

# 第三讲

计算机网络原理实验

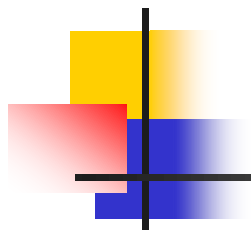
---

李勇军

# 本节实验内容

- 实验内容1：网络协议分析与验证
  - 实验五（P271）
  - 实验第6章（P197-P218）
- 实验内容2：网络广播报文发送编程
  - 实验内容6（P274）





# 实验内容1：网络协议分析与验证

## （P271）

教材第6章内容： P197–P218

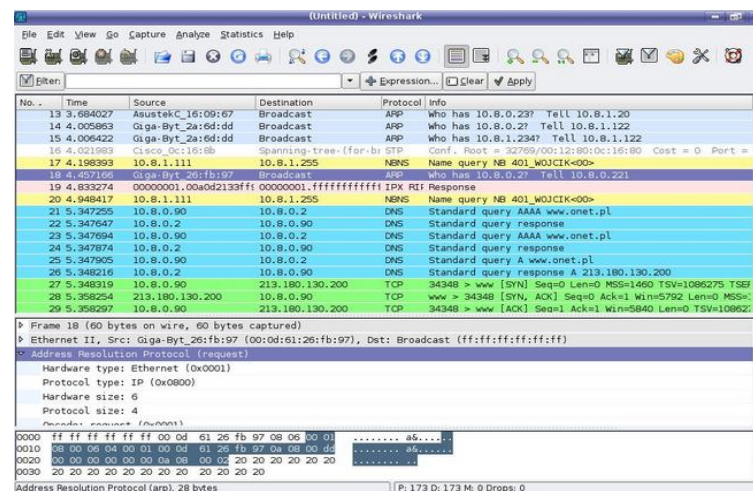
# 实验内容1:网络协议分析与验证

## 1、实验要求

- 每位同学独立;
- 提交文档: 实验报告

## 2、实验环境

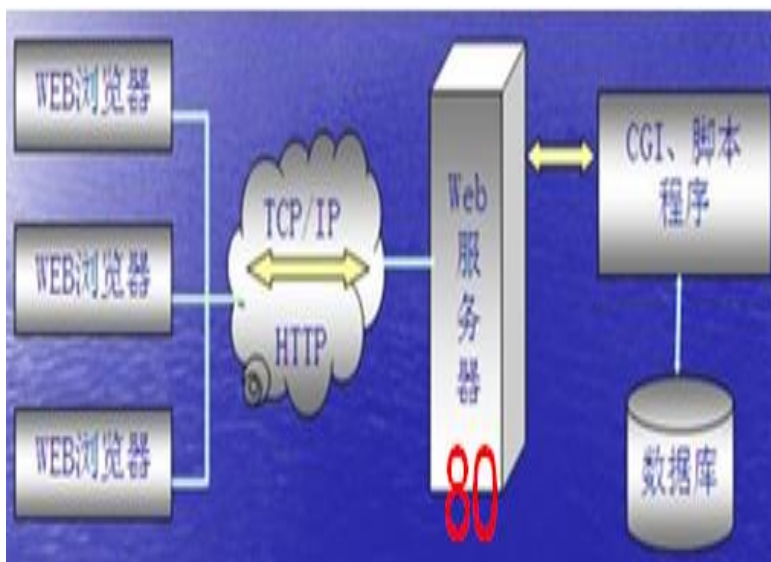
- WIN XP
- WINPCAP工具
- 抓包工具:Wireshark or  
Ethereal (选择一个工具即可)



