МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное

учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

ИМ. Р.Е. АЛЕКСЕЕВА

ИНСТИТУТ РАДИОЭЛЕКТРОНИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

|  |  |  |
| --- | --- | --- |
|  |  |  |

Курс “Сети и телекоммуникации”

Отчет по лабораторной работе №1

Выполнил: Слабунов И.Н.

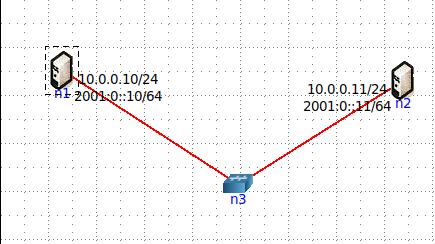
Проверил: Гай В.Е.

Нижний Новгород 2021

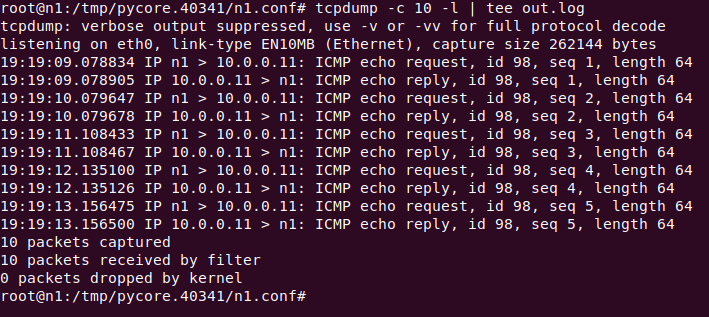
**Работа с анализатором протоколов tcpdump**

1. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл.

Структура сети:

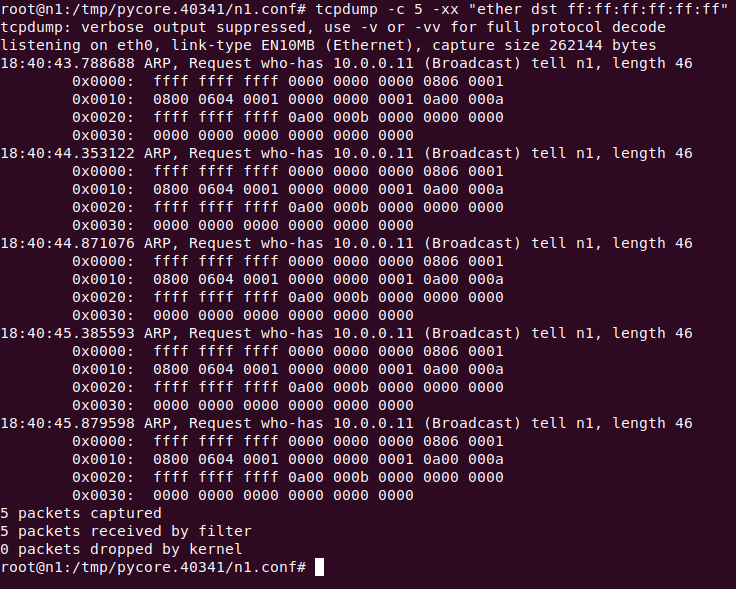


На хосте n1 запускаем tcpdump, где задаем нужные параметры:



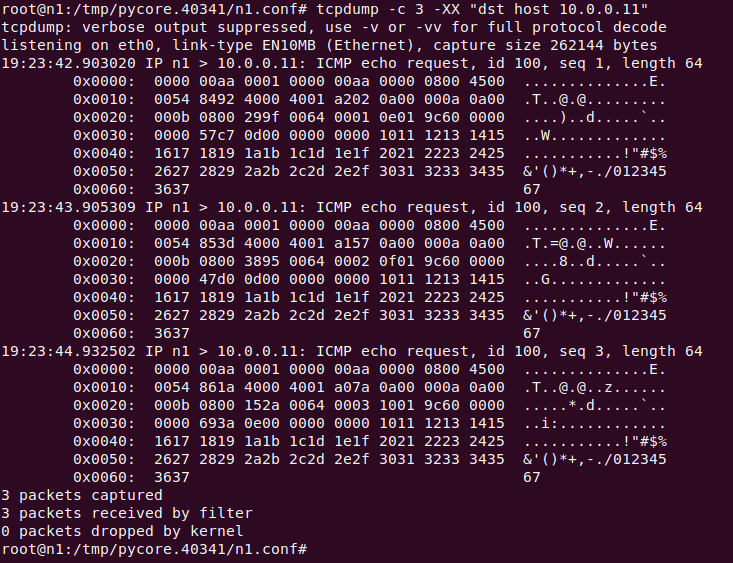
2. Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).

