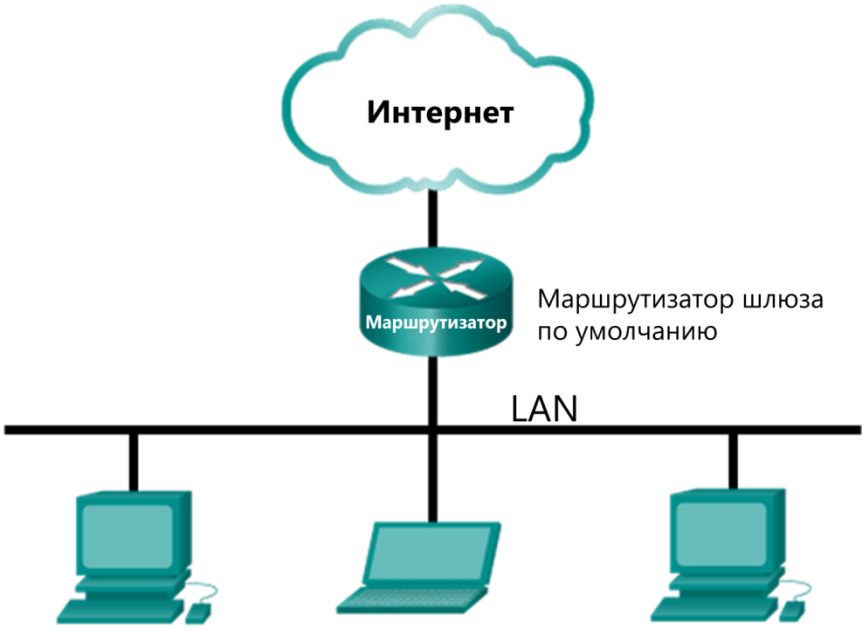
Лабораторная работа. Протокол разрешения адресов (ARP)

Топология



Цели

Часть 1. Загрузите и установите программу Wireshark

Часть 2. Сбор и анализ данных ARP в Wireshark

- Начало и остановка сбора данных трафика эхо-запросов с помощью команды ping к удалённым хостам.
- Поиск данных об IPv4- и MAC-адресах в полученных PDU.
- Анализ содержимого сообщений ARP, которыми обмениваются устройства в локальной сети.

Часть 3. Просмотр записей кэша ARP на компьютере

- Доступ к окну командной строки Windows.
- Использование команды Windows **arp** для просмотра локального кэша таблиц ARP на компьютере.

Общие сведения/сценарий

TCP/IP использует протокол разрешения адресов (ARP) для сопоставления адреса IPv4 уровня 3 с MAC-адресом уровня 2. При передаче кадра Ethernet по сети в нем должен быть указан MAC-адрес назначения. Чтобы динамически определить MAC-адрес известного места назначения, исходное устройство выполняет широковещательную рассылку ARP-запросов по сети. Устройство, для которого настроен IPv4-адрес назначения, отправляет на запрос ARP-ответ, а MAC-адрес записывается в кэш ARP.

Каждое устройство в локальной сети сохраняет собственный кэш ARP. Кэш ARP представляет собой небольшую область в ОЗУ, в которой содержатся ARP-ответы. При просмотре кэша ARP на компьютере отображается адрес IPv4 и MAC-адрес каждого устройства в локальной сети, с которым компьютер обменивался ARP-сообщениями.

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 прохождения потоков данных туда и обратно по сети анализатор выполняет сбор каждого блока данных протокола (PDU) и может расшифровать и проанализировать его содержимое согласно соответствующим спецификациям протокола.

Программа Wireshark удобна при работе с сетями и подходит для выполнения большинства лабораторных работ на курсах Cisco, когда требуется проанализировать данные и устранить неполадки. В данной лабораторной работе содержатся инструкции по загрузке и установке программы Wireshark. Воспользуйтесь ими, если программа не установлена. В этой лабораторной работе необходимо будет использовать программу Wireshark для сбора пересылаемых данных ARP в локальной сети.

Необходимые ресурсы

- 1 компьютер с Windows 10 и доступом в Интернет.
- Один или несколько дополнительных компьютеров в локальной сети для ответа на запросы **ping**. Если дополнительные компьютеры в локальной сети отсутствуют, для ответа на запросы **ping** будет использоваться адрес основного шлюза.

Часть 1: Загрузка и установка программы Wireshark

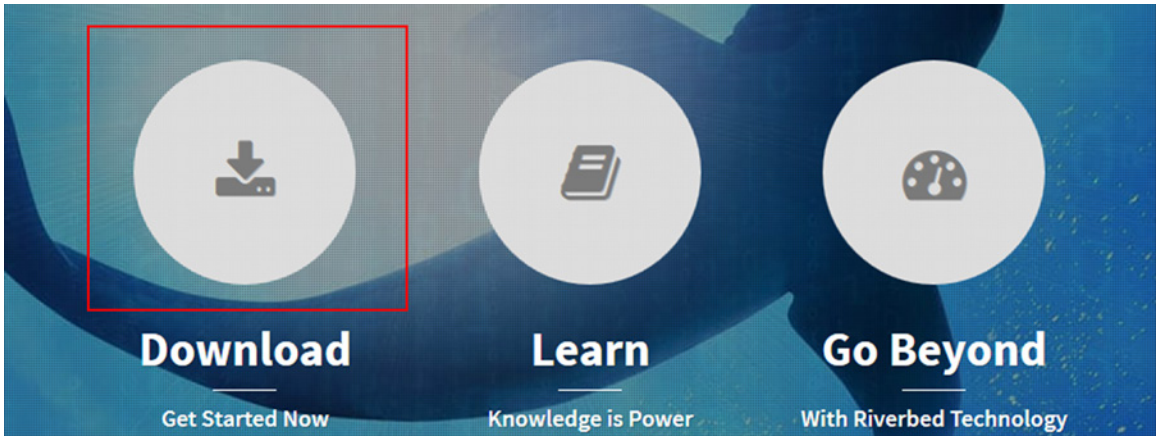
Программа Wireshark стала стандартным анализатором пакетов, используемым сетевыми инженерами. Версии этой программы с открытым исходным кодом доступны для различных операционных систем, включая Windows, Mac и Linux.

Если на компьютере уже установлена программа Wireshark, можно пропустить часть 1 и перейти сразу к части 2. Если программа Wireshark на вашем ПК не установлена, узнайте у инструктора о правилах загрузки программного обеспечения в вашем учебном заведении.

