Санкт-Петербургский государственный политехнический университет

Институт компьютерных наук и кибербезопасности

Высшая школа компьютерных технологий и информационных систем

**Отчет по лабораторной работе №5**

**по курсу «Технологии компьютерный сетей»**

«Wireshark: DHCP & Ethernet\_ARP»

**Работу выполнил студент группы №5130901/10203:**

Алексеев Лев Сергеевич

Подпись:

**Работу принял преподаватель:**

Богач Наталья Владимировна

Подпись:

Санкт-Петербург

2024

**Wireshark: DHCP**

В этой лабораторной работе мы бегло рассмотрим протокол DHCP. Протокол DHCP исследован в разделе 4.4.2 книги. Как мы помним, протокол DHCP активно применяется в корпоративных, университетских и домашних проводных и беспроводных локальных сетях. DHCP обеспечивает динамическое присваивание IP-адресов хостам (а также конфигурирование другой информации о состоянии сети). Эта лабораторная работа краткая, так как мы просто исследуем DHCP-пакеты, захваченные хостом.



Рис. 1. Работа последовательности команд ipconfig.

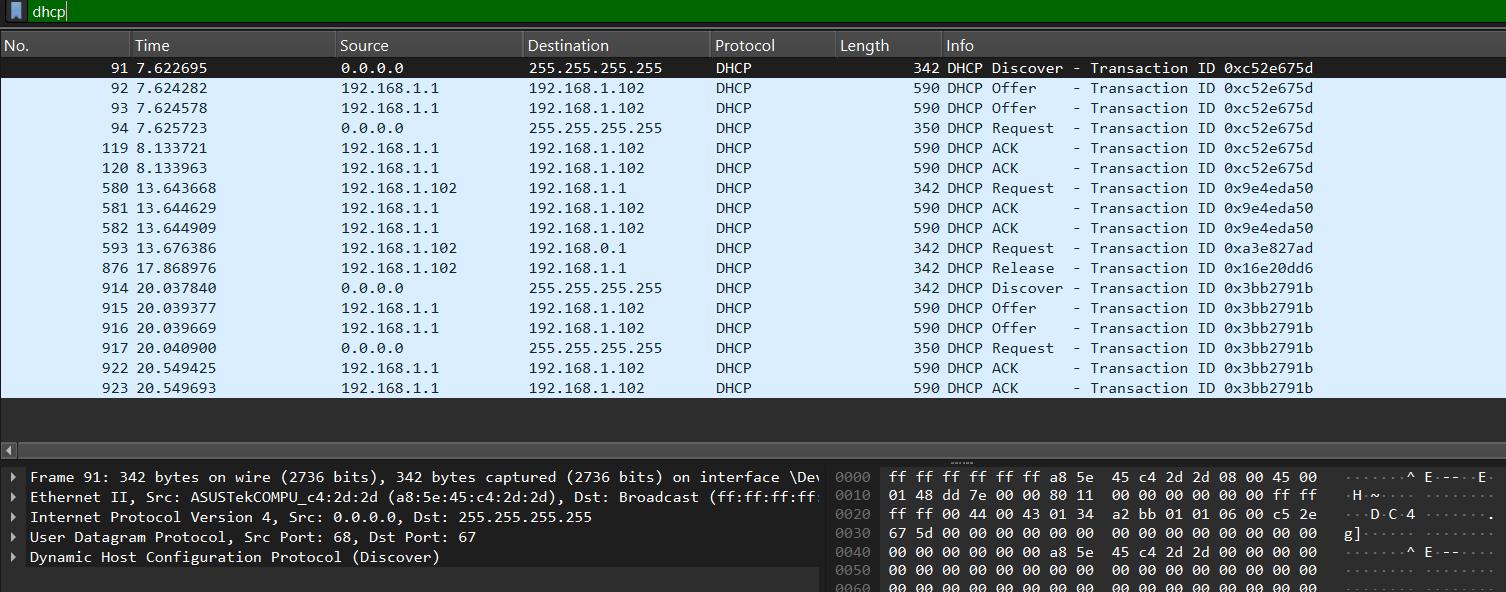
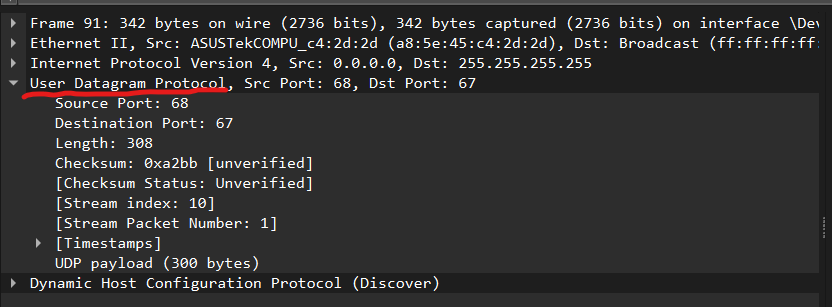