Составляем широковещательный MAC-пакет на хосте n2 с помощью PackETH. На другом хосте n1 запускаем tcpdump с нужными параметрами и фильтрами, совершаем 5 раз широковещательную рассылку (send) в PackETH:



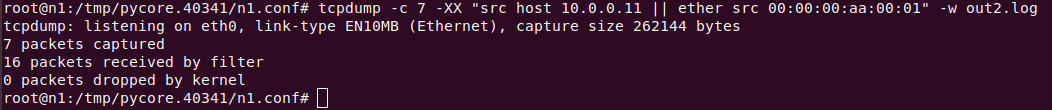
3. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования пакетов воспользоваться утилитой ping.

Запускаем tcpdump на хосте n1 c нужными параметрами и фильтрами:

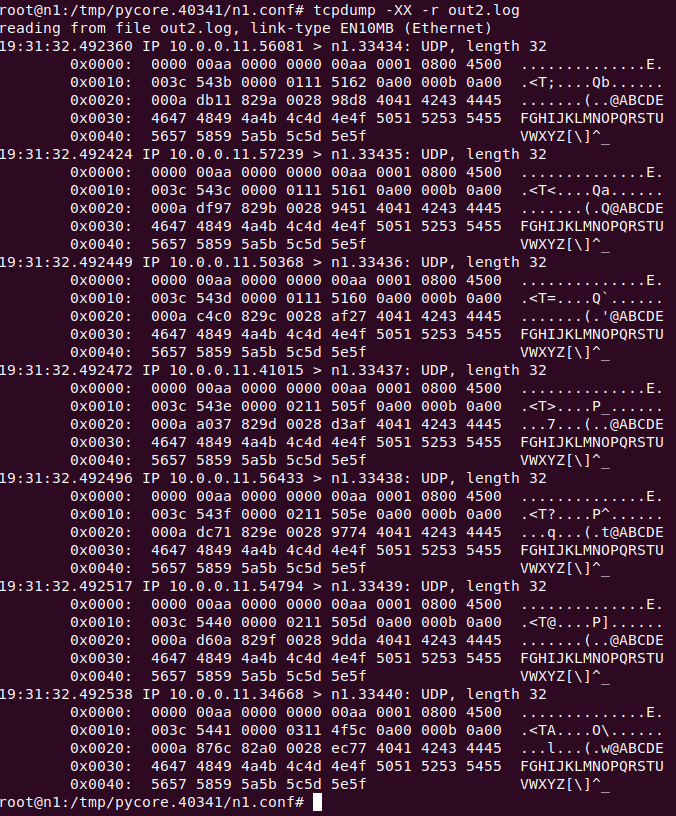


4. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 7. Результат работы программы писать в файл.

Запустим tcpdump на хосте n1 с нужными параметрами, фильтрами и одновременно передадим пакеты с хоста n2 с помощью утилиты traceroute:

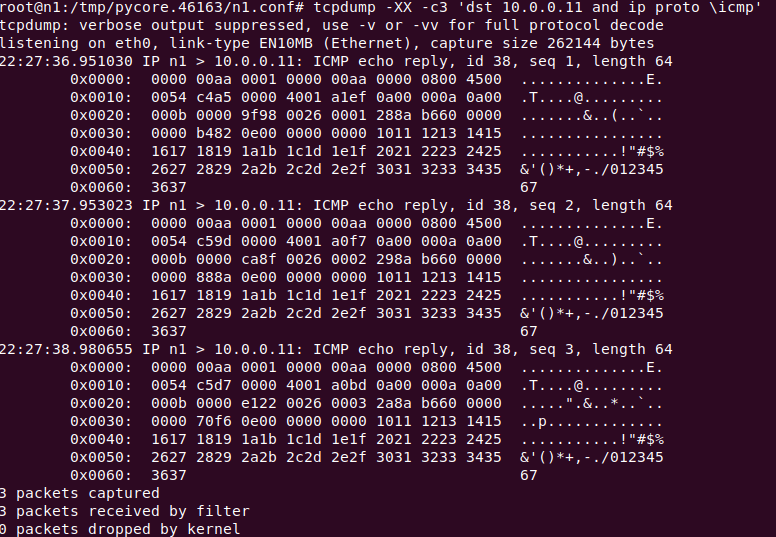


5. Прочесть программой tcpdump созданный в предыдущем пункте файл.

