Федеральное государственное бюджетное образовательное учреждение

Высшего образования

Дальневосточный государственный университет путей сообщений

Кафедра: «ИТиС»

Лабораторная работа №1

Установка и настройка сниффера

«Wireshark»

Выполнил: Жифарский Д.А. 23К

Проверил: Епанешников В.Д.

г. Хабаровск

2017 г

**Цель работы:** получение практических навыков установки и на­стройки программы перехвата сетевых пакетов на примере сниффера **Wireshark.**

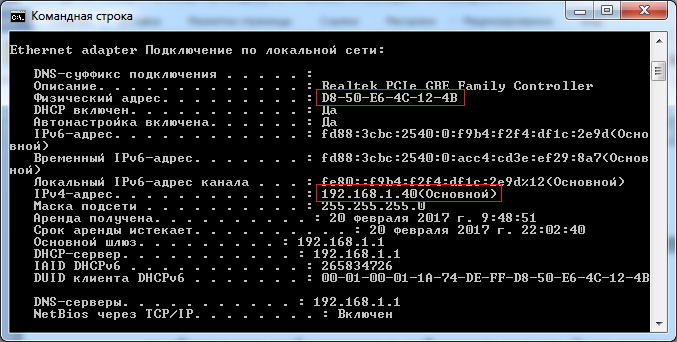
**Краткие теоретические сведения:**

Wireshark — это программа для анализа протоколов (анализатор пакетов), которая используется для поиска и устранения неполадок в сети, анализа, разработки программного обеспечения и протоколов, а также обучения. По мере движения потоков данных по сети анализатор перехватывает каждый протокольный блок данных (PDU), после чего расшифровывает или анализирует его содержание согласно соответствующему документу RFC или другим спецификациям.

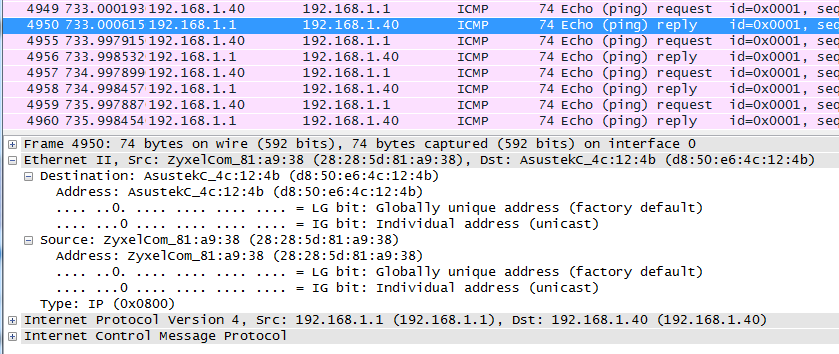
Wireshark — полезный инструмент для всех, кто работает с сетями. Его можно использовать для анализа данных, а также для поиска и устранения неполадок при выполнении большинства лабораторных работ в рамках курсов CCNA. В данной лабораторной работе содержатся инструкции по загрузке и установке программы Wireshark. Воспользуйтесь ими, если программа не установлена. В ходе лабораторной работы вы научитесь пользоваться программой Wireshark для перехвата IP-адресов пакетов данных ICMP и МАС-адресов Ethernet-кадров.

Ход выполнения работы.

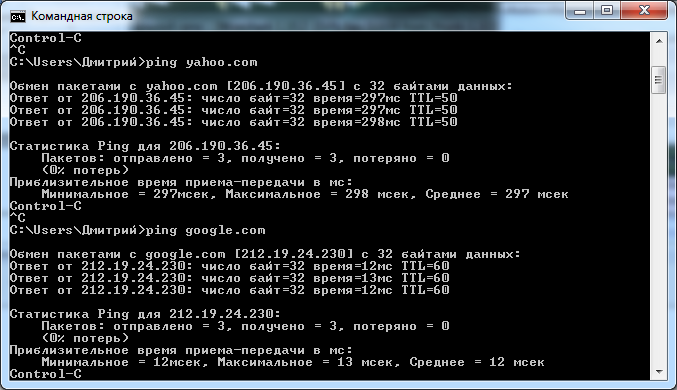
Результат команды ipconfig /all



Результат команды ping 192.168.1.1



Результат выполнения команды ping yahoo.com



1. yahoo.com

IP адрес: 206.190.36.45

MAC: 28:28:5D:81:A9:38

1. cisco.com

IP адрес: 72.163.4.161

MAC: 28:28:5D:81:A9:38

1. google.com

MAC: 28:28:5D:81:A9:38

MAC адреса у этих источников соответствуют MAC адресу шлюза, застроенном на компьютере.

Вывод: в ходе выполнения данной лабораторной работы были получены практические навыки по установке и настройке программы перехвата сетевых пакетом на примере сниффера Wireshark, а также проанализированы результаты его работы после выполнения ICMP запросов.