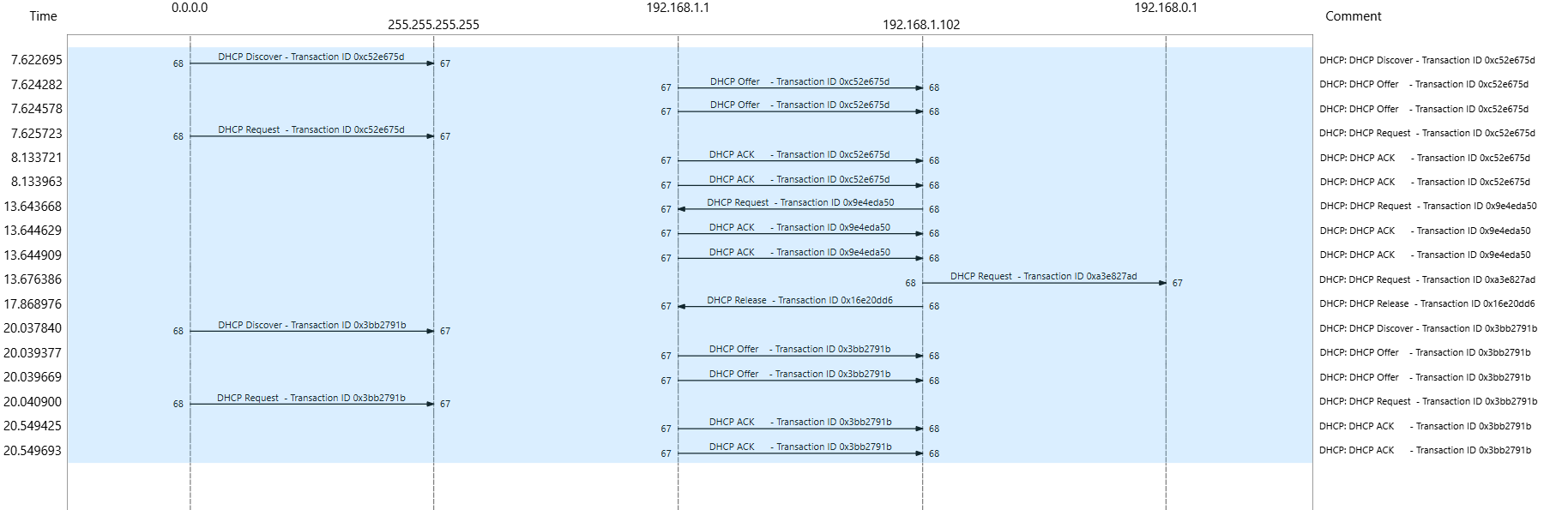
Рис. 2. Окно Wireshark с перехваченными пакетами DHCP.

1. Поверх какого протокола посылаются сообщения DHCP – UDP или TCP?

DHCP-сообщения пересылаются по UDP (протоколу пользовательских дейтаграмм).

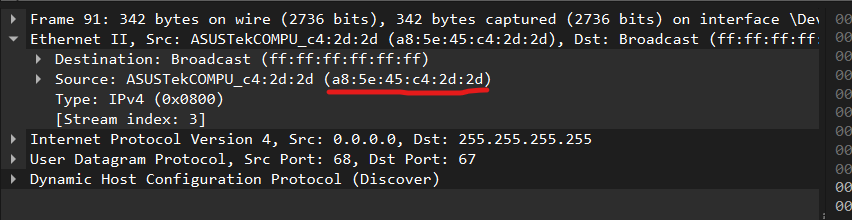


1. Начертите временную диаграмму, иллюстрирующую последовательность обмена первыми четырьмя пакетами Discover/Offer/Request/ACK DHCP между клиентом и сервером. Для каждого пакета укажите номера начального и конечного портов. Совпадают ли эти номера с теми, что были даны в примере к заданию из этой лабораторной работы?



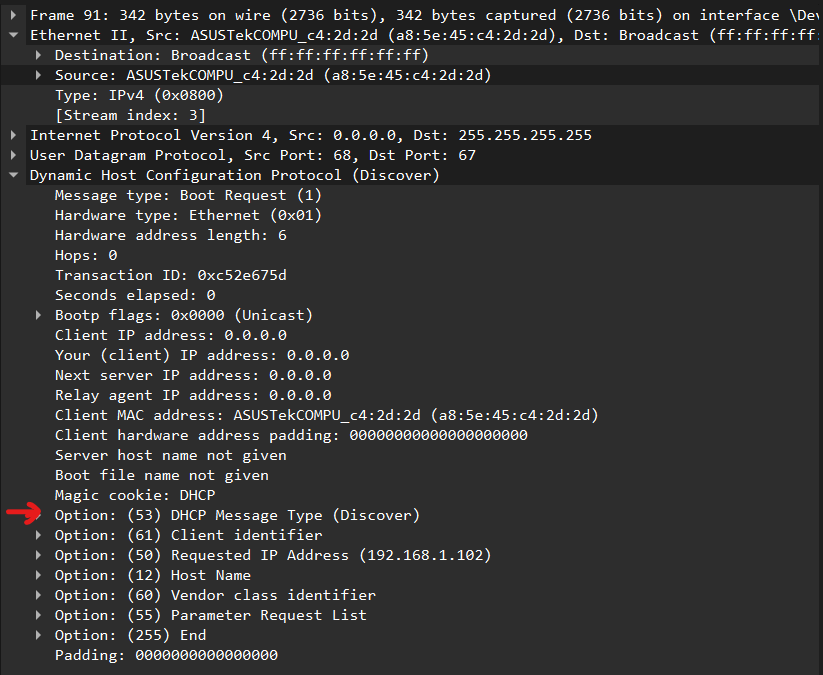
Порты совпадают, 67 и 68 порты.