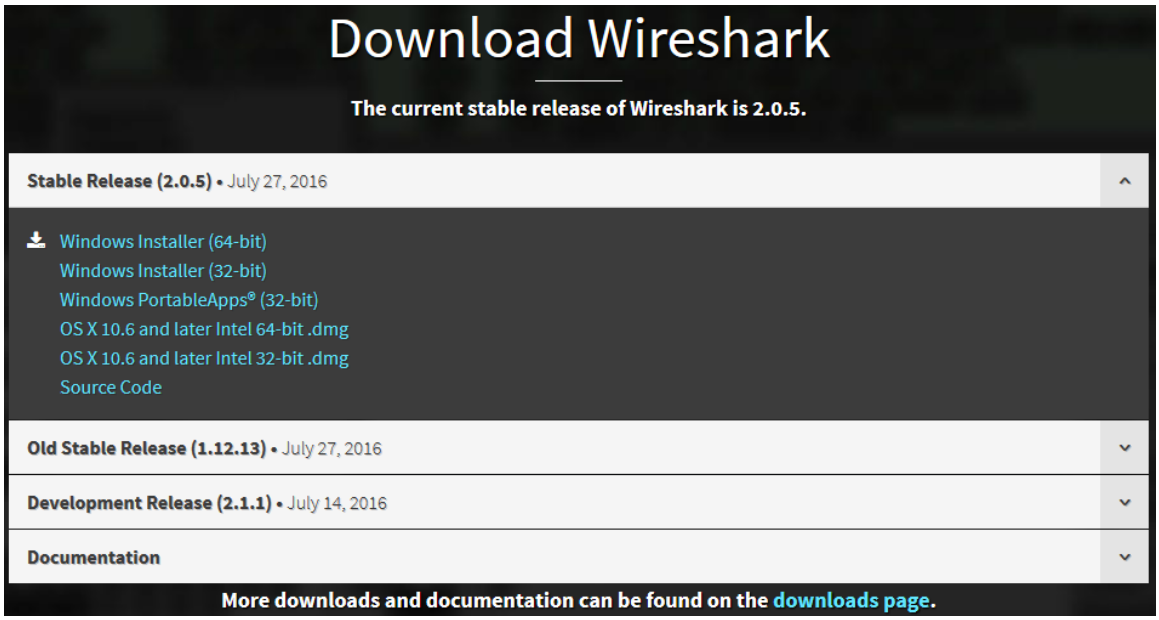
Шаг 1: Загрузите Wireshark.

a. Программу Wireshark можно загрузить по адресу www.wireshark.org.

b. Нажмите **Загрузить**.



c. Выберите версию программы в соответствии с архитектурой и операционной системой вашего ПК. Например, если у вас 64-разрядный ПК с ОС Windows, выберите **Windows Installer (64-bit)**.

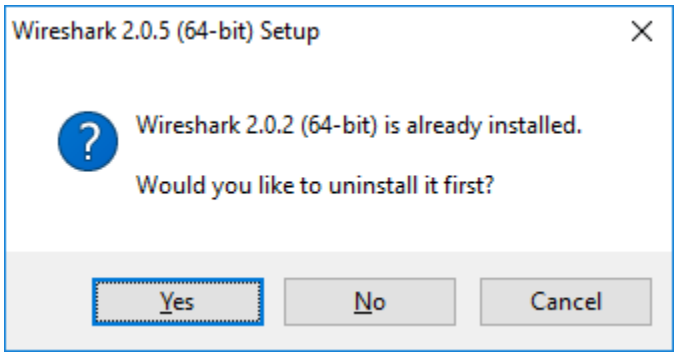


d. Сразу после этого начнется загрузка. При появлении запроса выберите **Сохранить файл**. Местонахождение загруженного файла зависит от браузера и операционной системы, которыми вы пользуетесь. При использовании Windows местоположением по умолчанию является папка **Загрузки**.

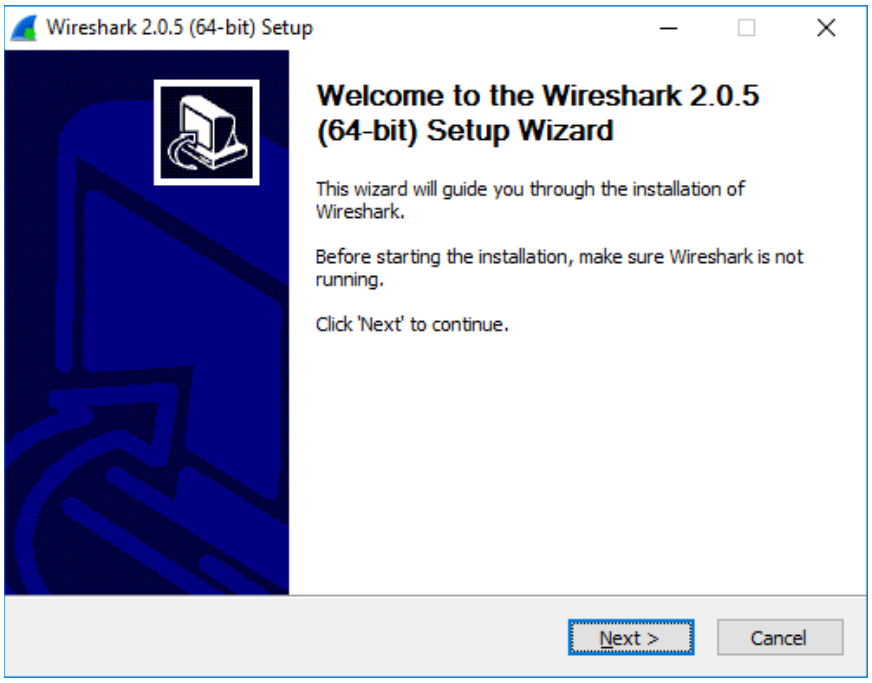
Шаг 2: Установите программу Wireshark.

a. Имя загруженного файла: **Wireshark-win64-x.x.x.exe**, где **x** обозначает номер версии. Дважды нажмите на файл, чтобы начать установку. В данном примере используется версия 2.0.5.

b. Ответьте на все сообщения о безопасности, которые появятся на экране. Если на вашем ПК уже имеется копия Wireshark, перед установкой программы появится запрос на удаление прежней версии. Рекомендуется удалить старую версию программы перед установкой новой. Чтобы удалить предыдущую версию Wireshark, щелкните **Да**.



