

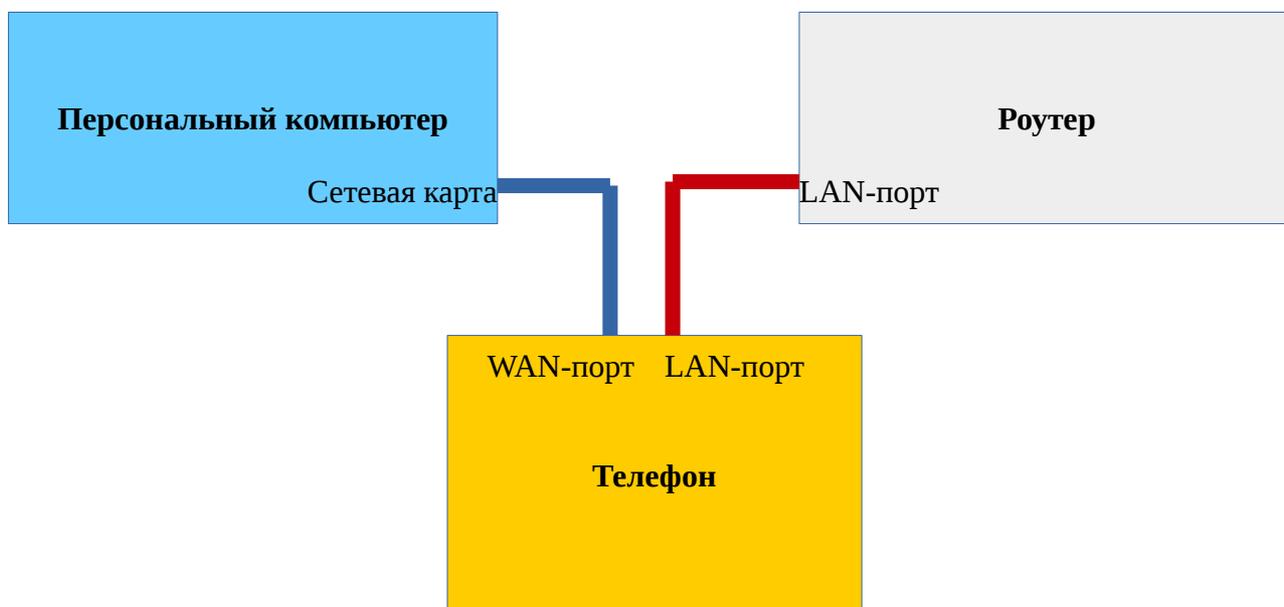
Анализ трафика телефона

Программа **Wireshark** предназначена для снятия трафика. Основным её достоинством является наглядность анализируемых данных. Существуют различные топологии систем, которым может потребоваться анализ трафика.

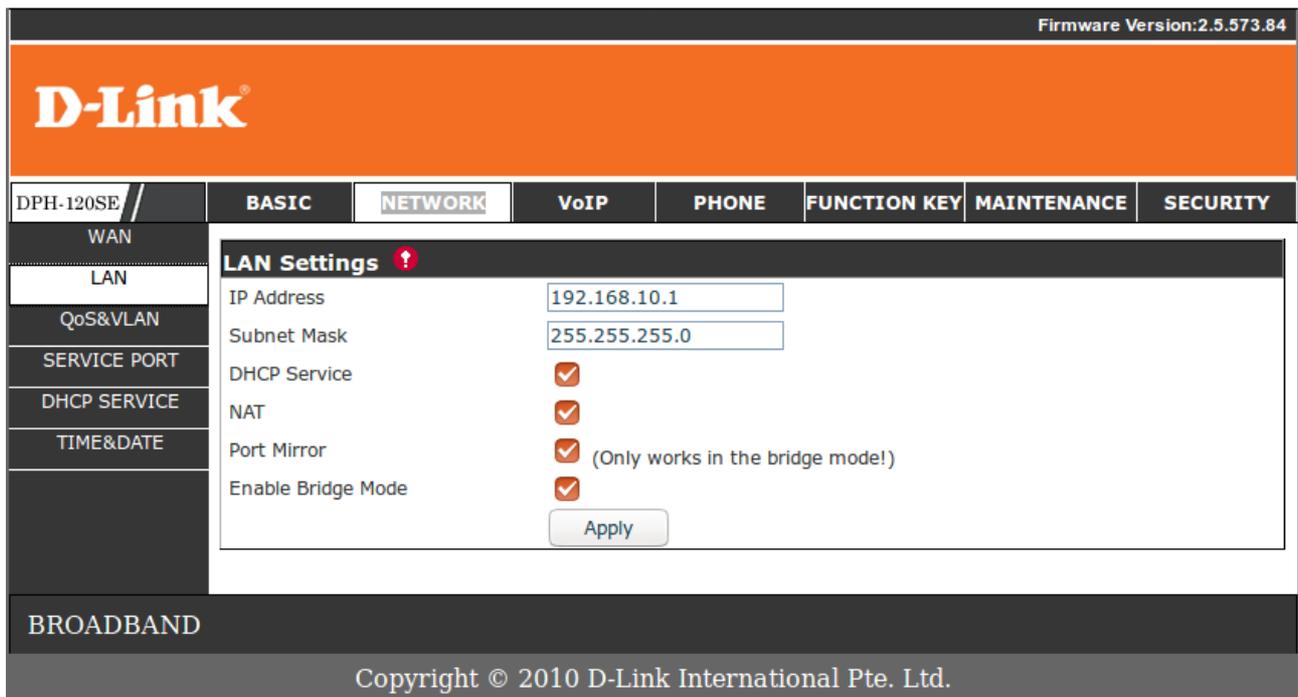
В данном примере рассматривается настройка следующего вида: телефон DPH-120 (это может быть любой другой телефон серии D-Link аппаратной ревизий F3 и выше), который подключен к роутеру через WAN-порт и к сетевой карте компьютера через LAN-порт. При этом на телефоне и на сетевой карте компьютера настроены следующие параметры:

	Телефон	Сетевая карта
IP-адрес	192.168.8.1	192.168.8.2
Сетевая маска	255.255.255.0	255.255.255.0
Шлюз	192.168.8.254	192.168.8.254
Первичный DNS	8.8.8.8	8.8.8.8
Вторичный DNS	8.8.4.4	8.8.4.4

Стоит отметить, что адрес роутера совпадает с адресом шлюза настроек сетевой карты и телефона. Подключены между собой устройства таким образом, как показано на изображении:

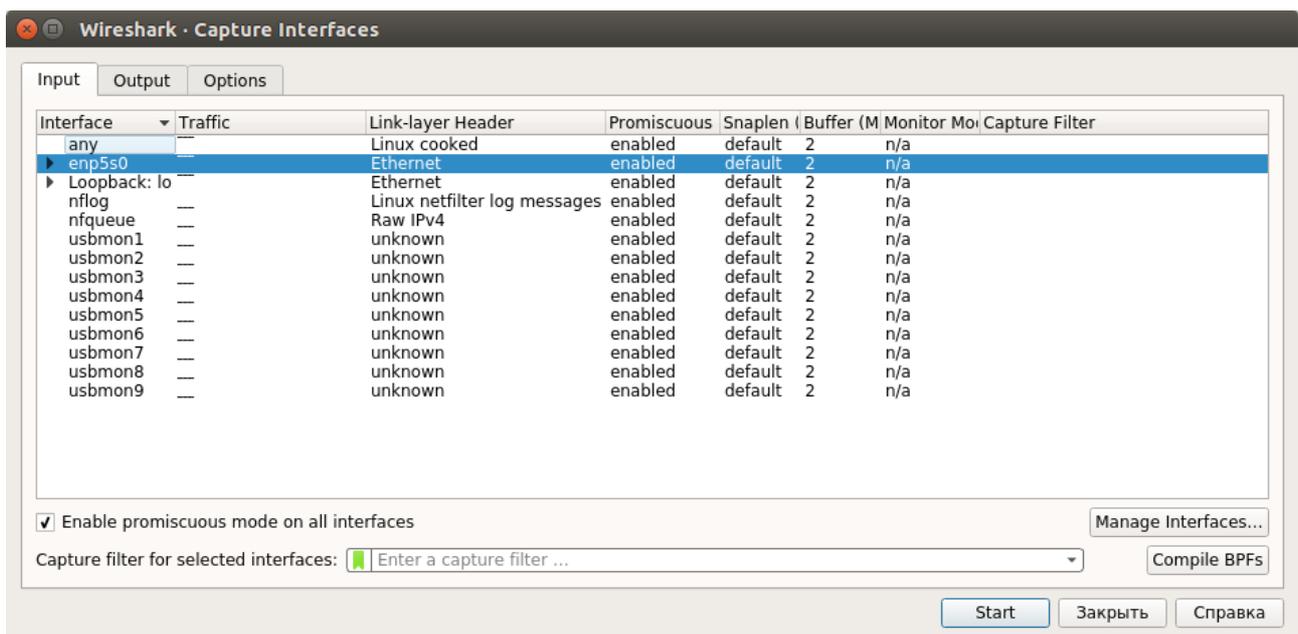


Чтобы настроить зеркалирование портов, заходим на страницу настройки телефона DPH-120 в пункт меню NETWORK — LAN, и там отмечаем галочками поля Port Mirror и Enable Bridge Mode:



После указанных действий внизу нужно применить изменения, нажав кнопку Apply. Когда эти действия будут завершены, зайти в раздел MAINTANCE — REBOOT и нажать кнопку Reboot для перезагрузки и корректного сохранения данных.

Теперь для получения трафика необходимо открыть предварительно установленную программу Wireshark, щёлкнуть по кнопке Capture Options  и выбрать интерфейс, с которого будет производиться снятие данных. В рассматриваемом случае это интерфейс сетевой карты enp5s0. После выбора, нажать внизу кнопку Start.



Для удобства, в верхнем окне программы Wireshark стоит выбрать протокол анализируемого трафика. Т.к. в данном примере рассматривается сигнальный VoIP трафик, выберем протокол SIP.



В случае, если всё будет настроено правильно, при звонке с этого телефона, в окне программы Wireshark появятся строки следующего вида:

