

**ОТЧЁТ**

**по лабораторной работе № 1**

«Освоение инструментария для выполнения работ, построение простой сети»

**по модулю 4: «***Сети***»**

Выполнил:Проверил:

*Азява Д.А.* *Менжулин С.А.*

Новосибирск 2023

Задание:

1) Установить и настроить эмулятор GNS3

2) Создать простейшую сеть, состоящую из 1 коммутатора и 2 компьютеров, назначить им произвольные ip адреса из одной сети

3) Запустить симуляцию, выполнить команду ping с одного из компьютеров, изпользуя ip адрес второго компьютера

4) Перехватить трафик протокола ARP и проанализировать заголовки пакетов в программе Wireshark, для фильтрации трафика, относящегося к указанному протоколу использовать фильтры Wireshark

Установив и настроив эмулятор GNS3, создадим простейшую сеть, состоящую из 1 коммутатора и 2 компьютеров.

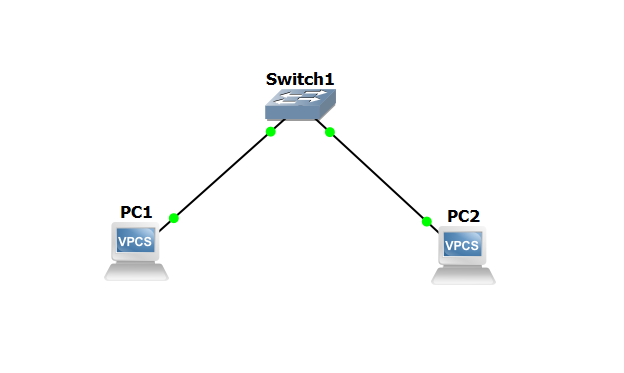


Рисунок 1 – Сеть

Зададим первому компьютеру IP-адрес 192.168.0.2 и шлюз 192.168.0.1 с маской подсети 255.255.255.0 (Рисунок 2)

Зададим второму компьютеру IP-адрес 192.168.0.3 и шлюз 192.168.0.1 с маской подсети 255.255.255.0 (Рисунок 3)