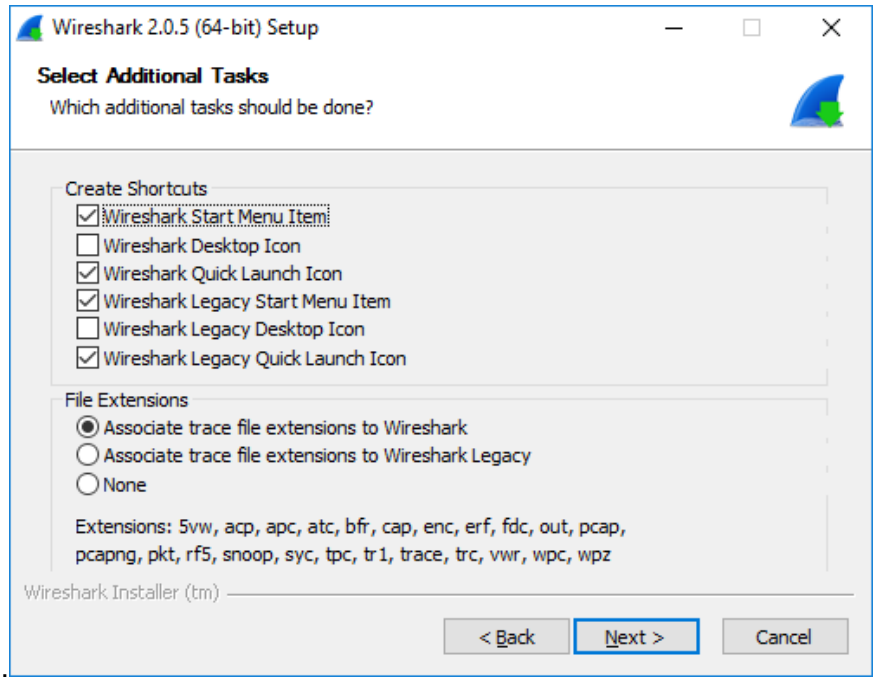
c. Если программа Wireshark устанавливается впервые или предыдущая версия была удалена, откроется мастер установки программы Wireshark. Нажмите **Next** (Далее).



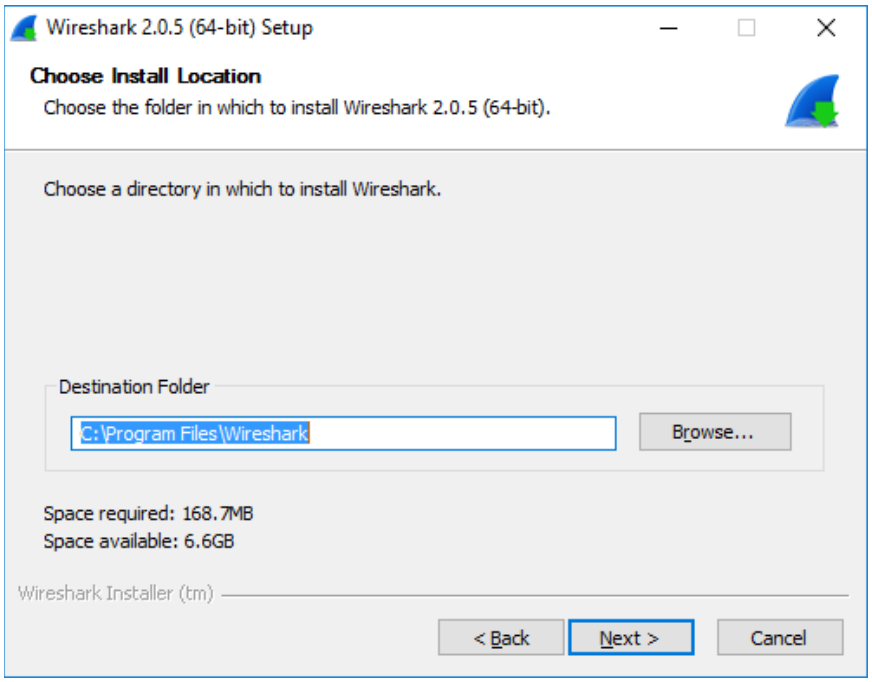
d. Выполните инструкции по установке. При отображении окна лицензионного соглашения щелкните **Принимаю**.

e. При выборе компонентов оставьте настройки по умолчанию и нажмите кнопку **Next** (Далее).

f. Выберите желаемые ярлыки и нажмите кнопку **Далее**.

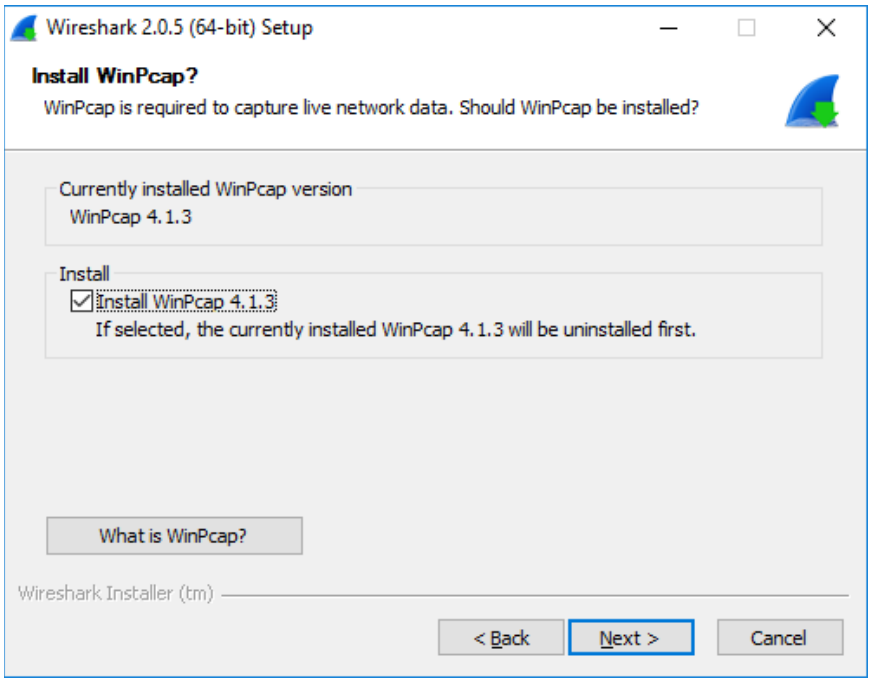


g. Если не хватает места на диске, адрес установки Wireshark можно изменить. Однако рекомендуется оставить адрес, указанный по умолчанию.