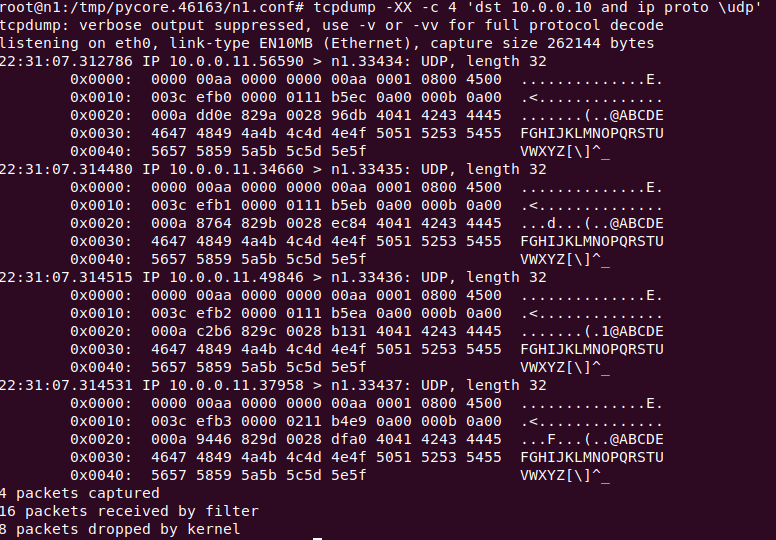


6. Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP, ICMP

1) Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Генерация пакетов с помощью ping.

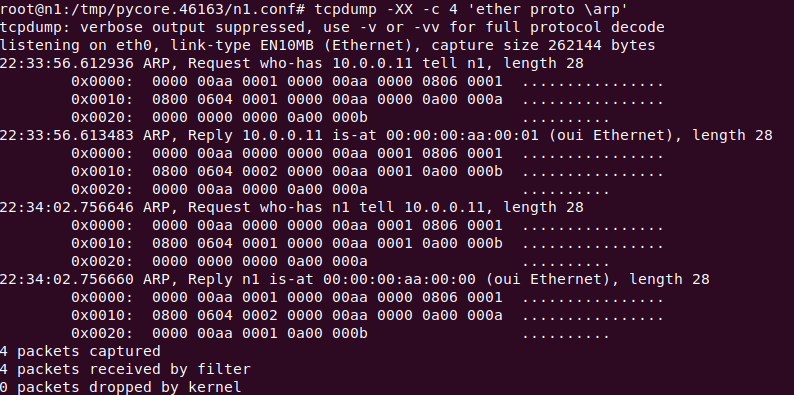


2) Запустить tcpdump, перехватывающий пакеты с фильтром протокола UDP. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить до 4.



3) Запустить tcpdump так, чтобы он перехватывал пакеты протокола ARP, созданные утилитой ping. Включить распечатку пакета в шестнадцатеричной системе ( включая заголовок канального уровня). Количество захватываемых пакетов ограничить 4.

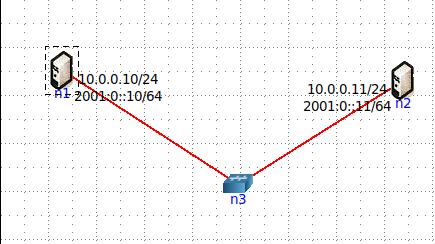
Для генерирования пакетов c помощью ping.



