МИНИСТЕРСТВО НАУКИ
И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования

«Новосибирский государственный технический университет»

НГТУ
НЭТИ | Факультет прикладной
математики и информатики

Лабораторная работа №1

Освоение инструментария для выполнения работ, построение простой сети.

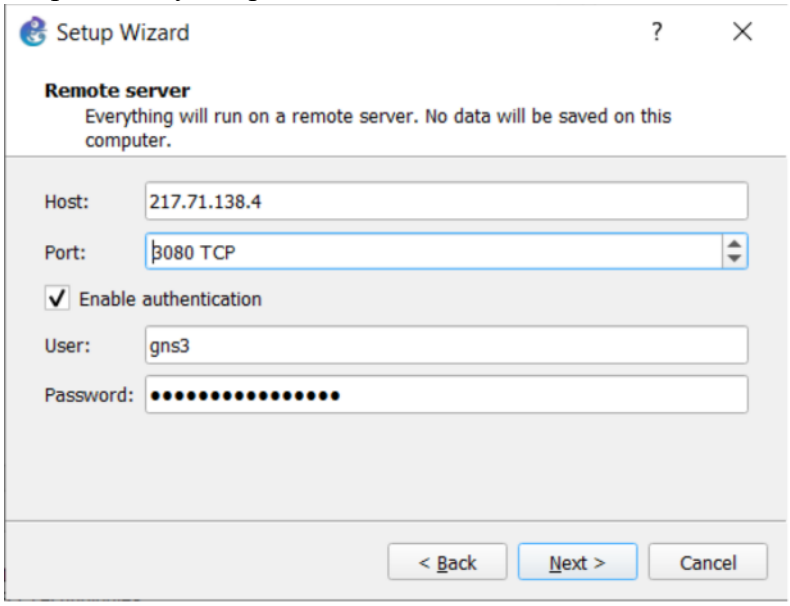
Студент **Истратенко Валерий**

Новосибирск, 2024

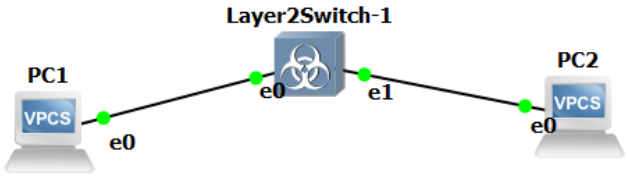
Все команды для настройки включены в отчет в текстовом виде вместе с скриншотами, чтобы наглядно отобразить ход работы.

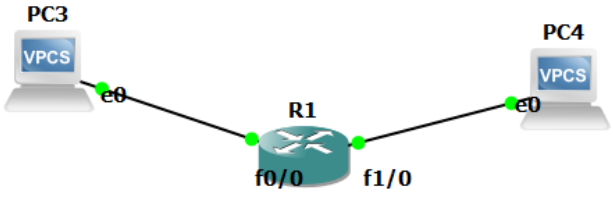
nb! - отметка в тексте, "обратите особое внимание"!

1. **Установить и настроить эмулятор GNS3**
   После установки и настройки эмулятора GNS3:

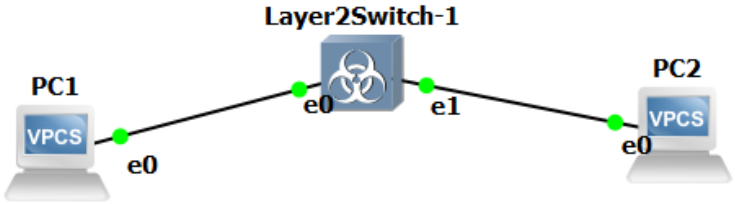


   были собраны 2 схемы, которые указаны на скриншоте ниже:





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



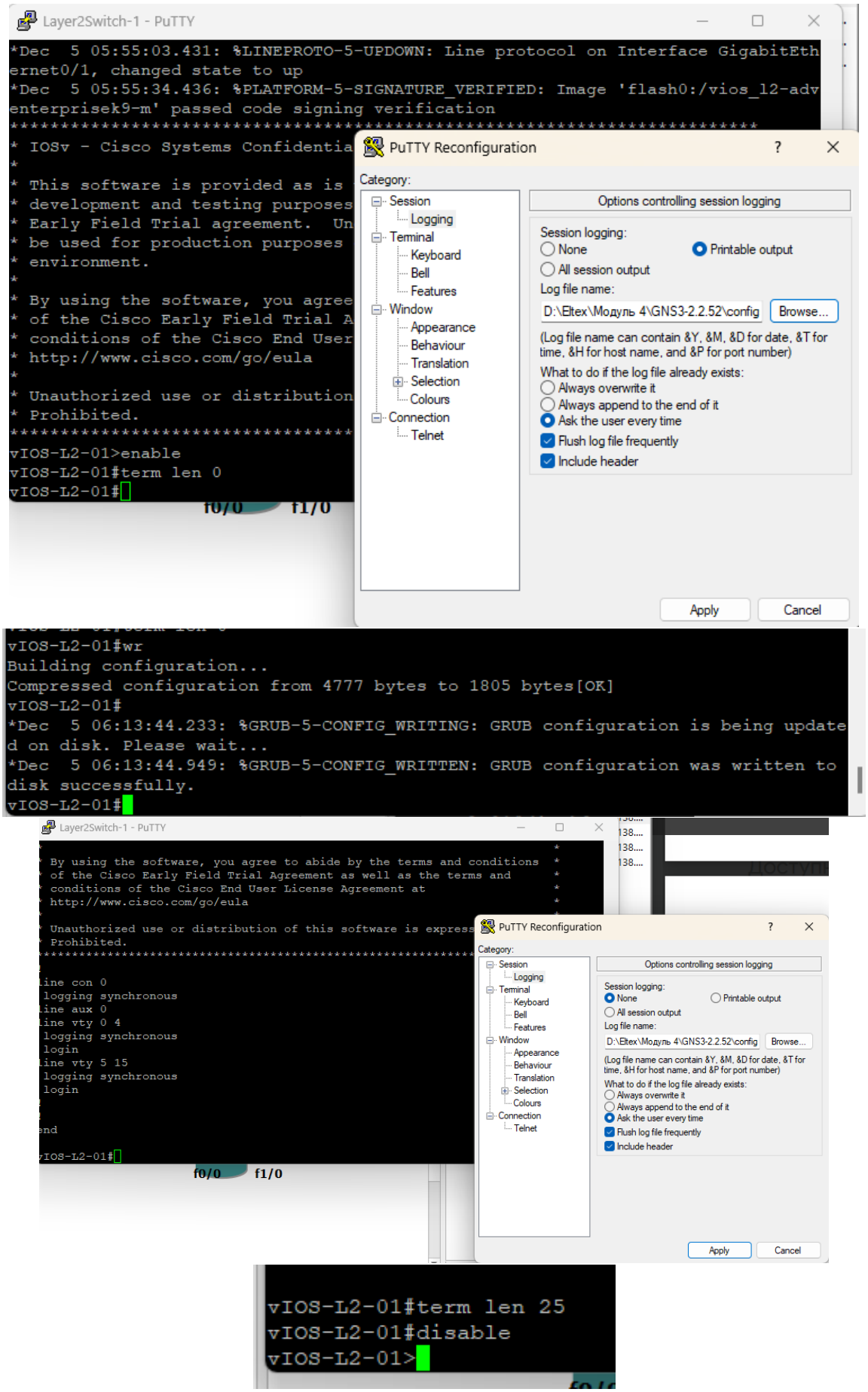
На этом скриншоте (ниже set pcname PC1) указаны ip-адрес и маска подсети для PC1, которые были добавлены в config устройства.

```
# This the configuration for PC1
#
# Uncomment the following line to enable DHCP
# dhcp
# or the line below to manually setup an IP address and subnet mask
# ip 192.168.1.1 255.0.0.0
#

set pcname PC1
ip 192.168.1.1 255.255.255.0
```

На этом скриншоте (ниже set pcname PC2) указаны ip-адрес и маска подсети для PC2, которые были добавлены в config устройства.

```
# This the configuration for PC2
#
# Uncomment the following line to enable DHCP
# dhcp
# or the line below to manually setup an IP address and subnet mask
# ip 192.168.1.1 255.0.0.0
#

set pcname PC2
ip 192.168.1.2 255.255.255.0
```

Ниже показано последовательное выполнение операций для выгрузки конгфигурации устройств в наш файл.