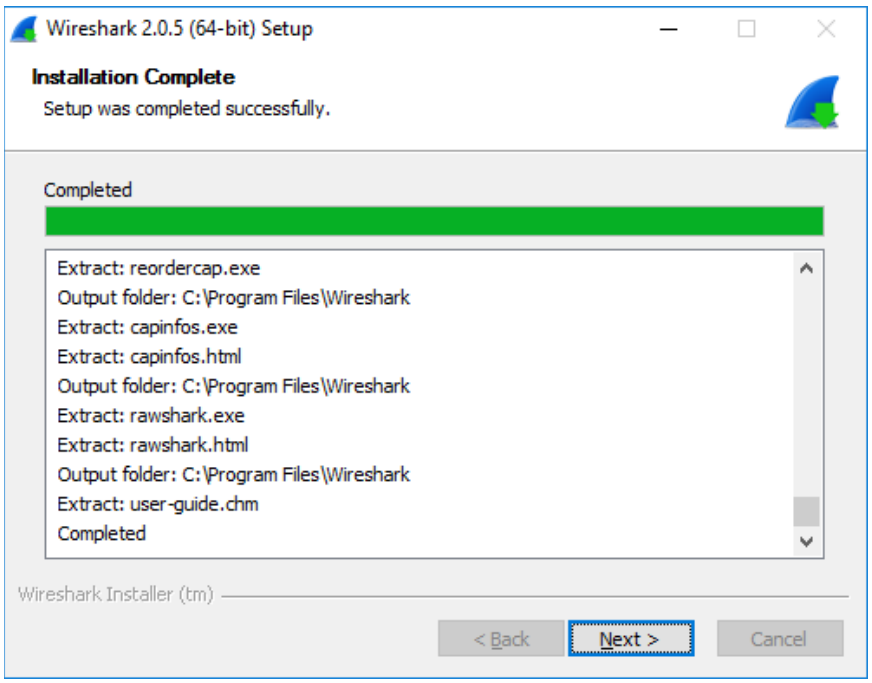
h. Для сбора сетевых данных на ваш ПК необходимо установить программу WinPcap. Если она уже установлена, флажок установки будет снят. Если на компьютере установлена более ранняя версия WinPcap по сравнению с версией, прилагаемой к Wireshark, рекомендуется разрешить установку более поздней версии. Для этого установите флажок **Установить WinPcap x.x.x** (где x.x.x обозначает номер версии).

Если установка прошла успешно, закройте мастер установки WinPcap.

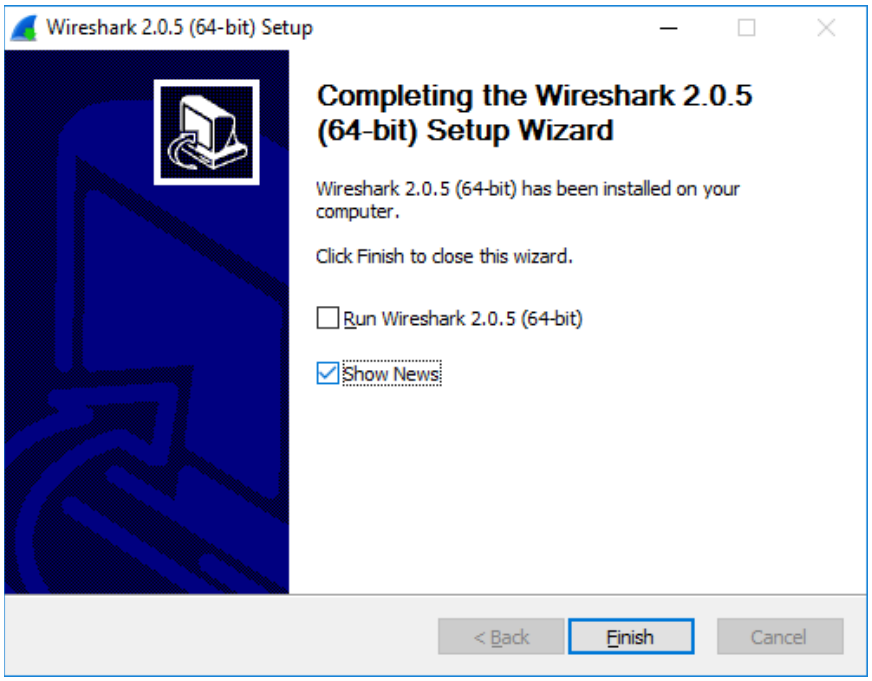


Примечание. Может быть предложено установить USBPcap. Установка USBPcap не является обязательной.

i. После этого начнется установка программы Wireshark. Статус установки будет отображаться в отдельном окне. После завершения установки щелкните **Далее**.



j. Чтобы завершить процесс установки Wireshark, щелкните **Готово**.



Часть 2: Сбор и анализ локальных данных ARP с помощью Wireshark

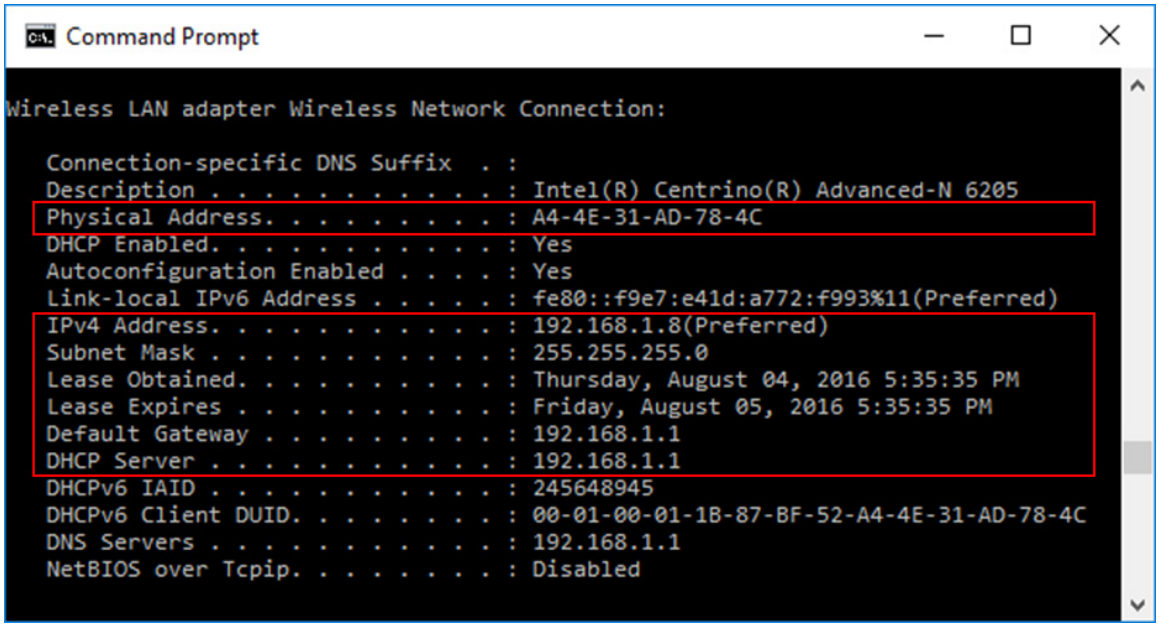
В части 2 данной лабораторной работы необходимо будет отправить ping-запрос на другой компьютер в локальной сети и выполнить сбор ARP-запросов и ответов с помощью Wireshark. Кроме того, вам нужно найти необходимую информацию в собранных кадрах. Этот анализ поможет понять, как используются заголовки пакетов для передачи данных по месту назначения.

