ФГБОУ ВО “Чувашский государственный университет им. И. Н. Ульянова” Факультет: ИВТ

Кафедра: Вычислительной техники

Предмет: Сети и телекоммуникации

Лабораторная работа 6

**Отладка сети**

Выполнил: студент группы ИВТ-41-20

Галкин Дмитрий

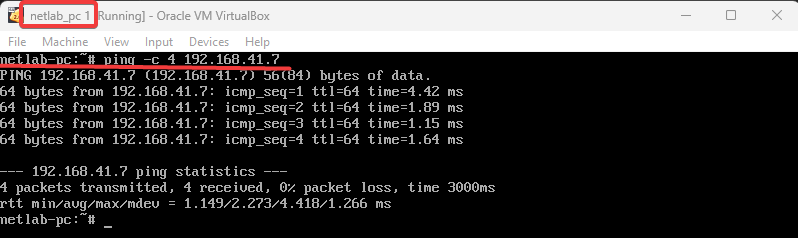
Проверила: Путевская И.В.

Чебоксары 2023 г.

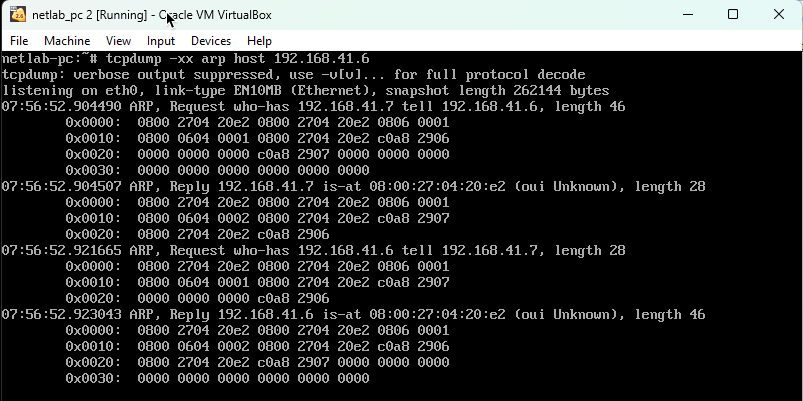
**Цель:** научиться мониторить и выявлять проблемы в сети с помощью анализатора сетевого трафика (tcpdump, wireshark, libcap).

**Задача 1:** проанализировать (визуально показать поля пакетов) трафик при подключении к сети – arp-запросы и ответы (+dhcp, усли настроен)

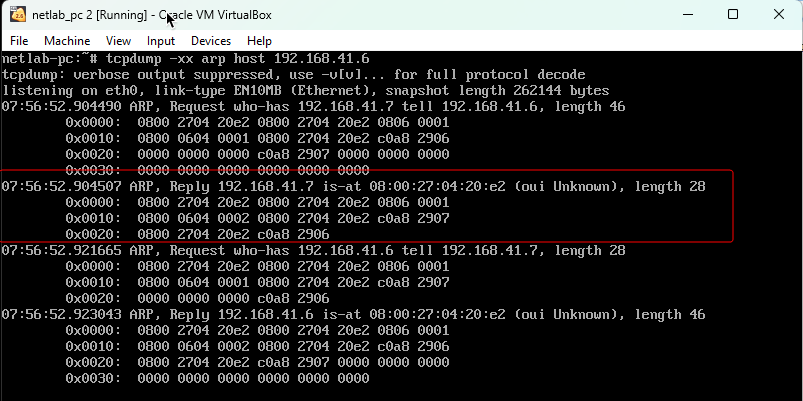
1. Выполнить ping -c 4 первого узла



1. Запустить tcdump c фильтром arp



1. Рассмотрим пакет (2)



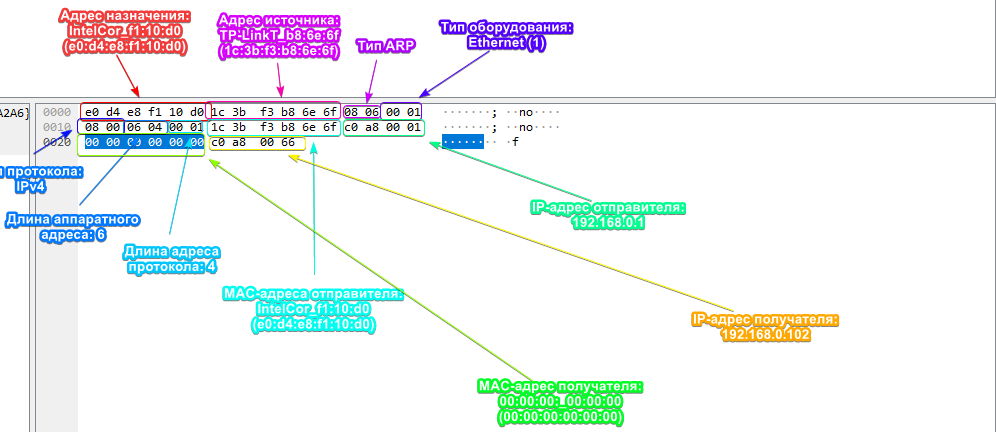
Описание пакета (2):