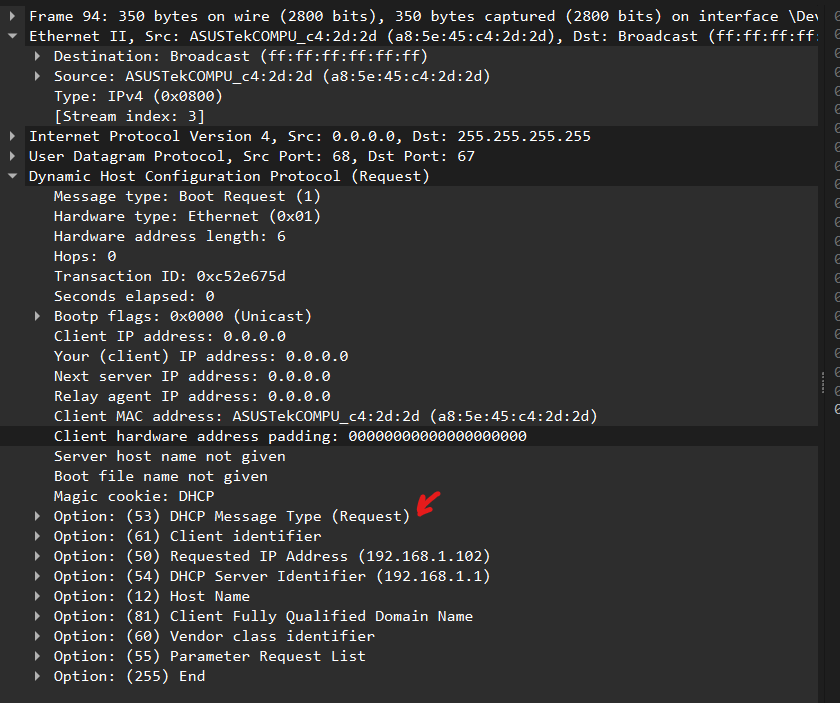
1. Каков адрес канального уровня (т.е., Ethernet-адрес) у вашего хоста?



Моя рабочая станция имеет адрес канального уровня a8:5e:45:c4:2d:2d.

1. Какие значения в сообщении обнаружения DHCP отличают это сообщение от сообщения с DHCP-запросом?





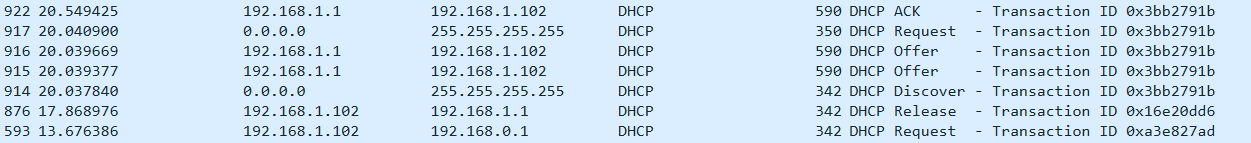
Значения, отличающие сообщение обнаружения (Discover) от сообщения запроса (Request): Option 53: DHCP Message Type.

1. Каково значение транзакционного идентификатора (Transaction-ID) в каждом из первых четырех (Discover/Offer/Request/ACK) DHCP-сообщений? Каковы значения Transaction-ID во втором наборе (Request/ACK) DHCP-сообщений? Опишите назначение поля Transaction-ID.

Значение транзакционного идентификатора (Transaction ID) равно 0xc52e675d. Второй транзакционный идентификатор – 0x9e4eda50. Транзакционный идентификатор используется для того, чтобы DHCP-сервер мог в процессе запрашивания различать разные клиентские запросы.

1. Хост использует DHCP-протокол, в частности, для получения IP-адреса. Но IP-адрес хоста остается неподтвержденным до завершения обмена первыми четырьмя сообщениями! Если IP-адрес не установлен до завершения обмена первыми четырьмя сообщениями, то какие значения используются в IP-дейтаграммах при обмене этими сообщениями? Для каждого из четырех DHCP-сообщений (Discover/Offer/Request/ACK DHCP) укажите исходный и конечный IP-адреса, передаваемые в инкапсулирующей IP-дейтаграмме.

В качестве адреса назначения и DHCP-сервер, и клиент используют адрес 255.255.255.255. Исходный IP-адрес у клиента – 0.0.0.0, а сервер использует в качестве исходного свой актуальный IP-адрес

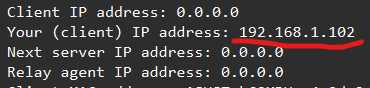


1. Каков IP-адрес вашего DHCP-сервера?