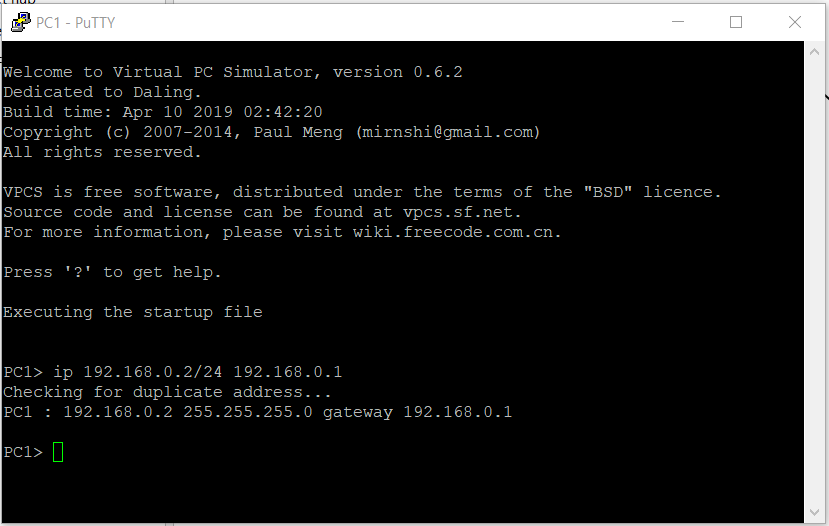


Рисунок 2 – Настройка IP-адреса на ПК 1

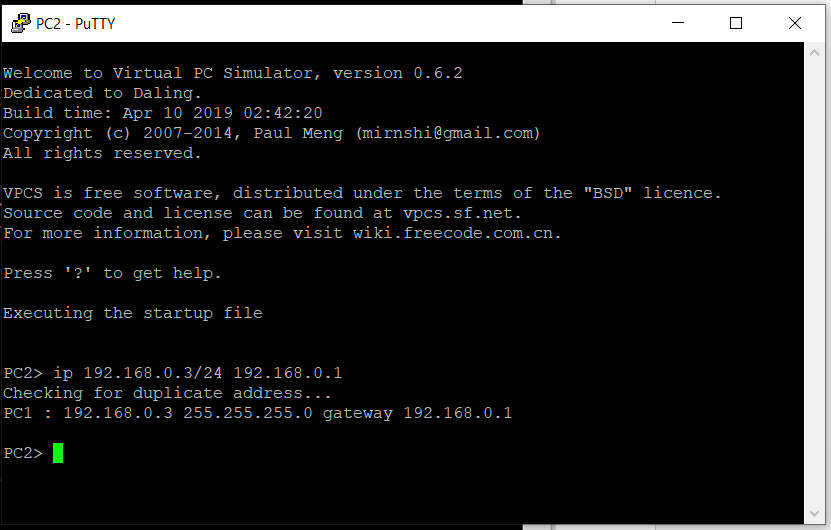


Рисунок 3 – Настройка IP-адреса на ПК 2

Теперь, воспользовавшись утилитой WireShark, перехватим и проанализируем ARP-пакеты.

Для этого, щёлкнем правой клавишей мышки по кабелю, и выберем «Start capture». (Рисунок 4)

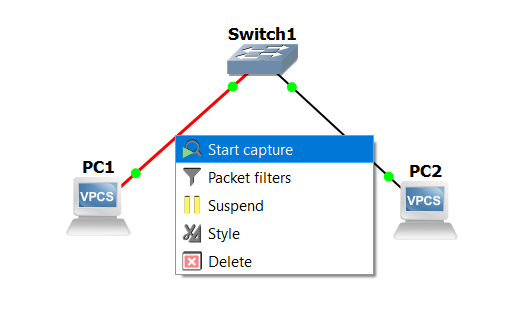


Рисунок 4 – Выбор канала «прослушивания»

Воспользуемся утилитой ping на ПК-1 и проверим доступность ПК-2.

Видим, что ПК-1 получил ICMP-ответ от ПК-2, следовательно, сеть настроена верно и работает. (Рисунок 5)

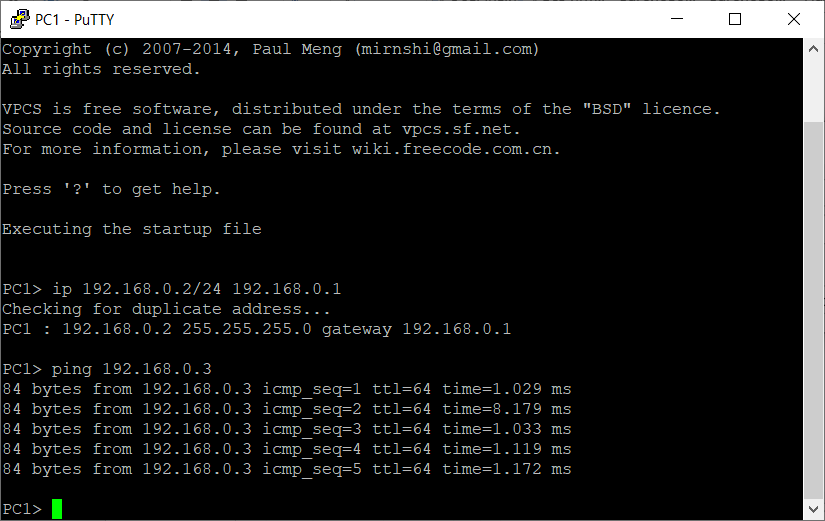


Рисунок 5 – Выполнение утилиты ping

В утилите WireShark мы видим, что перехваченные пакеты (Рисунок 6). Так как нас интересуют лишь ARP-пакеты, отфильтруем список (Рисунок 7).