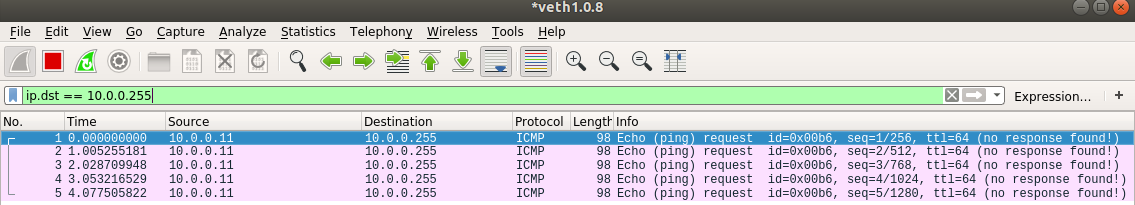
**Работа с анализатором протоколов wireshark**

1. Захватить 5-7 пакетов широковещательного трафика (фильтр по IP-адресу). Результат сохранить в текстовый файл.

Структура сети:

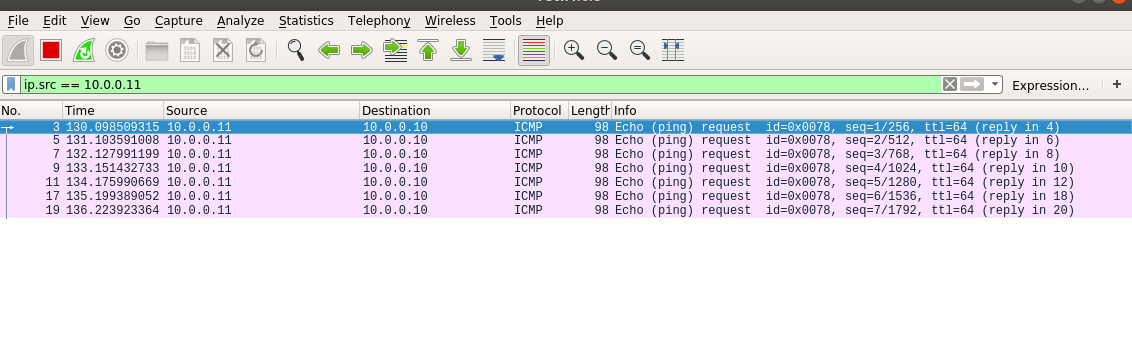


Захват пакетов с помощью Wireshark (фильтр по IP-адресу):



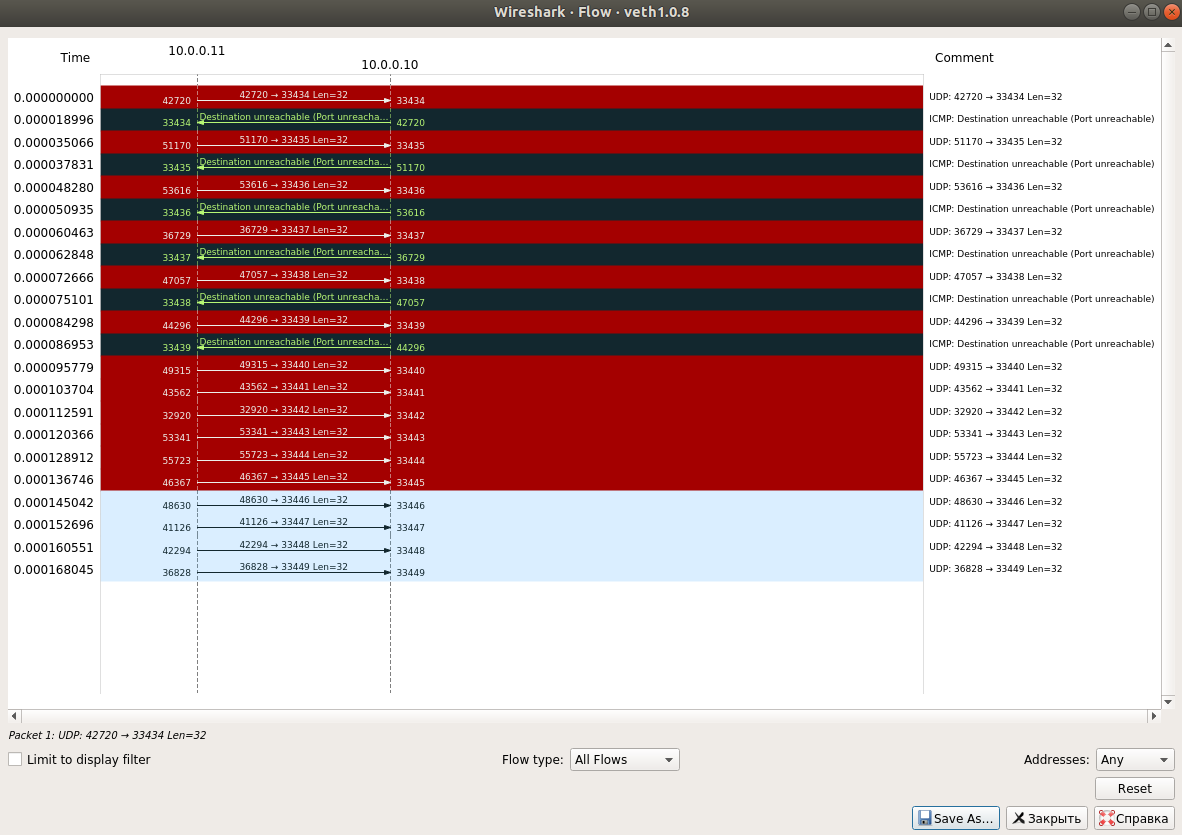
2. Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воспользоваться утилитой ping. Результат сохранить в текстовый файл.