IP-адрес DHCP-сервера – 192.168.1.1.

1. Какой IP-адрес DHCP-сервер предлагает вашему хосту в сообщении DHCP Offer? Укажите, какое DHCP-сообщение содержит предложенный DHCP-адрес.

DHCP-сервер предложил моей клиентской машине IP-адрес 192.168.1.102. В DHCP-сообщении DHCP Message Type = DHCP Offer содержался предложенный IP-адрес



1. На снимке, приведенном в этом задании для примера, отсутствует ретранслирующий агент между хостом и DHCP-сервером. Какие значения в трассе указывают на отсутствие ретранслирующего агента? Есть ли ретранслирующий агент в вашем эксперименте? Если да – каков IP-адрес этого агента?

IP-адрес ретранслирующего агента» равен 0.0.0.0; это означает, что в данном случае не используется DHCP-ретрансляция. Действительно, в моем эксперименте ретранслирующий агент использовался.

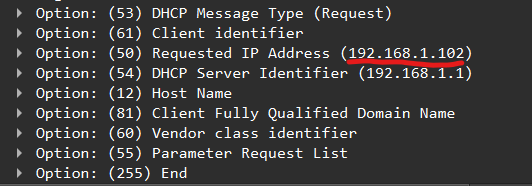
**Relay agent IP address: 0.0.0.0**

1. Опишите назначение строк с указанием маршрутизатора и маски подсети в сообщении с DHCP-предложением.

Строка с указанием маршрутизатора сообщает клиенту, каков должен быть его шлюз, используемый по умолчанию. Строка с маской подсети указывает клиенту, с какой маской подсети он должен работать.

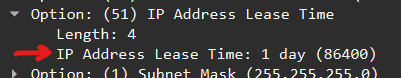
1. В файле трассы DHCP, упомянутом в сноске 2, DHCP-сервер предлагает клиенту конкретный IP-адрес (также см. вопрос 8). Принимает ли клиент этот IP-адрес в своем ответе на первое полученное им серверное сообщение OFFER? Где в клиентском сообщении отклика (RESPONSE) находится запрошенный адрес клиента?

В моем эксперименте хост запрашивает предложенный IP-адрес в сообщении с DHCP-запросом



1. Объясните назначение срока аренды IP-адреса. Какова длительность срока аренды в вашем эксперименте?

Время аренды – это срок, на который DHCP-сервер выдает клиенту IP-адрес. В течение этого времени DHCP-сервер не выдаст другому клиенту сданный в аренду адрес, если сам клиент не высвободит этот адрес. Когда время аренды истечет, IP-адрес может быть повторно использован DHCP-сервером – то есть, передан другому клиенту. В моем эксперименте время аренды составляет 1 день.

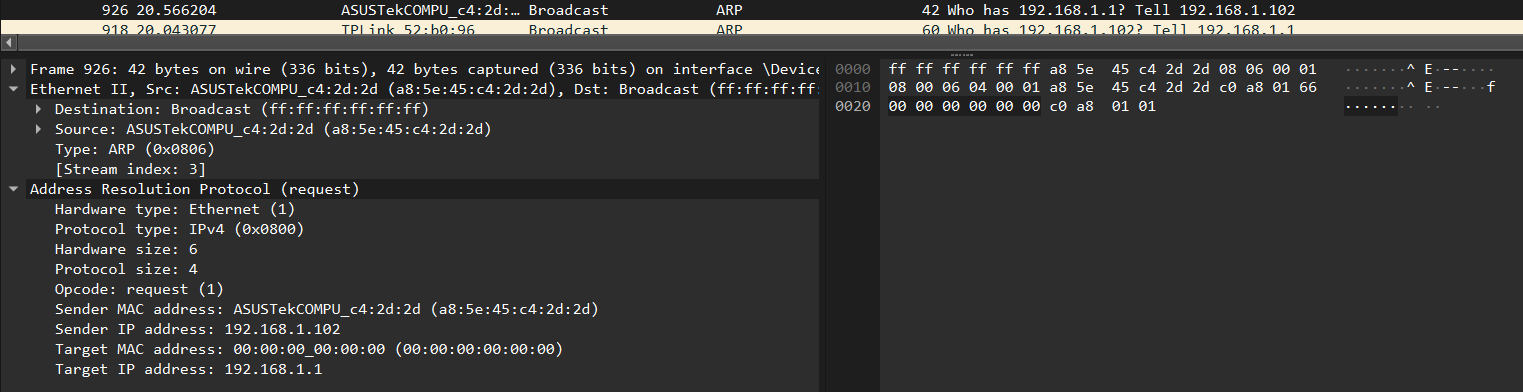


1. Каково назначение высвобождающего сообщения DHCP? Дает ли DHCP-сервер уведомление о получении клиентского DHCP-запроса? Что произойдет, если клиентское DHCP-сообщение о высвобождении адреса потеряется?

Клиент отсылает DHCP-сообщение Release, чтобы прекратить аренду IP-адреса, выданного ему DHCP-сервером. В ответ на сообщение DHCP Release DHCP-сервер ничего не посылает клиенту. Если сообщение DHCP Release от клиента будет потеряно, то сервер дождется окончания времени аренды, после чего сможет передать этот IP-адрес другому клиенту.

1. Сбросьте фильтр bootp в окне Wireshark. Были ли отправлены или получены какие-либо ARP-пакеты на этапе обмена первыми четырьмя пакетами DHCP? Если так – объясните назначение этих ARP-пакетов.

Да, DHCP-сервер выполняет ARP-запросы. Прежде, чем предложить клиенту IP-адрес, DHCP-сервер делает ARP-запрос к предложенному IP-адресу, чтобы убедиться, что этот IP-адрес уже не используется другой рабочей станцией.



**Wireshark: Ethernet и ARP**

В этой лабораторной работе мы исследуем протоколы Ethernet и ARP. В стандарте RFC 826 (ietf.org/rfc/rfc826.txt) описаны всевозможные тонкости протокола ARP, используемого IP-устройствами для определения IP-адреса удаленного интерфейса, чей Ethernet-адрес уже известен.

**Захват и анализ Ethernet-кадров**

1. Каков 48-разрядный Ethernet-адрес вашего компьютера?

Ethernet-адрес моего компьютера - Source: ASUSTekCOMPU\_c4:2d:2d (a8:5e:45:c4:2d:2d)

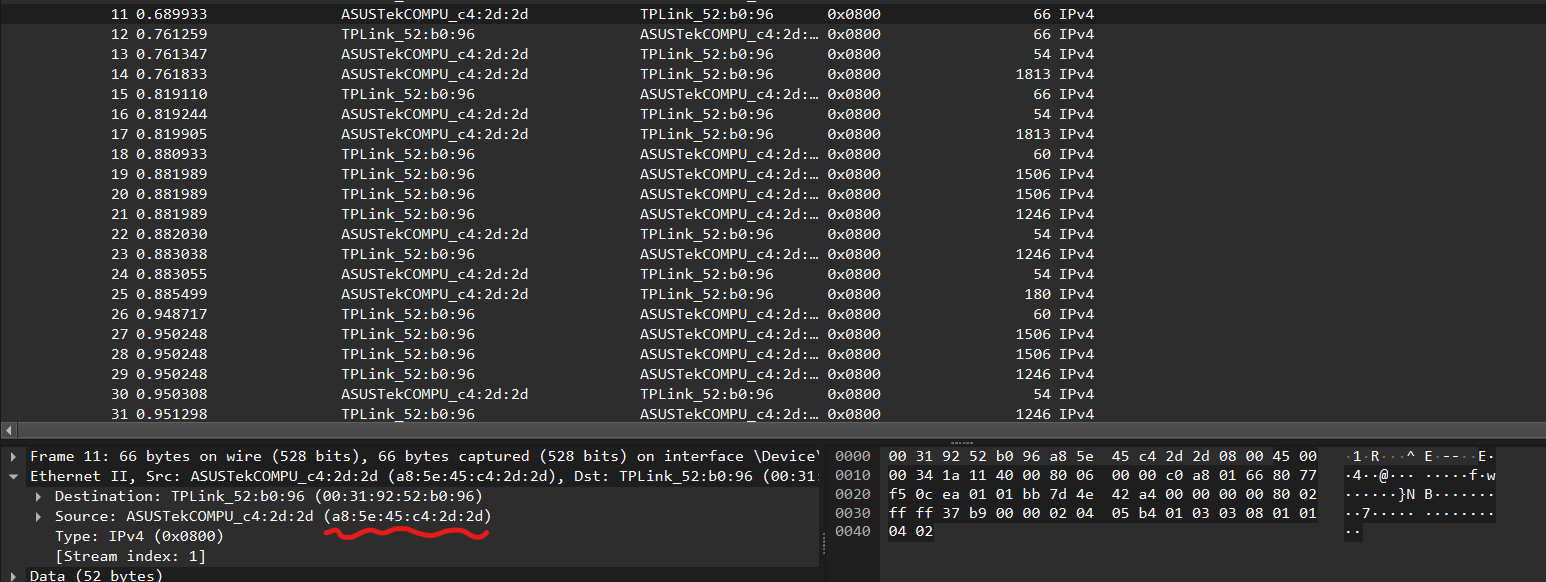


Рис. 1. Ethernet-кадр, в котором находится HTTP-запрос GET.

1. Каков 48-разрядный адрес назначения в Ethernet-кадре? Соответствует ли этот Ethernet-адрес gaia.cs.umass.edu? (Подсказка: правильный ответ нет). Какое устройство имеет такое значение Ethernet-адреса? [Примечание: это важный вопрос, причем иногда отвечают на него неверно. Перечитайте раздел «Передача дейтаграммы узлу за пределы подсети» главы 5 книги и убедитесь, что понимаете правильный ответ.]