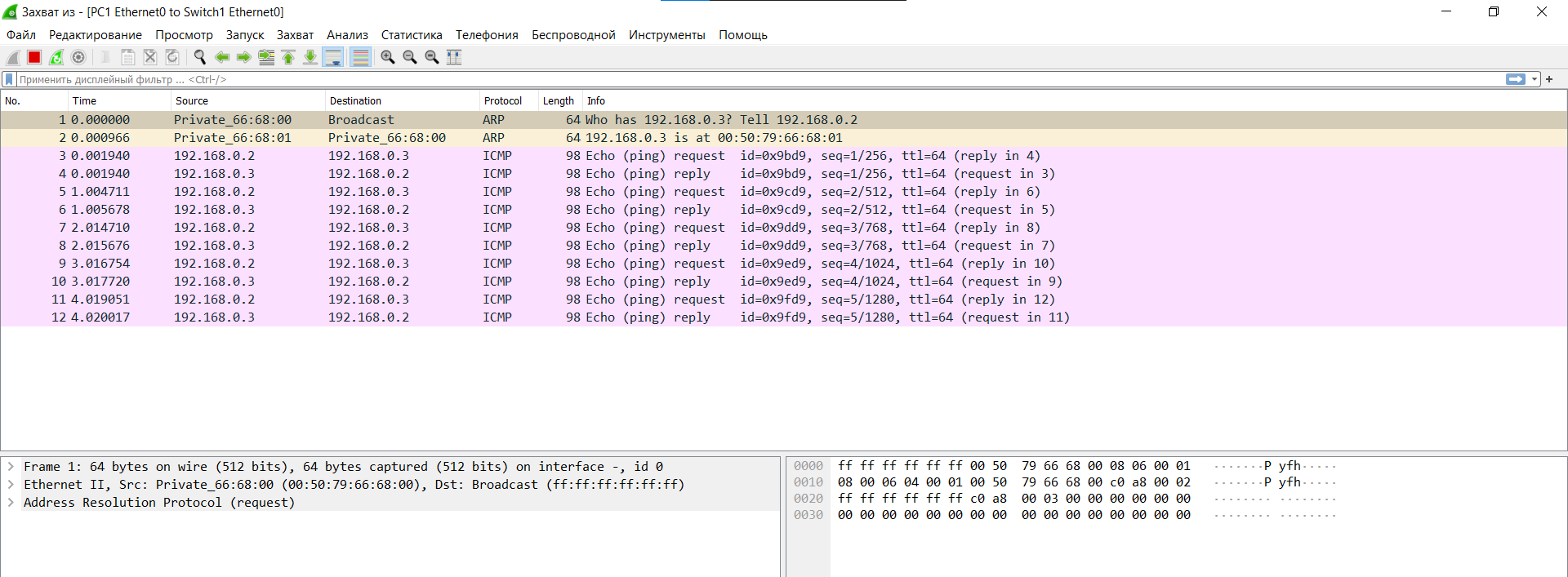


Рисунок 6 – Перехваченный трафик

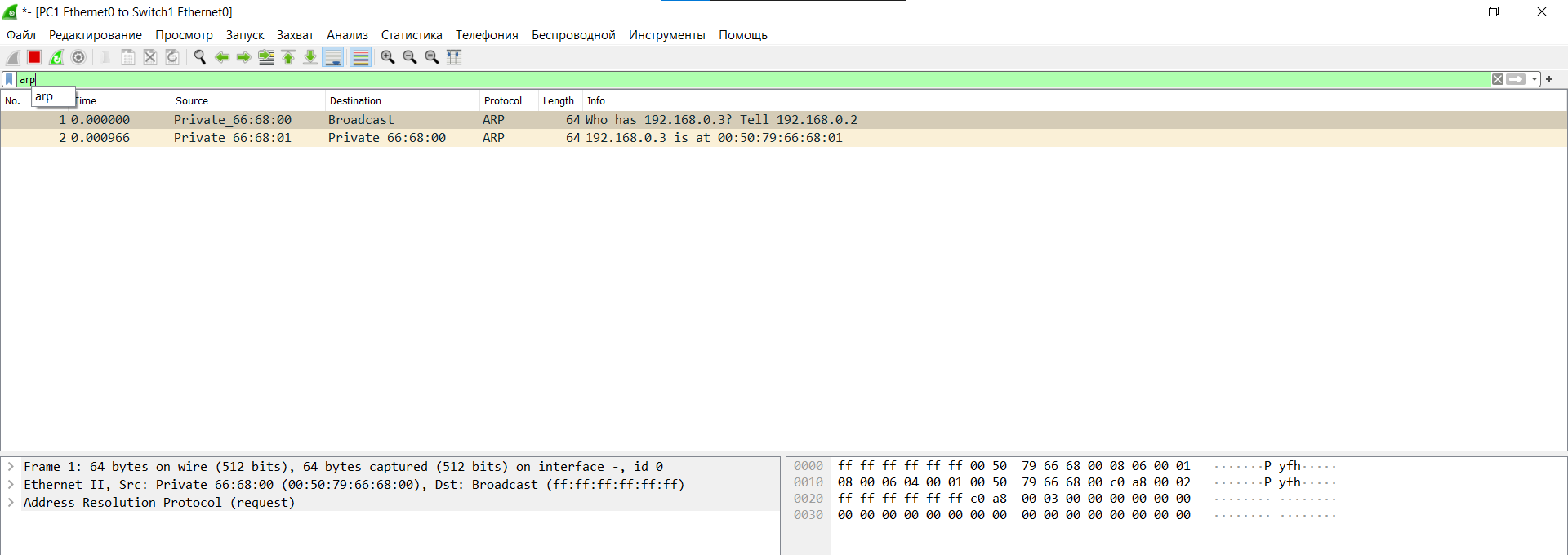


Рисунок 7 – Отфильтрованный список

Сперва рассмотрим ARP-запрос.



Рисунок 8 – Содержимое ARP-запроса

Пакет начинается с МАС-адреса получателя (красный прямоугольник на рисунке 8), так как он ещё не известен, используется широковещательный МАС-адрес (Broadcast – ff:ff:ff:ff:ff:ff).

Затем идёт МАС-адрес отправителя -00:50:79:66:68:00 (зелёный прямоугольник на рисунке 8).

За ним следует идентификатор протокола ARP равный 0x0806 (жёлтый прямоугольник на рисунке 8).

Следом идёт идентификатор оборудования, в данном случае Ethernet (фиолетовый прямоугольник на рисунке 8), вместе с ним приходит идентификатор протокола IPv4, равный 0x0800 (жёлтый прямоугольник на рисунке 8).

Hardware size (чёрный прямоугольник на рисунке 8) содержит в себе размер аппаратного адреса (Для Ethernet это будет шесть октетов (48 бит)).

Protocol size (розовый прямоугольник на рисунке 8) содержит в себе размер адреса сетевого протокола (Для IPv4 это будет четыре октета (32 бита)).

Затем мы видим код операции ARP (синий прямоугольник на   
рисунке 8): 0001 для запроса ARP или 0002 для ответа ARP.

Затем снова следует МАС-адрес отправителя (зелёный прямоугольник на рисунке 8). И за ним IP-адрес отправителя (голубой прямоугольник на рисунке 8) представленный в шестнадцатеричном виде: c0.a8.00.02.

Затем следует МАС-адрес получателя (красный прямоугольник на рисунке 8), так как он ещё не известен, используется широковещательный МАС-адрес (Broadcast – ff:ff:ff:ff:ff:ff) и его IP-адрес в шестнадцатеричном виде: c0.a8.00.03

Затем идёт наполнение ARP пакета, в данном случае он пуст.

И всё завершается контрольной суммой пакета (синий прямоугольник на рисунке 8). В данном случае проверка на целостность отсутствует.

Всё это можно увидеть в более доступном виде в соседнем окне (рисунок 9).

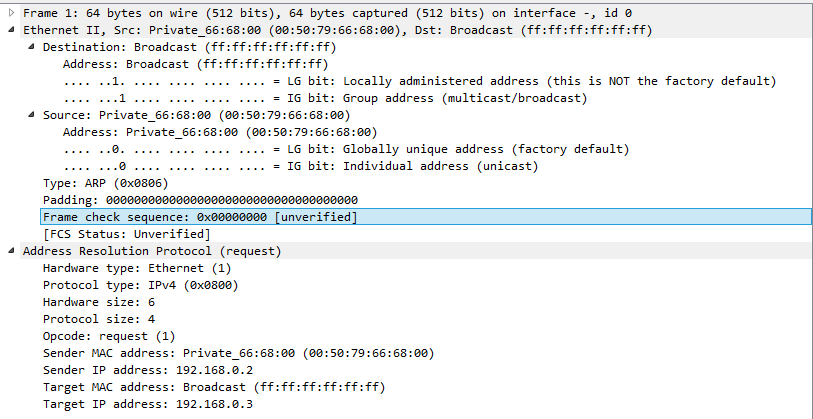


Рисунок 9 – Содержимое пакета ARP

Теперь рассмотрим ARP-ответ.



Рисунок 10 – Содержимое ARP-ответа

Пакет начинается с МАС-адреса получателя (красный прямоугольник на рисунке 10), равный МАС-адресу ПК-1 00:50:79:66:68:00

Затем идёт МАС-адрес отправителя - 00:50:79:66:68:01 (зелёный прямоугольник на рисунке 10).

За ним следует идентификатор протокола ARP равный 0x0806 (жёлтый прямоугольник на рисунке 10).

Следом идёт идентификатор оборудования, в данном случае Ethernet (фиолетовый прямоугольник на рисунке 10), вместе с ним приходит идентификатор протокола IPv4, равный 0x0800 (жёлтый прямоугольник на рисунке 10).

Hardware size (чёрный прямоугольник на рисунке 10) содержит в себе размер аппаратного адреса (Для Ethernet это будет шесть октетов (48 бит)).

Protocol size (розовый прямоугольник на рисунке 10) содержит в себе размер адреса сетевого протокола (Для IPv4 это будет четыре октета (32 бита)).

Затем мы видим код операции ARP (синий прямоугольник на   
рисунке 10): 0001 для запроса ARP или 0002 для ответа ARP.

Затем снова следует МАС-адрес отправителя (зелёный прямоугольник на рисунке 10). И за ним IP-адрес отправителя (голубой прямоугольник на рисунке 10) представленный в шестнадцатеричном виде: c0.a8.00.03.

Затем следует МАС-адрес получателя (красный прямоугольник на рисунке 10), равный МАС-адресу ПК-1 00:50:79:66:68:00 и его IP-адрес в шестнадцатеричном виде: c0.a8.00.02

Затем идёт наполнение ARP пакета, в данном случае он пуст.

И всё завершается контрольной суммой пакета (синий прямоугольник на рисунке 10). В данном случае проверка на целостность отсутствует.

Всё это можно увидеть в более доступном виде в соседнем окне (рисунок 11).

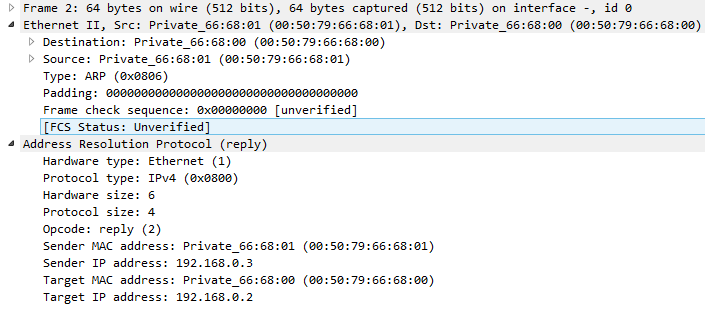


Рисунок 11 – Содержимое ARP-ответа

Вывод: В результате выполнения работы был установлен и настроен эмулятор GNS3, который будет работать на локальном компьютере. Без подключения к внешнему серверу.

Построена простейшая сеть, состоящая из 1 коммутатора и 2 компьютеров. Сеть была настроена и протестирована при помощи утилиты ping. Так же были перехвачен трафик утилитой WireShark и проанализировано содержимое ARP-пакета. Невыясненным осталось то, что должен содержать в себе ARP-пакет в сегменте padding.

Ссылка на папку с проектами по модулю 4 в github: [git@github.com:DimWorks/Module\_4](mailto:git@github.com:DimWorks/Module_4)