Захват пакетов с помощью Wireshark на хосте n2 (фильтр по протоколу ICMP и IP-адресу отправителя):

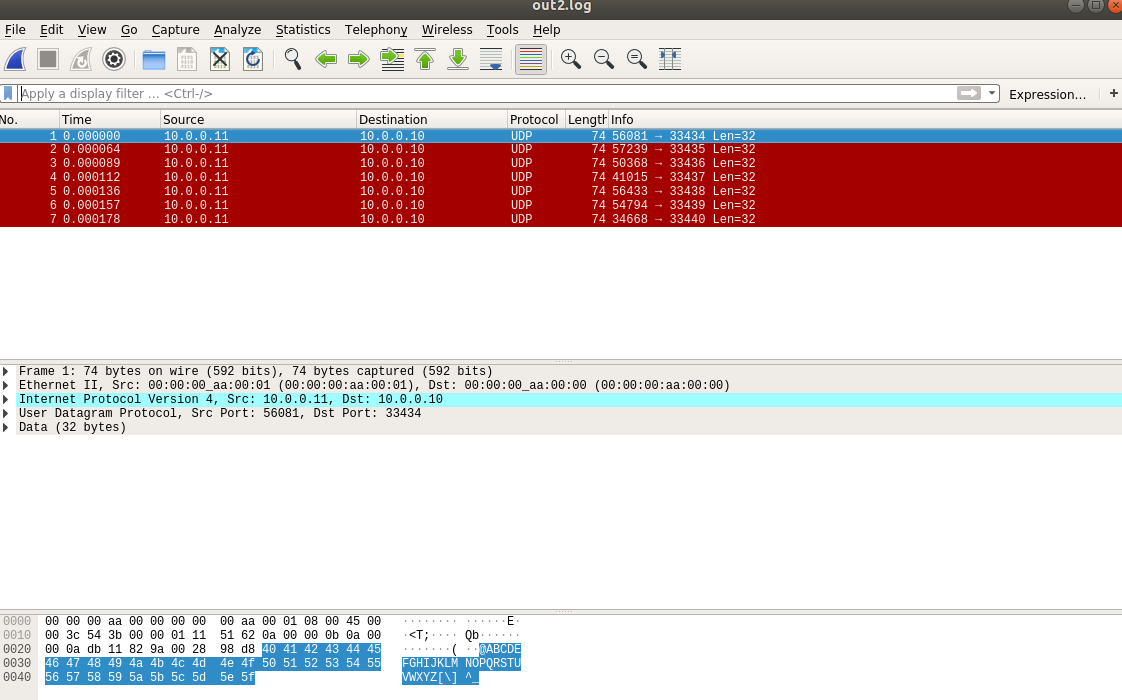


3. Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму Flow Graph. Диаграмму сохранить либо в виде текстового файла, либо в виде изображения.

Диаграмма Flow Graph:



4. Прочесть файл, созданный программой tcpdump. Сравнить с тем, что было получено утилитой wireshark.



В Wireshark представлена более подробная информация о пересылаемых пакетах.