Адрес назначения b0:4e:26:a7:6c:75 не является Ethernet-адресом с gaia.cs.umass.edu. Это адрес моего маршрутизатора TpLink, с которого начинается канал для выхода из подсети.

1. Задайте шестнадцатеричное значение для двухбайтового поля с типом кадра. Какому вышестоящему протоколу оно соответствует?

Шестнадцатеричное значение поля с типом кадра равно 0x0800. Оно соответствует протоколу IP (зафиксированный здесь тип кадра указывает, что следующий уровень выше IP – то есть, тот уровень, на который будет передаваться полезная нагрузка Ethernet-кадра – это TCP).

1. Через сколько байт после самого начала Ethernet-кадра в этом кадре идет ASCII-символ G из слова GET? Далее ответьте на следующие вопросы, ориентируясь на содержимое Ethernet-кадра, в котором находится первый байт сообщения с HTTP-откликом.

ASCII-символ G из слова GET идет через 52 байта после начала Ethernet-кадра. До начала HTTP-данных успевают пройти 14 B Ethernet-кадра, а затем 20 байт IP-заголовка и 20 байт TCP-заголовка.

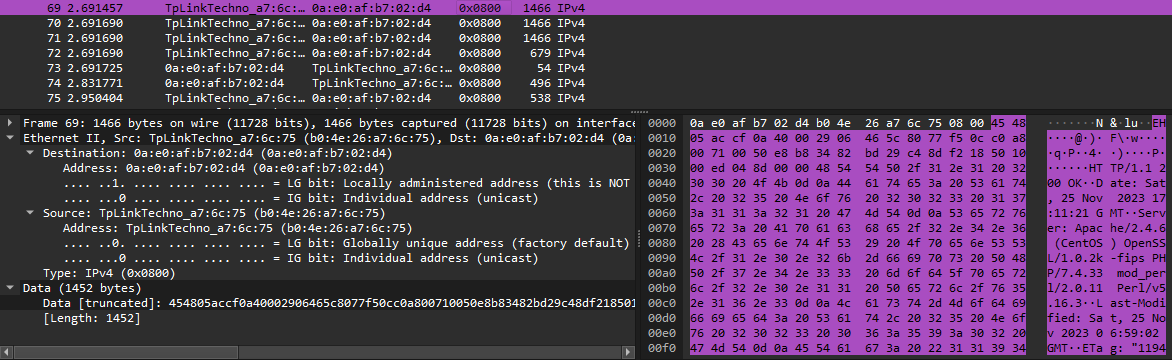


Рис. 2. Ethernet-кадр, в котором находится HTTP-отклик OK.

1. Каково значение исходного Ethernet-адреса? Это адрес вашего компьютера или хоста gaia.cs.umass.edu? (Подсказка: правильный ответ нет). Какое устройство имеет такой Ethernet-адрес?

Исходный адрес b0:4e:26:a7:6c:75 не является ни Ethernet-адресом с gaia.cs.umass.edu, ни адрес моего компьютера. Это адрес моего маршрутизатора TpLink, используемый для входа в подсеть.

1. Каков адрес назначения в этом Ethernet-кадре? Это Ethernet-адрес вашего компьютера?

Адрес назначения – a8:5e:45:c4:2d:2d. Это адрес моего компьютера.

1. Дайте шестнадцатеричное значение для двухбайтового поля с типом кадра. Какому вышестоящему протоколу оно соответствует?

Шестнадцатеричное значение для двухбайтового поля с типом кадра равно 0x0800. Это значение соответствует протоколу IP.

1. Через сколько байт после самого начала Ethernet-кадра в этом кадре идет ASCII-символ O из слова OK (то есть, код отклика HTTP)?

ASCII-символ O из слова OK идет через 52 байта после начала Ethernet-кадра. Опять же, до начала HTTP-данных успевают пройти 14 байт Ethernet-кадра, а затем 20 байт IP-заголовка и 20 байт TCP-заголовка.

**ARP-кэширование**

Как мы помним, протокол ARP обычно поддерживает на компьютере кэш пар трансляции IP-адресов в Ethernet-адреса. Команда arp (и в MS-DOS, и в Linux/Unix) применяется для просмотра содержимого кэша и манипуляций с ним. Поскольку команда arp и протокол ARP являются одноименными, их легко перепутать. Команда arp применяется для анализа содержимого кэша ARP и манипуляций с ним, а протокол ARP определяет формат и значение получаемых и отправляемых сообщений, а также регламентирует действия, выполняемые при передаче и приеме сообщений.

1. Выпишите содержимое ARP-кэша с вашего компьютера. Прокомментируйте значения каждого из столбцов

В столбце Адрес в интернете содержится IP-адрес, в столбце Физический адрес – MAC-адрес, а в поле Тип указан тип протокола.

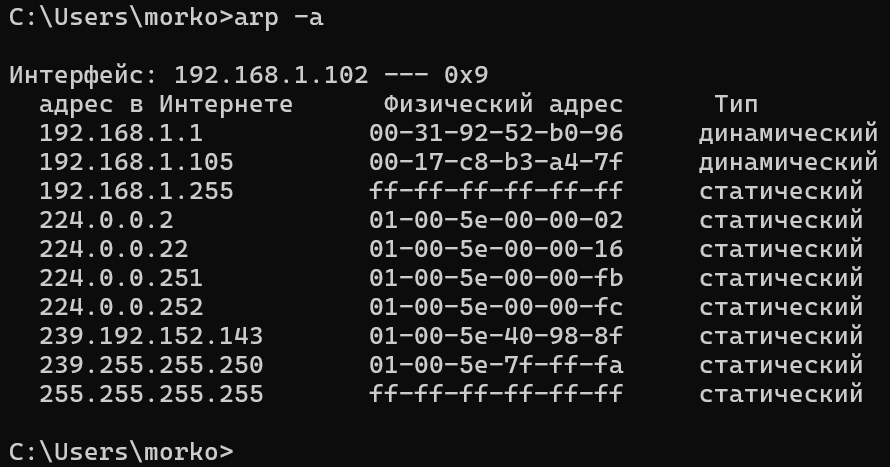


Рис. 3. Выполнение команды arp.

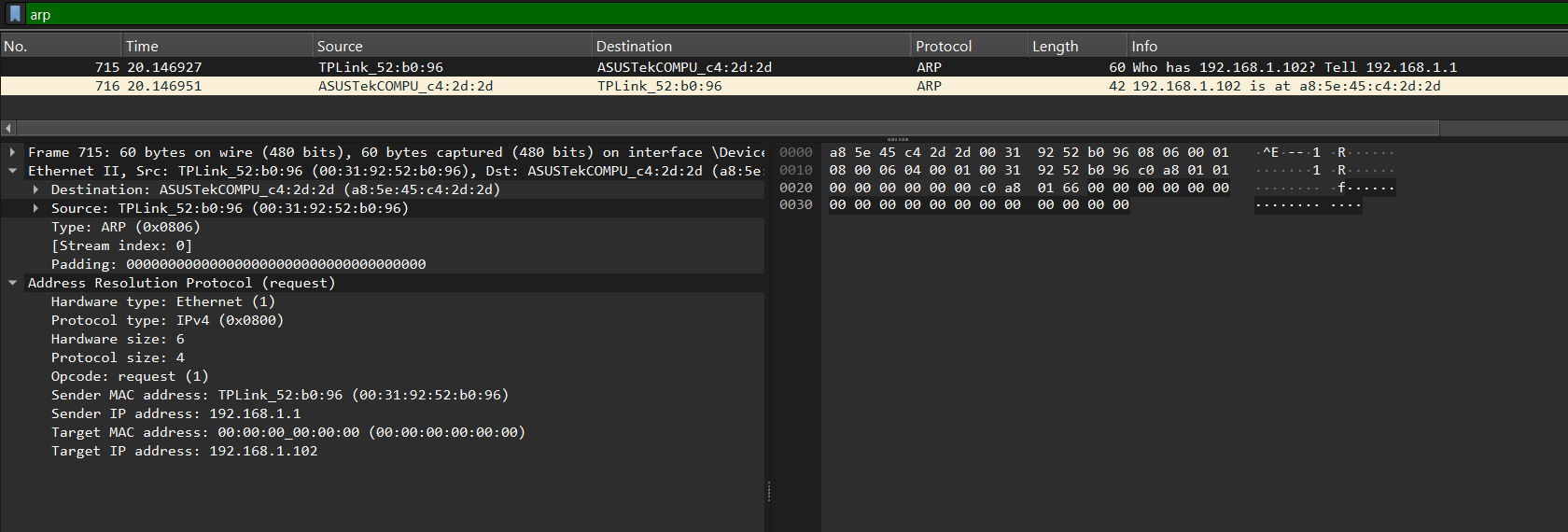


Рис. 4. ARP-сообщения.

1. Каковы шестнадцатеричные значения исходного и конечного адресов в Ethernet-кадре, содержащем сообщение с ARP-запросом?

Шестнадцатеричное значение исходного адреса равно 0a:e0:af:b7:02:d4. Шестнадцатеричное значение адреса назначения равно ff:ff:ff:ff:ff:ff, то есть, это широковещательный адрес.

1. Дайте шестнадцатеричное значение для двухбайтового поля с типом Ethernet-кадра. Какому вышестоящему протоколу оно соответствует?

Шестнадцатеричное значение в поле с типом Ethernet-кадра равно 0x0806, оно соответствует протоколу ARP.

1. Загрузите спецификацию протокола ARP с сайта ftp.rfc-editor.org/in-notes/std/std37.txt. Интересное и подробное обсуждение протокола ARP приведено по адресу erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.

а. Через сколько байт после начала Ethernet-кадра начинается поле ARP с кодом операции (opcode)?

Поле ARP с кодом операции (opcode) начинается через 20 байт после начала Ethernet-кадра.

б. Каково значение поля с кодом операции (opcode) в части Ethernet-кадра с полезной нагрузкой ARP? Имеется в виду тот кадр, в котором делается ARP-запрос.