Файл my_switch1.conf содержит текст конфигурации свича.

3. Запустить симуляцию, выполнить команду ping с одного из компьютеров, используя ip адрес второго компьютера

Описание вывода на экран:

- **84 bytes** — количество байт, полученных в ответе от хоста.
- **from 192.168.1.2**— IP-адрес хоста, от которого пришел ответ.
- **icmp_seq=1** — номер последовательности ICMP (каждый пакет ICMP имеет уникальный номер).
- **ttl=64** — TTL (Time to Live) пакета, который указывает на количество маршрутизаторов, через которые пакет может пройти, прежде чем будет уничтожен.
- **time=0.408 ms** — время отклика в миллисекундах, т.е. время, которое потребовалось пакету, чтобы дойти от вашего компьютера до целевого хоста и обратно.

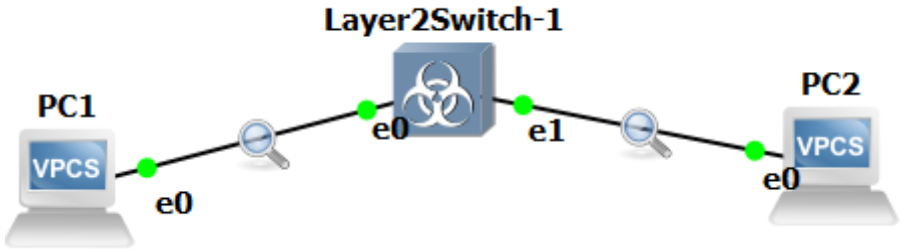
Это скриншот из консоли первого компьютера, при отправке эхо-повтора второму компьютеру через коммутатор.

```
PC1> ping 192.168.1.2

84 bytes from 192.168.1.2 icmp_seq=1 ttl=64 time=0.408 ms
84 bytes from 192.168.1.2 icmp_seq=2 ttl=64 time=5.774 ms
84 bytes from 192.168.1.2 icmp_seq=3 ttl=64 time=0.493 ms
84 bytes from 192.168.1.2 icmp_seq=4 ttl=64 time=0.741 ms
84 bytes from 192.168.1.2 icmp_seq=5 ttl=64 time=4.526 ms

PC1>
```

Это скриншот из консоли второго компьютера, при отправке эхо-повтора первому компьютеру через коммутатор.

```
PC2> ping 192.168.1.1

84 bytes from 192.168.1.1 icmp_seq=1 ttl=64 time=0.486 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=64 time=6.162 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=64 time=0.583 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=64 time=0.651 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=64 time=1.868 ms

PC2>
```

4. Перехватить трафик протокола arp на всех линках(nb!), задокументировать и проанализировать заголовки пакетов в программе Wireshark, для фильтрации трафика, относящегося к указанному протоколу использовать фильтры Wireshark



Описание перехваченного трафика протокола ARP:

Разбор полей:

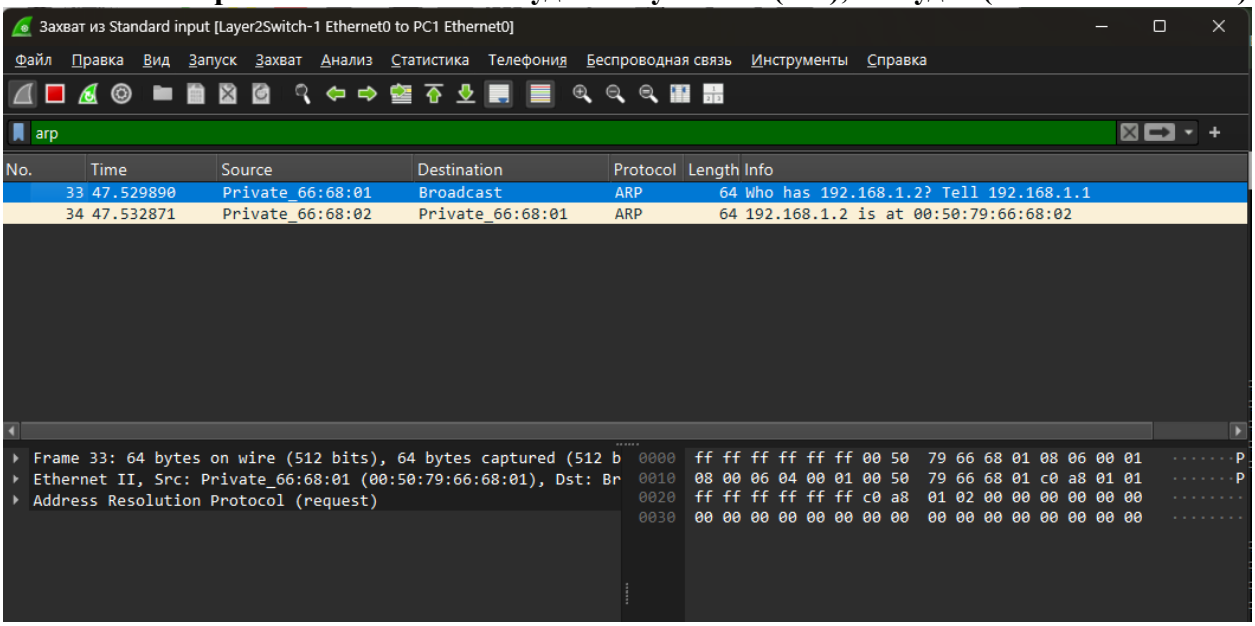
- **No. (Номер пакета)** - Это номер пакета в списке.
- **Time (Время)** - Время, прошедшее с начала захвата трафика до момента получения пакета.
- **Source (Источник)** - IP-адрес устройства, которое отправило пакет. В примере выше:
  - Для первого пакета: 192.168.1.1
  - Для второго пакета: 192.168.1.2
- **Destination (Назначение)** - IP-адрес устройства, к которому отправлен пакет:
  - Для первого пакета: 192.168.1.2

- Для второго пакета: 192.168.1.1

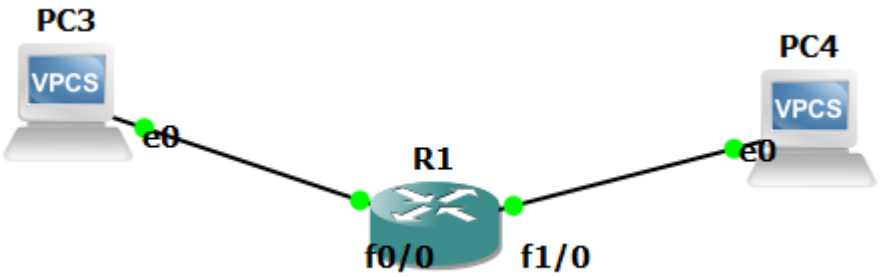
- **Protocol (Протокол)** - Указывает, какой протокол был использован в пакете. В нашем случае это ARP.
- **Length (Длина)** - Размер пакета в байтах.
- **Info (Информация)** - Информация о типе ARP-пакета и дополнительной информации. Это ключевая часть, которая дает больше сведений о содержимом пакета:

Дальнейший разбор пакета:

- **Frame** - Количество байт и битов в кадре, а также время прибытия кадра в Wireshark.
- **Ethernet II** - Это Ethernet-кадр, где указаны MAC-адреса отправителя и получателя. В случае ARP-запроса, получатель (**Dst**) будет **Broadcast** (ff:ff:ff:ff:ff:ff), так как запрос направлен всем устройствам в сети.
- **Type** - Протокол, который используется в кадре. В данном случае это **ARP (0x0806)**.
- **Address Resolution Protocol** - Это сам протокол ARP.
- **В arp-ответе отличаться будет получатель (Dst), он будет (00:50:79:66:68:01)**



5. Создать простейшую сеть, состоящую из 1 маршрутизатора и 2 компьютеров, назначить им произвольные ip адреса из разных сетей



На этом скриншоте (ниже set pcname PC3) указаны ip-адрес, маска подсети и ip шлюза для PC3, которые были добавлены в config устройства.

```
# This the configuration for PC3
#
# Uncomment the following line to enable DHCP
# dhcp
# or the line below to manually setup an IP address and subnet mask
# ip 192.168.1.2 255.255.255.0 gateway 192.168.1.1
#

set pcname PC3
ip 192.168.1.2 255.255.255.0 192.168.1.1
```

