# 实验1 Ethernet及ARP网络协议分析与验证

## 实验目的：

1. 理解DIX Ethernt V2 帧结构。
2. 验证ARP协议的请求报文和响应报文结构
3. 学习常用网络协议分析工具wireshark

## 实验内容：

1. 使用wireshark捕获数据包
2. 分析数据包结构；

## 实验环境（包括拓扑结构图及参数）：

windows操作系统；交换机；wireShark软件

## 实验步骤：

**1、启动wiresshark，开始数据包捕获。**

**2、打开cmd窗口（以管理员身份运行），键入如下命令：ping** [**www.baidu.com**](http://www.baidu.com)**（备注：每位同学自己选择ping的目标主机：实验报告删除备注文字）**

****

仔细观察本计算机与[www.baidu.com](http://www.baidu.com) 主机在数据链路层的交互帧回答一下问题：

(1)任选一个本计算---》[www.baidu.com](http://www.baidu.com)链路层帧，分析结构。

(2) 任选一个[www.baidu.com---](http://www.baidu.com---)>本主机的链路层帧，分析结构。

(3) 数据链路层帧的目的地址一定是你所Ping的主机MAC地址吗？什么时候是？什么时候不是？

3、**启动wiresshark，开始数据包捕获。打开cmd窗口（以管理员身份运行），键入如下命令：arp -d，删除ARP高速缓存。键入如下命令：ping** [**www.baidu.com**](http://www.baidu.com)**。在wiresshark条件过滤栏输入arp。回答如下问题：**

(1) 分析一对ARP请求报文和响应报文的结构，并给出没有字段的含义

(2) 哪里看出ARP请求报文是广播类型的报文？

(3) 清除ARP高速缓存内容(arp -d \*)， ping 实验组内的另外一台实验机器(或互联网中的一台主机)，查询高速缓存（arp -a）的变化

实验总结

# 实验2 ICMP协议分析

## 实验目的：

1. 理解ICMP询问报文和差错报告报文的过程。
2. 了解ICMP包的格式

## 实验内容：

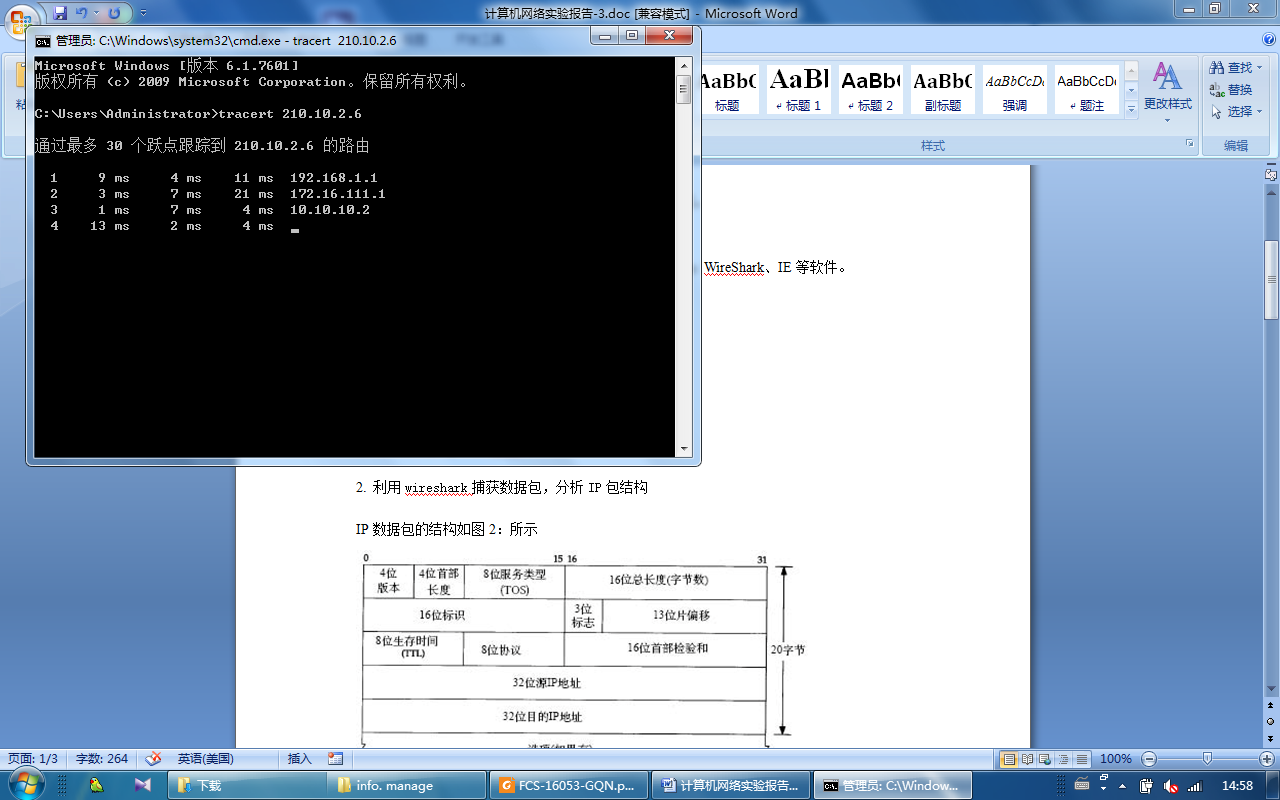
1. 使用命令或工具构造ping（ICMP）包；
2. 利用wireshark捕获数据包并分析数据包内容。

## 实验环境（包括拓扑结构图及参数）：

与因特网连接的计算机网络系统；操作系统为windows；WireShark、IE等软件。

## 实验步骤：

1. 启动wireshark捕获数据包软件。
2. 利用trace route 命令跟踪路由，命令如下。



3. 利用wireshark捕获数据包，分析IP及ICMP包结构。

4. 分析路由跟踪的过程。

5. 选择一个差错报告报文并分析其结构

实验总结