Шестнадцатеричное значение в поле с кодом операции (opcode) в полезной нагрузке ARP в запросе равно 0x0001, оно соответствует запросу.

в. Содержится ли в ARP-сообщении IP-адрес отправителя?

Да, в ARP-сообщении содержится IP-адрес отправителя, а именно – 192.168.1.102.

г. Где в ARP-запросе находится сама «вопросная часть» – Ethernet-адрес устройства, чей соответствующий IP-адрес мы запрашиваем?

В поле Target MAC address (Целевой MAC-адрес) установлено значение 00:00:00:00:00:00, что позволяет узнать устройство, соответствующий которому IP-адрес (192.168.1.1) здесь запрашивается. Ниже приведен снимок сообщения с ARP-откликом.

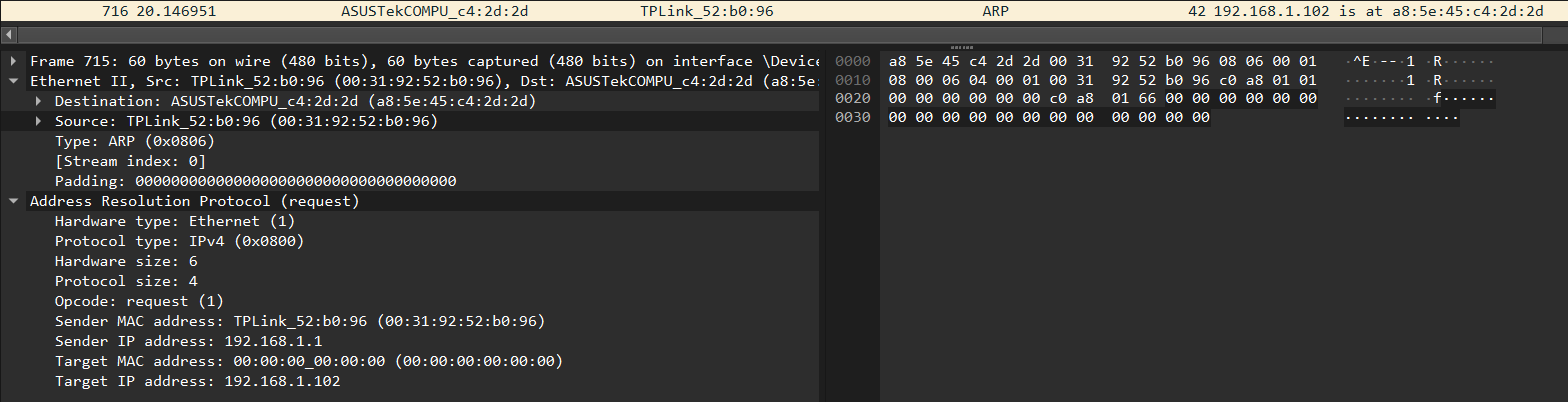


Рис. 5. ARP-отклик.

1. Теперь рассмотрим ARP-отклик, посланный в ответ на ARP-запрос.

а. Через сколько байт после начала Ethernet-кадра начинается поле ARP с кодом операции (opcode)?

Поле ARP с кодом операции (opcode) начинается через 20 байт после начала Ethernet-кадра.

б. Каково значение поля с кодом операции (opcode) в части Ethernet-кадра с полезной нагрузкой ARP? Имеется в виду тот кадр, в котором содержится ARP-отклик.

Шестнадцатеричное значение в поле с кодом операции (opcode) в полезной нагрузке ARP в запросе равно 0x0002, оно соответствует отклику.

в. Где в этом ARP-сообщении находится «ответ» на более ранний ARP-запрос – то есть, IP-адрес.

Отклик на сделанный ранее ARP-запрос содержится в поле «Sender MAC-address» (MAC-адрес отправителя), где мы видим Ethernet-адрес Destination: 00:31:92:52:b0:96, соответствующий отправителю с IP-адресом 192.168.1.1.

1. Каковы шестнадцатеричные значения исходного и конечного адресов в Ethernet-кадре, содержащем сообщение с ARP-откликом?

Шестнадцатеричное значение исходного адреса равно 00:31:92:52:b0:96, а шестнадцатеричное значение целевого адреса – a8:5e:45:c4:2d:2d.

1. Откройте файл трассировки ethernet-ethereal-trace-1 из папки wireshark-traces. Первый и второй ARP-пакеты в этой трассе соответствуют ARP-запросу, отосланному тем компьютером, где работает Wireshark, и ARP-отклику, посланному на вышеупомянутый компьютер с Wireshark тем хостом, который имеет Ethernet-адрес, указанный в ARP-запросе. Но, как понятно из пакета 6, в сети есть еще один компьютер, пославший другой ARP-запрос. Почему мы не видим ARP-отклика (в ответ на ARP-запрос из пакета 6) в трассе пакета?

В этой трассе нет отклика, поскольку мы не работаем с машиной, отправившей запрос. Этот ARP-запрос является широковещательным, однако ARP-отклик отсылается непосредственно на Ethernet-адрес отправителя.