

## Урок 5. Транспортный уровень

1. Работа в Wireshark. Запустить Wireshark, выбрать любой веб-сайт, определить IP-адрес сервера, отфильтровать в Wireshark трафик по этому IP-адресу. Набрать адрес сервера в строке браузера. Сколько TCP-соединений было открыто и почему. В работе можно использовать источник 1 из списка дополнительных материалов.
2. Настроить перегруженный NAT в предложенной схеме в Cisco Packet Tracer. С помощью режима симуляции удостовериться, что при подключении на веб-сервер происходит подмена IP-адресов и портов. Посмотреть таблицу трансляции NAT на маршрутизаторе.

### 1. Работа в Wireshark

- Сайт *gb.ru*      *ping gb.ru*      (178.248.232.209)
- *ip.src == 178.248.232.209*

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The packet capture filter is set to `ip.src == 178.248.232.209`. The packet list pane shows a series of ICMP Echo (ping) replies from source 178.248.232.209 to destination 10.0.2.15. The selected packet (No. 2) is expanded in the packet details pane, showing the following structure:

- Ethernet II, Src: RealtekU\_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu\_0f:93:bf (08:00:27:0f:93:bf)
  - Source: RealtekU\_12:35:02 (52:54:00:12:35:02)
  - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 178.248.232.209, Dst: 10.0.2.15
- Internet Control Message Protocol

The packet bytes pane shows the raw data of the selected packet. The bottom status bar indicates that 802.11 packets are displayed, with 1840 (22.8%) of the total data shown.

## 2. Настроить перегруженный NAT в предложенной схеме в Cisco Packet Tracer

Файл DZ5 (18) hw v1.pkt загрузил

- *Примечание:* не будем анонсировать 192.168.1.0 сеть (она скрыта будет за NAT), но необходимо анонсировать сеть 70.70.70.0, иначе не получим данные о сетях от маршрутизатора Router1.