Шаг 1: Определите адреса интерфейсов вашего ПК.

Для выполнения этой лабораторной работы необходимо будет получить адрес IPv4 и MAC-адрес компьютера.

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

b. Обратите внимание на сетевой адаптер, используемый компьютером для доступа к сети. Запишите адрес IPv4 и MAC-адрес интерфейса компьютера (физический адрес).



c. Узнайте у участника группы адрес IPv4 его компьютера и сообщите ему адрес IPv4 вашего компьютера. но пока что не сообщайте им свой MAC-адрес.

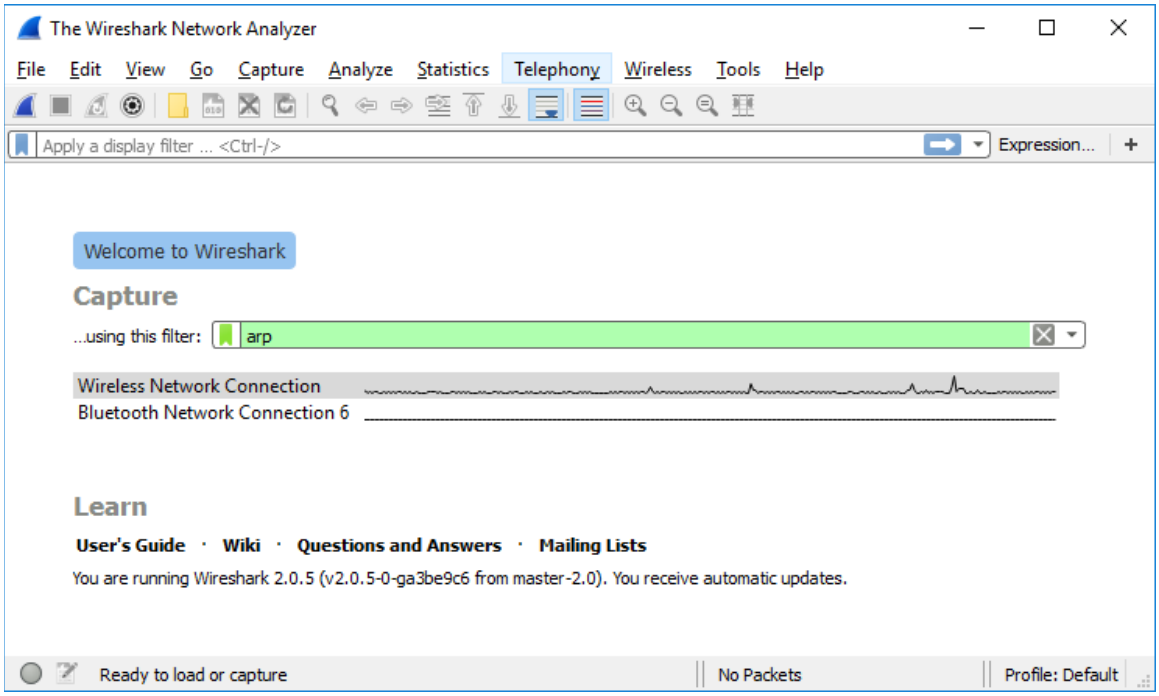
Запишите адреса IPv4 основного шлюза и других компьютеров в локальной сети.

Шаг 2: Запустите программу Wireshark и начните сбор данных.

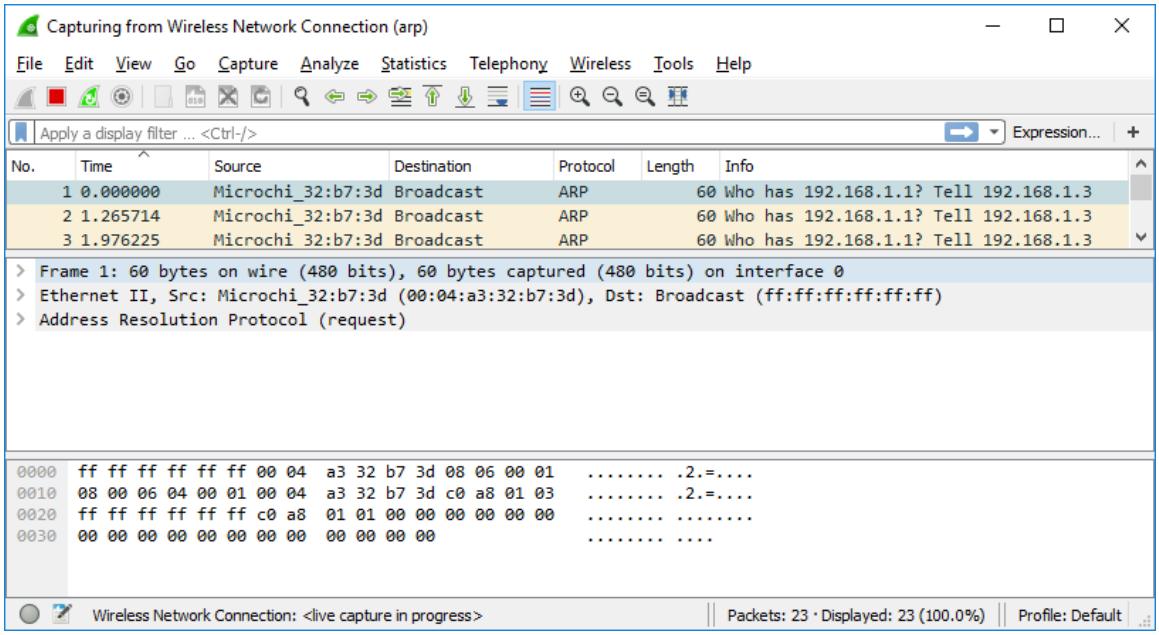
a. На вашем компьютере нажмите кнопку **Пуск** и введите **Wireshark**. Щелкните **Приложение Wireshark для настольных систем**, когда данный вариант появится в окне результатов поиска.

Примечание. В результате установки Wireshark также может быть доступна устаревшая версия Wireshark. Эта версия использует старый, но широко известный графический интерфейс пользователя Wireshark. При описании последующей части лабораторной работы используется более поздняя версия графического интерфейса пользователя приложения для настольных систем.

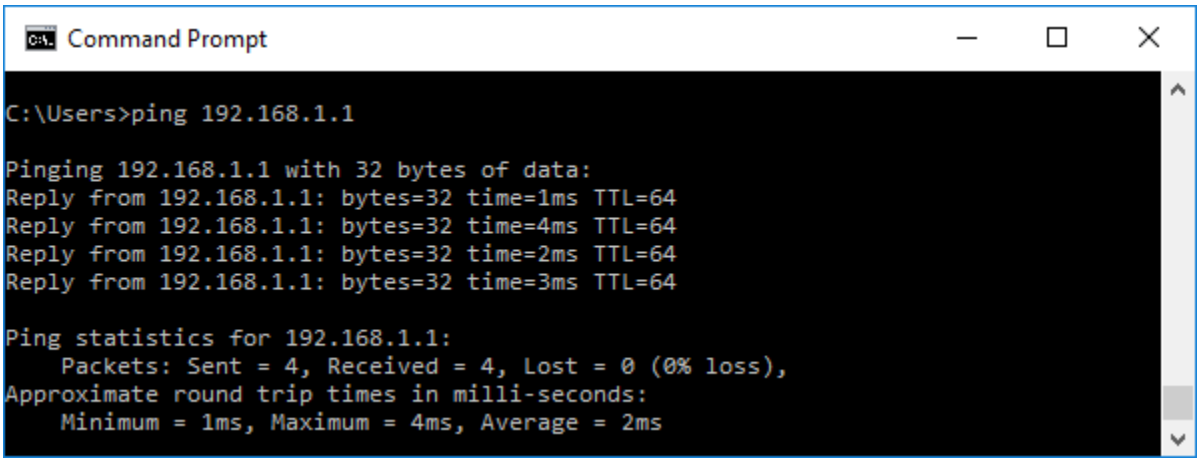
b. После запуска Wireshark выберите сетевой интерфейс, определенный с помощью команды **ipconfig**. В поле фильтра введите **arp**. При выборе этого варианта выполняется настройка Wireshark для отображения только пакетов, являющихся частью пересылаемых данных ARP между устройствами в локальной сети.



c. После выбора правильного интерфейса и ввода информации фильтра щелкните **Start capturing packets**, чтобы начать сбор данных. В верхней части окна программы Wireshark начнет прокручиваться информация. Каждая строка представляет сообщение, пересылаемое между устройством-источником и устройством-получателем в сети.



d. Откройте окно командной строки. С помощью команды **ping** проверьте подключение к адресу основного шлюза, определенному в части 2 на шаге 1c.



e. Отправьте ping-запрос на адреса IPv4 компьютеров локальной сети, предоставленные вам участниками группы.

Примечание. Если компьютеры других учащихся не отвечают на ваши эхо-запросы, это может быть вызвано тем, что брандмауэры их компьютеров блокируют эти запросы. Если необходимо отключить брандмауэр компьютера, обратитесь за помощью к инструктору.

f. Чтобы остановить сбор данных, щелкните **Stop capturing packets**  на панели инструментов.

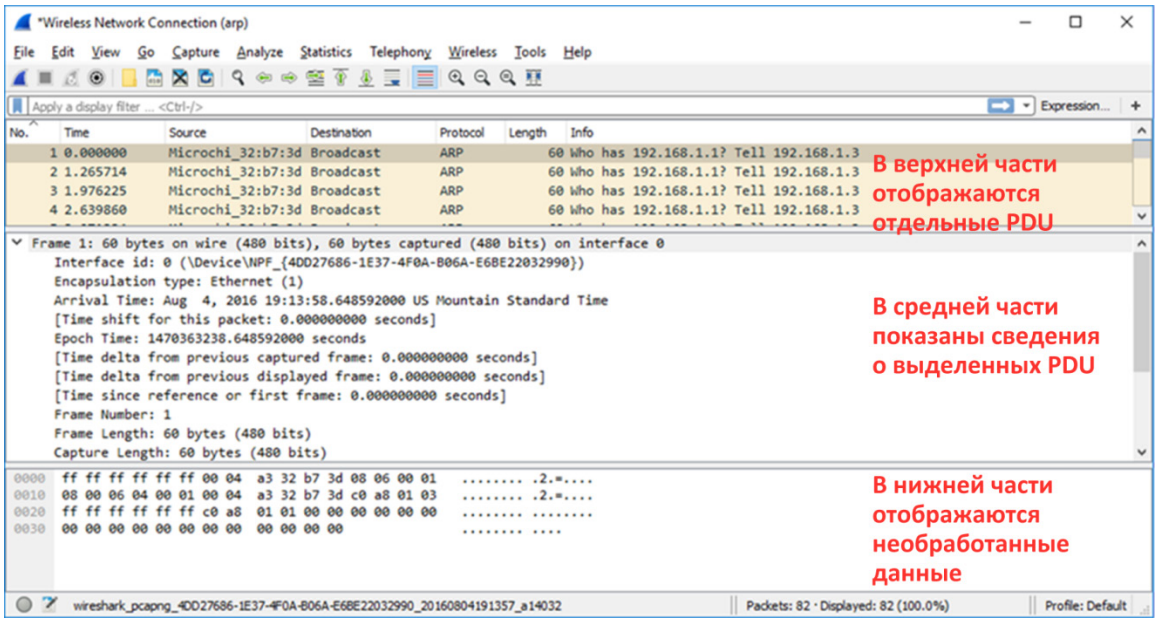
Шаг 3: Изучите полученные данные.

На шаге 3 проверьте данные, полученные с помощью отправки запросов **ping** на компьютер участника вашей группы. Данные Wireshark отображаются в трех частях окна программы.

1) В верхней части отображается список собранных кадров PDU со сводной информацией указанного в списке пакета IPv4.