На этом скриншоте (ниже set pcname PC4) указаны ip-адрес, маска подсети и ip шлюза для PC4, которые были добавлены в config устройства.

```
# This the configuration for PC4
#
# Uncomment the following line to enable DHCP
# dhcp
# or the line below to manually setup an IP address and subnet mask
# ip 192.168.1.1 255.0.0.0
#

set pcname PC4
ip 192.168.2.2 255.255.255.0 192.168.2.1
```

Описание выполненных команд:

- **Enable** - Эта команда используется для перехода в привилегированный режим (режим EXEC), где вы можете выполнять более высокоуровневые команды конфигурации. После ввода этой команды будет запрашиваться пароль (если он установлен).
- **configure terminal -** Команда для входа в режим глобальной конфигурации, где вы можете настраивать интерфейсы, маршруты и другие параметры устройства.
- **interface FastEthernet0/0** — входим в режим конфигурации для интерфейса FastEthernet0/0, который представляет собой физический интерфейс на маршрутизаторе.
- **ip address 192.168.1.1 255.255.255.0** — задаем IP-адрес 192.168.1.1 и маску подсети 255.255.255.0 для интерфейса FastEthernet0/0. Это позволяет маршрутизатору работать в подсети 192.168.1.0/24.
- **no shutdown** — активирует интерфейс (по умолчанию интерфейс может быть выключен, и команда no shutdown включает его).
- **Далее повторяем операцию для конфигурации для интерфейса FastEthernet1/0**

```
R1#enable
R1#interface FastEthernet0/0
   ^
% Invalid input detected at '^' marker.

R1#configure termnal
              ^
% Invalid input detected at '^' marker.

R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#
*Mar  1 00:06:59.767: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Mar  1 00:07:00.767: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
R1(config-if)#exit
R1(config)#interface FastEthernet1/0
R1(config-if)#ip address 192.168.2.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
*Mar  1 00:07:31.351: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state t
o up
*Mar  1 00:07:32.351: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et1/0, changed state to up
R1(config-if)#exit
R1(config)#
```

6. Запустить симуляцию, выполнить команду ping с одного из компьютеров, используя ip адрес второго компьютера

Описание вывода на экран:

- **84 bytes** — количество байт, полученных в ответе от хоста.
- **from 192.168.2.2**— IP-адрес хоста, от которого пришел ответ.
- **icmp_seq=2** — номер последовательности ICMP (каждый пакет ICMP имеет уникальный номер).
- **ttl=63** — TTL (Time to Live) пакета, который указывает на количество маршрутизаторов, через которые пакет может пройти, прежде чем будет уничтожен.
- **time=13.322ms** — время отклика в миллисекундах, т.е. время, которое потребовалось пакету, чтобы дойти от вашего компьютера до целевого хоста и обратно.

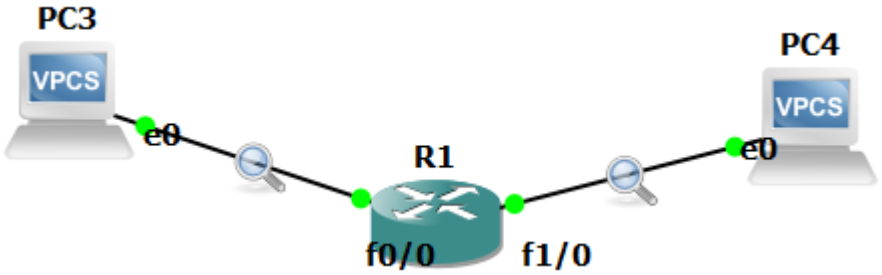
Это скриншот из консоли третьего компьютера, при отправке эхо-повтора четвертому компьютеру через маршрутизатор.

```
PC3> ping 192.168.2.2

192.168.2.2 icmp_seq=1 timeout
84 bytes from 192.168.2.2 icmp_seq=2 ttl=63 time=13.322 ms
84 bytes from 192.168.2.2 icmp_seq=3 ttl=63 time=15.551 ms
84 bytes from 192.168.2.2 icmp_seq=4 ttl=63 time=15.791 ms
84 bytes from 192.168.2.2 icmp_seq=5 ttl=63 time=16.011 ms

PC3>
```