* Тип интерфейса: 0800
* Тип протокола: 2704
* HA-Len: 20 (длина аппаратного адреса)
* PA-Len: e2 (длина протокольного адреса)
* Код операции: 0800
* Аппаратный адрес отправителя: 2704 20e2
* Адрес отправителя: 0806
* IP-адрес отправителя: 0001 0800
* Аппаратный адрес адресата: 0604 0002 0800
* IP-адрес адресата: 2704 20e2

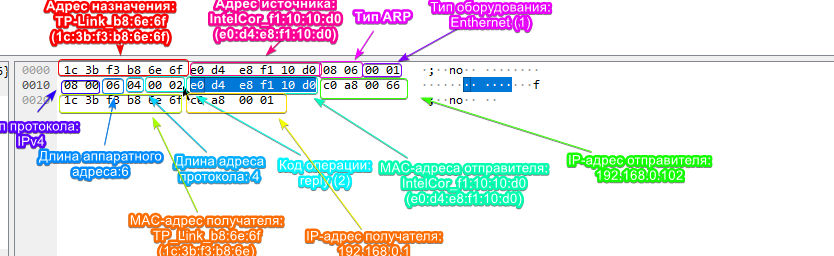


1. Описание ARP запросов/ответов в WireShark

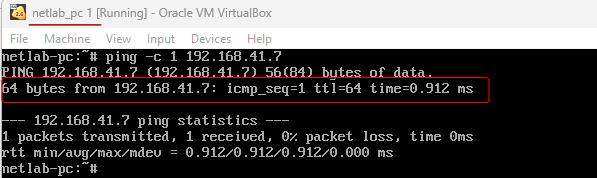
* ARP - запроса



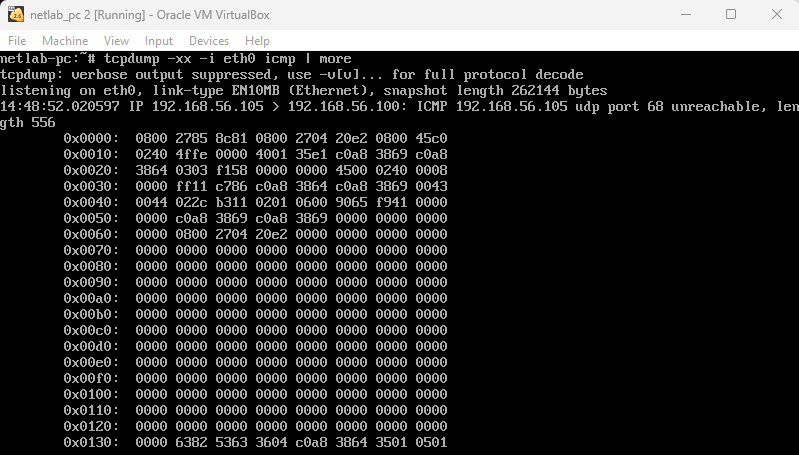
* ARP – ответа



1. Описать порядок пакетов в протоколе icmp при ping и показать их последовательность и содержимое в собранном трафике



* Выводим содержимое всех ICMP -пакетов, проходящих через интерфейс eth0 на машине netlab\_pc2

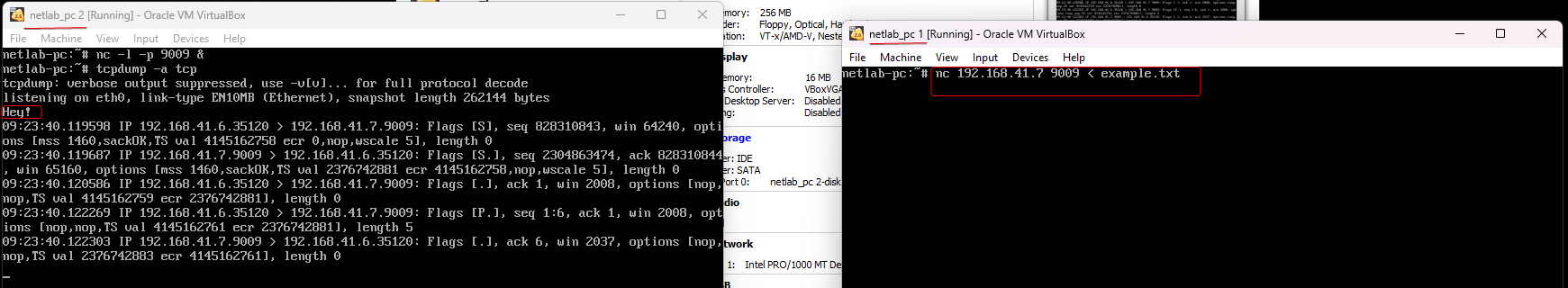


Характеристики:

* Метка времени 14:48:52.257767
* Протокол – IP
* IP адрес отправителя: 192.168.56.105
* IP адрес получателя – 192.168.56.100
* ICMP 192.168.56.105 upd port 68 uncreachable
* Порядковый номер пакета –
* Длина полезной нагрузки данных – 556
* Опция -xx выводит содержимое пакета

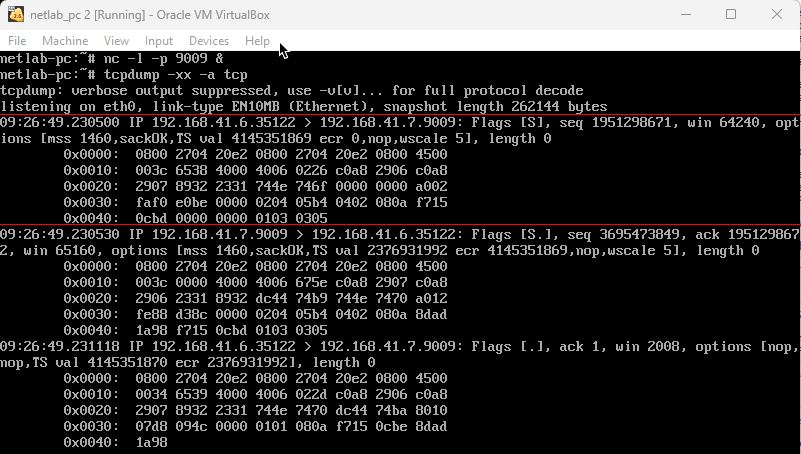
1. Мониторинг tcp соединения

* Передадим файл example.txt в netlab\_pc2



* Описать порядок протоколов





Характеристики:

* Метка времени: 09:26:49.230500
* Протокол: IP
* IP-адрес исходного хоста и помер порта: 192.68.41.7.9009
* IP-адрес назначения и номер порта: 192.168.41.6.35122
* Флаг TCP: Flags [S]
* Флаги показывают состояние и могут содержать более одного значения:
  + S – SYN: Первый шаг в установлении соединения
  + F – FIN: Прекращение соединения
  + . – ACK: Пакет подтверждения принят успешно
  + P – PUSH: Указывает получателю обрабатывать пакеты вместо их буферизации
  + R – RUST: Связь прервалась
* Порядковый номер данных в пакете:
* Номер подтверждение:
* Размер окна:
* Параметры TCP (option [mss1460, sackOK, TS val 4145351869 ecr 0, nop, wscale 51]):
  + mss: Максимальный размер сегмента
  + sack: Выборочное подтверждение и метка времени
* length 0: Отображает длину пакета в байтах, 0 потому что это лишь пакет SYN.

**Ответы на вопросы:**

1. Что такое и зачем нужен Promiscuous mode?

Promiscuous mode – режим работы сетевой карты, который позволяет ей получать и анализировать вест сетевой трафик, проходящий через нее, даже если этот трафик не адресован ей. Этот режим может быть полезен при анализе сетевых протоколов и обнаружении сетевых атак.

1. Для чего нужны сниферы?

Они используются для анализа сетевого трафика на определенном участке сети. Они могут перехватывать и записывать все данные, проходящие через сетевой интерфейс, включая пользовательские данные, сетевые протоколы, заголовки пакетов и другую информацию.

1. Что показывают сниферы?

* Содержимое пакетов данных, включая заголовки и пользовательские данные
* Адреса источника и назначения для каждого пакета
* Информацию о сетевых протоколах, используемых для обмена данными
* Время отправки и приема пакета
* Размер пакета и время передачи
* Информацию о сетевых устройствах, включая IP-адреса, MAC-адреса, имя устройства и другие данные

1. Какая структура сообщения перехваченного снифером?

* Заголовок сообщения: содержит информацию о сетевом протоколе, адресах отправителя и получателя, длине сообщения и другие параметры
* Тело сообщения: содержит непосредственно данные, передаваемые между устройствами в сети. Тело также может иметь различный формат в зависимости от протокола и типа данных, передаваемых в сообщении

1. Что происходит при подключении узла к сети?

* Физическое подключение: узел физически подключается к сетевому устройству, такому как коммутатор или маршрутизатор
* Назначение адреса: узлу назначается уникальный адрес в сети, который может быть либо статическим, т.е заданным вручную, либо динамическим, назначенным автоматически с помощью протокола DHCP
* Определение маршрута: устройства в сети должны знать, как доставлять данные к новому узлу, и для этого требуется определение маршрута, который маршрутизаторы в сети будут использовать для доставки данных до нового узла
* Проверка связи: после того, как узел подключен к сети и ему назначен адрес, происходит проверка связи, чтобы убедиться, что узел может успешно обмениваться данными с другими узлами в сети

1. Как пакет доходит до интернета и как меняется?

* Определение маршрута
* Передача пакета по сети
* Транспортный уровень: происходит разбивка больших пакетов на более мелкие единицы, называемые сегментами, и их пересылка между отправителем и получателем с помощью протоколов транспортного уровня, таких как TCP или UDP
* Преобразование адресов
* Проверка целостности