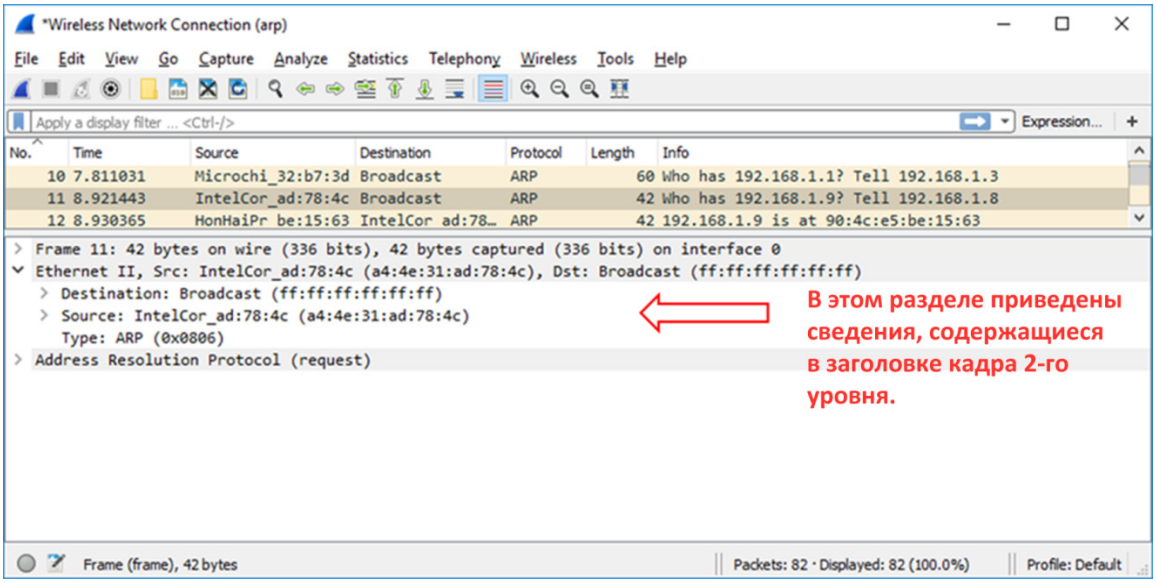
2) В средней части приведены сведения PDU для кадра, выбранного в верхней части экрана, и полученный кадр PDU разделен уровнями протокола.

3) В нижней части показаны необработанные данные каждого уровня. Необработанные данные отображаются как в шестнадцатеричном, так и в десятичном форматах.



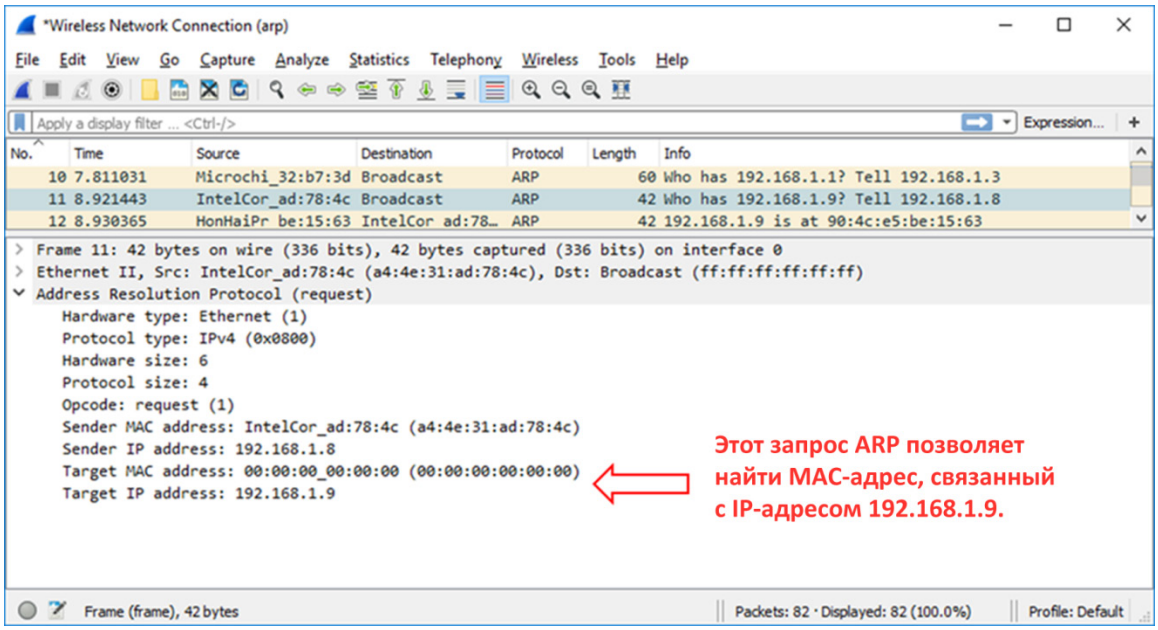
a. Щелкните один из кадров ARP в верхней части, для которого в качестве адреса источника в кадре указан MAC-адрес вашего компьютера, и выполните его широковещательную рассылку в качестве места назначения кадра.

b. Не меняя выбор кадра PDU в верхнем разделе окна, перейдите в средний раздел. Щелкните стрелку слева от строки Ethernet II, чтобы просмотреть MAC-адреса источника и назначения.



Совпадает ли MAC-адрес источника с интерфейсом вашего компьютера?

c. Щелкните стрелку слева от строки «Протокол разрешения адресов (запрос)», чтобы просмотреть содержимое ARP-запроса.



Шаг 4: Найдите кадр ARP-ответа, соответствующего выделенному ARP-запросу.

a. С помощью целевого адреса IPv4, указанного в ARP-запросе, найдите кадр ARP-ответа в верхней части экрана сбора Wireshark.

Какой адрес IPv4 целевого устройства указан в вашем ARP-запросе?

b. Выделите кадр ответа в верхней части выходных данных программы Wireshark. Может потребоваться прокрутить окно для поиска кадра ответа, соответствующего целевому адресу IPv4, который был определен на предыдущем шаге. В средней части экрана разверните строки протокола ARP (ответ) и Ethernet II.

Является ли ответный кадр ARP кадром широковещательной рассылки?

Какой MAC-адрес назначения у этого кадра?

Это MAC-адрес вашего компьютера?

Какой MAC-адрес является источником кадра?