Это скриншот из консоли четвертого компьютера, при отправке эхо-повтора третьему компьютеру через маршрутизатор.

```
PC4> ping 192.168.1.2

84 bytes from 192.168.1.2 icmp_seq=1 ttl=63 time=12.418 ms
84 bytes from 192.168.1.2 icmp_seq=2 ttl=63 time=15.732 ms
84 bytes from 192.168.1.2 icmp_seq=3 ttl=63 time=16.447 ms
84 bytes from 192.168.1.2 icmp_seq=4 ttl=63 time=16.686 ms
84 bytes from 192.168.1.2 icmp_seq=5 ttl=63 time=16.915 ms

PC4>
```

7. Перехватить трафик протокола arp и icmp на всех линках(nb!), задокументировать и проанализировать заголовки пакетов в программе Wireshark, для фильтрации трафика, относящегося к указанному протоколу использовать фильтры Wireshark



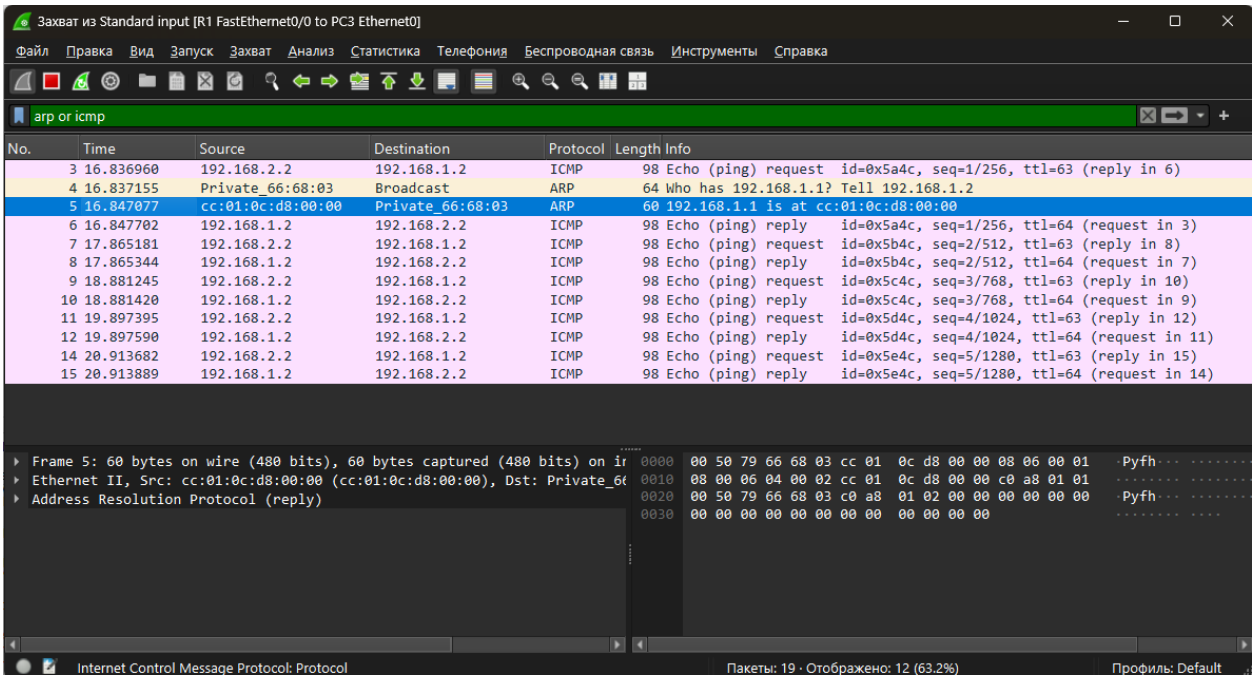
Описание перехваченного трафика протокола ARP:

Разбор полей:

- **No. (Номер пакета)** - Это номер пакета в списке.
- **Time (Время)** - Время, прошедшее с начала захвата трафика до момента получения пакета.
- **Source (Источник** - IP-адрес устройства, которое отправило пакет. В примере выше:
  - Для первого пакета: 192.168.1.1
  - Для второго пакета: 192.168.1.2
- **Destination (Назначение)** - IP-адрес устройства, к которому отправлен пакет:
  - Для первого пакета: 192.168.1.2
  - Для второго пакета: 192.168.1.1
- **Protocol (Протокол)** - Указывает, какой протокол был использован в пакете. В нашем случае это ARP.
- **Length (Длина)** - Размер пакета в байтах.
- **Info (Информация)** - Информация о типе ARP-пакета и дополнительной информации. Это ключевая часть, которая дает больше сведений о содержимом пакета:

Дальнейший разбор пакета:

- **Frame** - Количество байт и битов в кадре, а также время прибытия кадра в Wireshark.
- **Ethernet II** - Это Ethernet-кадр, где указаны MAC-адреса отправителя и получателя. В случае ARP-запроса, получатель (**Dst**) будет **Broadcast** (ff:ff:ff:ff:ff:ff), так как запрос направлен всем устройствам в сети.
- **Type** - Протокол, который используется в кадре. В данном случае это **ARP (0x0806)**.
- **Address Resolution Protocol** - Это сам протокол ARP.



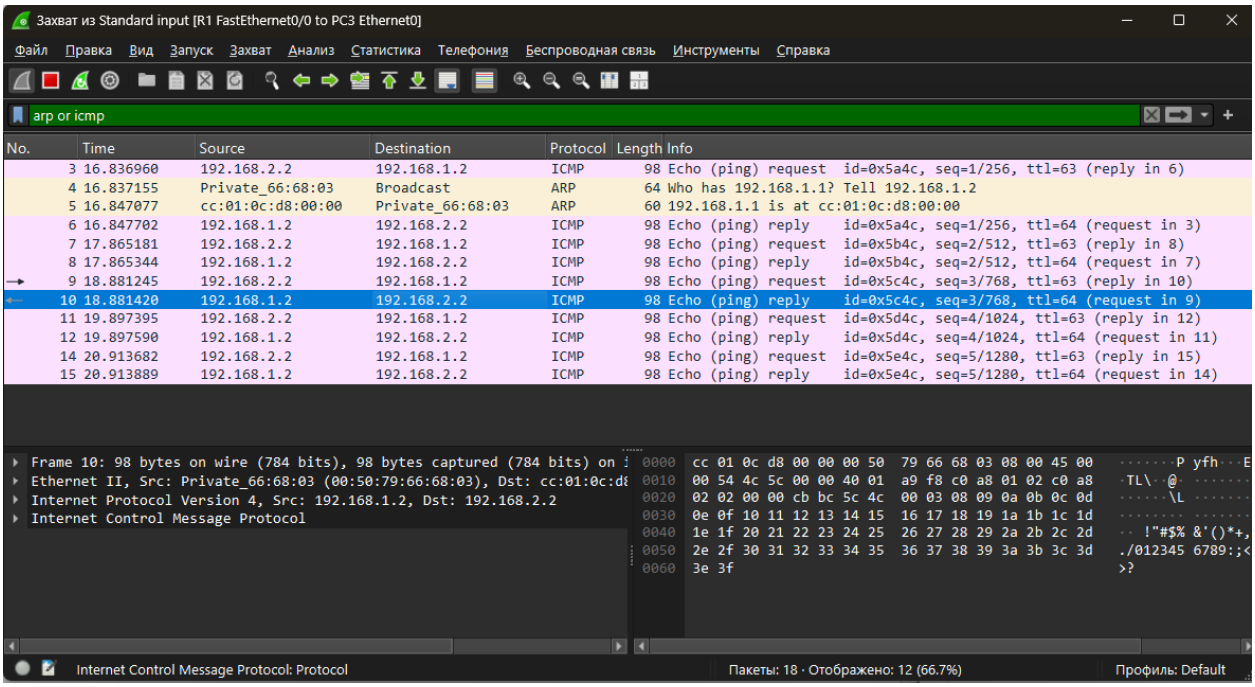
Описание перехваченного трафика протокола ICMP:

Разбор полей:

- **No. (Номер пакета)** - Это номер пакета в списке. Например, пакет №1 (Echo Request) и пакет №2 (Echo Reply).
- **Time (Время)** - Время, прошедшее с начала захвата трафика до момента получения пакета.
- **Source (Источник)** - IP-адрес устройства, которое отправило пакет. В примере выше:
  - Для первого пакета: 192.168.1.2
  - Для второго пакета: 192.168.2.2
- **Destination (Назначение)** - IP-адрес устройства, к которому отправлен пакет:
  - Для первого пакета: 192.168.1.2 адрес получателя Echo Reply).
  - Для второго пакета: 192.168.2.2 адрес отправителя Echo Reply).
- **Protocol (Протокол)** - Указывает, какой протокол был использован в пакете. В нашем случае это ICMP.
- **Length (Длина):** Размер пакета в байтах.
- **Info (Информация)** - Информация о типе ICMP-пакета и дополнительной информации. Это ключевая часть, которая дает больше сведений о содержимом пакета:
  - В строке для пакета *Echo Request* указано, что это *Echo (ping) request* с идентификатором id=0x5a4c, последовательностью seq=1/256 и временем жизни 64.
  - В строке для пакета *Echo Reply* указано, что это *Echo (ping) reply* с теми же параметрами id=0x5a4c и seq=1/256.

Дальнейший разбор пакета:

- **Frame** - Количество байт и битов в кадре, а также время прибытия кадра в Wireshark.
- **Ethernet II** - Это Ethernet-кадр, где указаны MAC-адреса отправителя и получателя.
- **Type** - Протокол, который используется в кадре.
- **Internet Control Message Protocol** - Это сам протокол ICMP.


Захват из Standard input [R1 FastEthernet0/0 to PC3 Ethernet0]
Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка
arp or icmp
No. Time Source Destination Protocol Length Info
3 16.836960 192.168.2.2 192.168.1.2 ICMP 98 Echo (ping) request id=0x5a4c, seq=1/256, ttl=63 (reply in 6)
4 16.837155 Private_66:68:03 Broadcast ARP 64 Who has 192.168.1.1? Tell 192.168.1.2
5 16.847077 cc:01:0c:d8:00:00 Private_66:68:03 ARP 60 192.168.1.1 is at cc:01:0c:d8:00:00
6 16.847702 192.168.1.2 192.168.2.2 ICMP 98 Echo (ping) reply id=0x5a4c, seq=1/256, ttl=64 (request in 3)
7 17.865181 192.168.2.2 192.168.1.2 ICMP 98 Echo (ping) request id=0x5b4c, seq=2/512, ttl=63 (reply in 8)
8 17.865344 192.168.1.2 192.168.2.2 ICMP 98 Echo (ping) reply id=0x5b4c, seq=2/512, ttl=64 (request in 7)
9 18.881245 192.168.2.2 192.168.1.2 ICMP 98 Echo (ping) request id=0x5c4c, seq=3/768, ttl=63 (reply in 10)
10 18.881420 192.168.1.2 192.168.2.2 ICMP 98 Echo (ping) reply id=0x5c4c, seq=3/768, ttl=64 (request in 9)
11 19.897395 192.168.2.2 192.168.1.2 ICMP 98 Echo (ping) request id=0x5d4c, seq=4/1024, ttl=63 (reply in 12)
12 19.897590 192.168.1.2 192.168.2.2 ICMP 98 Echo (ping) reply id=0x5d4c, seq=4/1024, ttl=64 (request in 11)
14 20.913682 192.168.2.2 192.168.1.2 ICMP 98 Echo (ping) request id=0x5e4c, seq=5/1280, ttl=63 (reply in 15)
15 20.913889 192.168.1.2 192.168.2.2 ICMP 98 Echo (ping) reply id=0x5e4c, seq=5/1280, ttl=64 (request in 14)
Frame 10: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on i
Ethernet II, Src: Private_66:68:03 (00:50:79:66:68:03), Dst: cc:01:0c:d8
Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.2.2
Internet Control Message Protocol
0000 cc 01 0c d8 00 00 00 50 79 66 68 03 08 00 45 00 ·····P yfh··E
0010 00 54 4c 5c 00 00 40 01 a9 f8 c0 a8 01 02 c0 a8 ·TL\··@· ····
0020 02 02 00 00 cb bc 5c 4c 00 03 08 09 0a 0b 0c 0d ·····\L ····
0030 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d ···· ····
0040 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d ·· !"#$% &'()*+,
0050 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d ./012345 6789:;<
0060 3e 3f >?
Internet Control Message Protocol: Protocol
Пакеты: 18 · Отображено: 12 (66.7%)
Профиль: Default