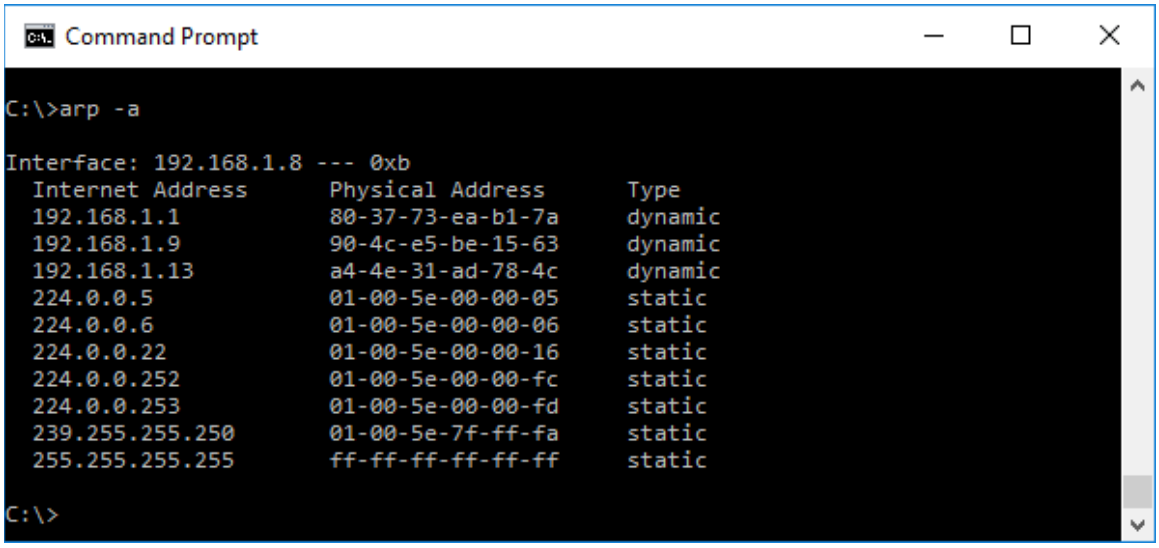
c. Совместно с другим участником группы убедитесь, что этот MAC-адрес совпадает с MAC-адресом его компьютера.

Часть 3: Проверьте записи в кэше ARP на компьютере.

После получения компьютером ответа ARP связь MAC-адреса с адресом IPv4 будет сохранена в кэш-памяти на компьютере. Эти записи будут храниться в памяти в течение короткого периода времени (от 15 до 45 секунд), затем, если они не использовались в течение этого времени, они будут удалены из кэша.

Шаг 1: Просмотрите записи кэша ARP на компьютере Windows.

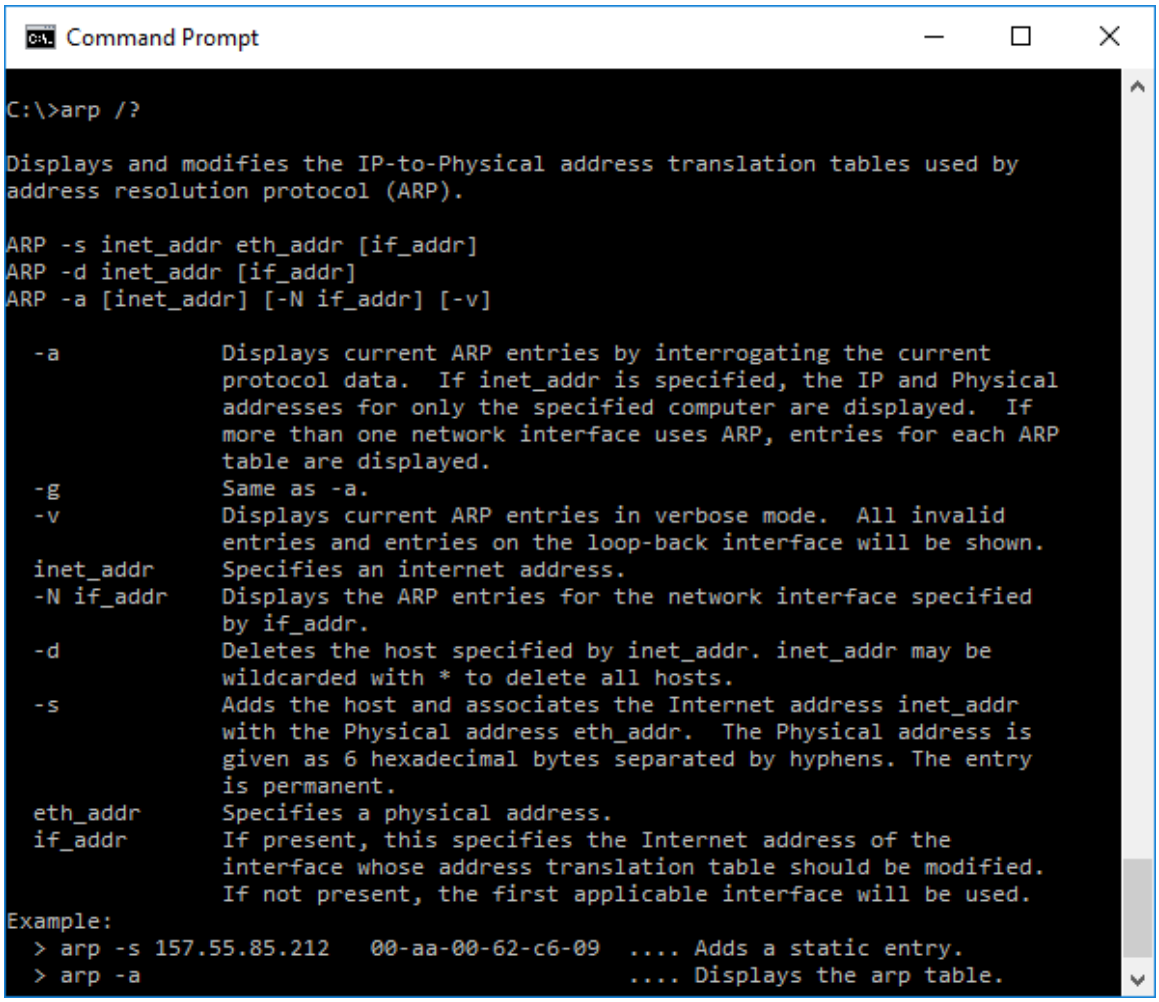
a. Откройте на компьютере окно с командной строкой. В командной строке введите **arp –a** и нажмите Enter.



Показанные результаты выполнения команды **arp –a** будут содержать записи, сохраненные в кэше на компьютере. В приведенном примере на компьютере имеются записи для основного шлюза (192.168.1.1) и для двух компьютеров, находящихся в той же локальной сети (192.168.1.9 и 192.168.1.13).

Каков результат выполнения команды **arp –a** на вашем компьютере?

b. Команда **arp** на компьютере Windows имеет другие возможности. Введите **arp /?** в командной строке и нажмите Enter. Параметры команды **arp** позволяют при необходимости просматривать, добавлять и удалять записи в таблице ARP.



Какой параметр позволяет удалить запись из кэша ARP?

Каков будет результат выполнения **arp –d *?

Вопросы для повторения

1. В чем заключается преимущество сохранения в памяти записей кэша ARP на исходном компьютере?

2. Если адрес IPv4 назначения не находится в той же сети, что и исходный хост, какой MAC-адрес будет использоваться в качестве целевого MAC-адреса назначения в кадре?