# 实验内容1:网络协议分析与验证

## ■ 3、实验目的

- (1) 以用户访问一个**WEB**网站首页为例，从应用层、传输层、网络层以及数据链路层分析网络为**WEB**服务提供的技术支持以及工作原理。

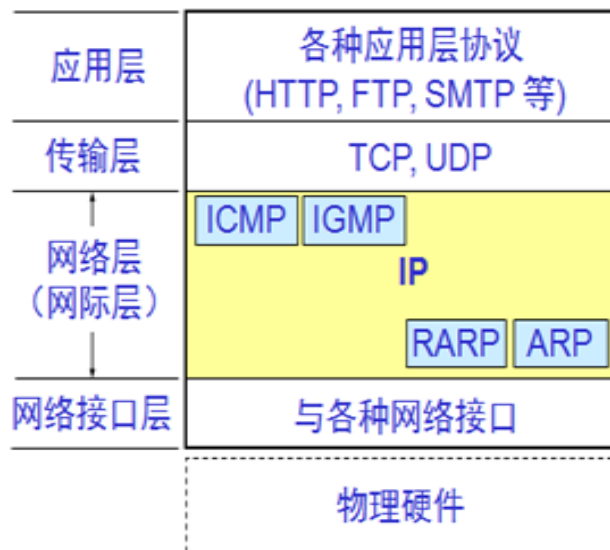
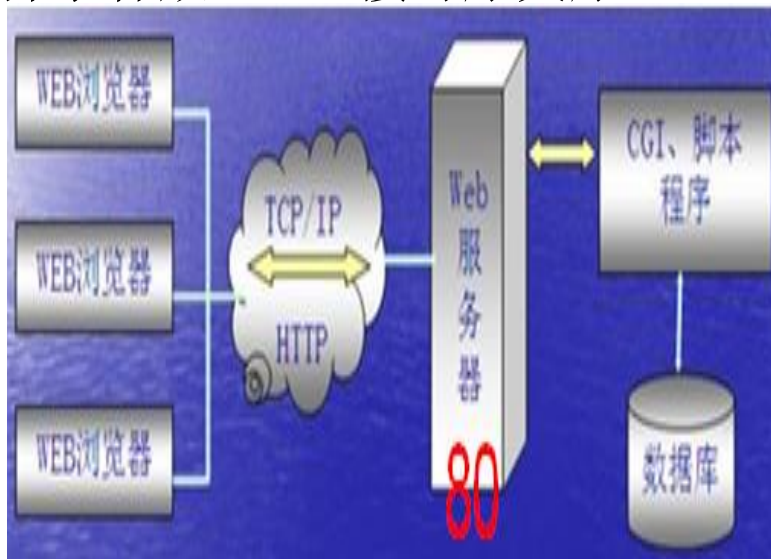


应用层	各种应用层协议 (HTTP, FTP, SMTP 等)
传输层	TCP, UDP
网络层 (网际层)	ICMP IGMP IP RARP ARP
网络接口层	与各种网络接口
	物理硬件

# 实验内容1:网络协议分析与验证

## ■ 3、实验目的

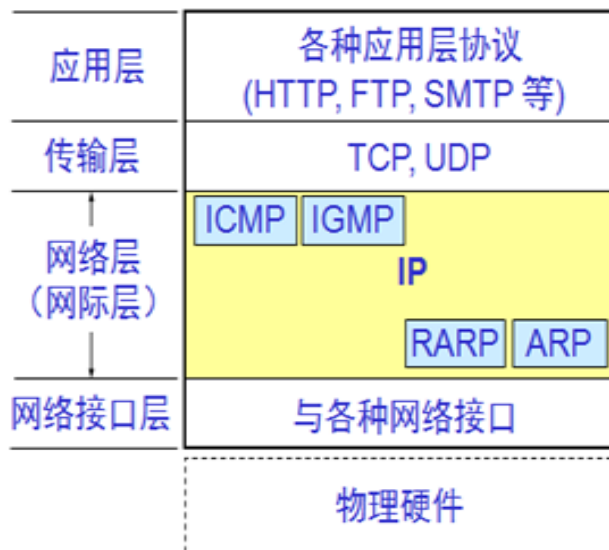
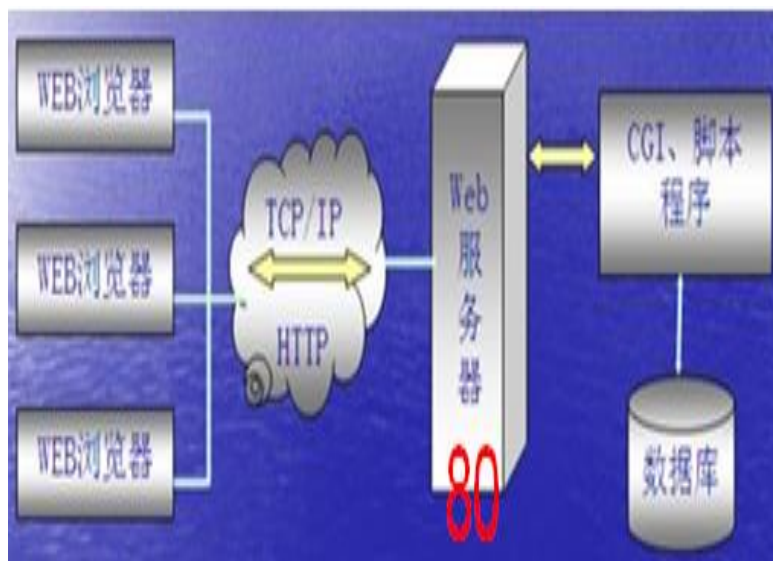
- （2）通过wireshark抓包工具抓取Web服务过程的数据报文，分析DNS、WEB协议工作原理；
- （3）分析TCP协议通过三次握手建立连接时序关系，以及通过四次挥手释放TCP连接时序关系。



# 实验内容1:网络协议分析与验证

## ■ 3、实验目的

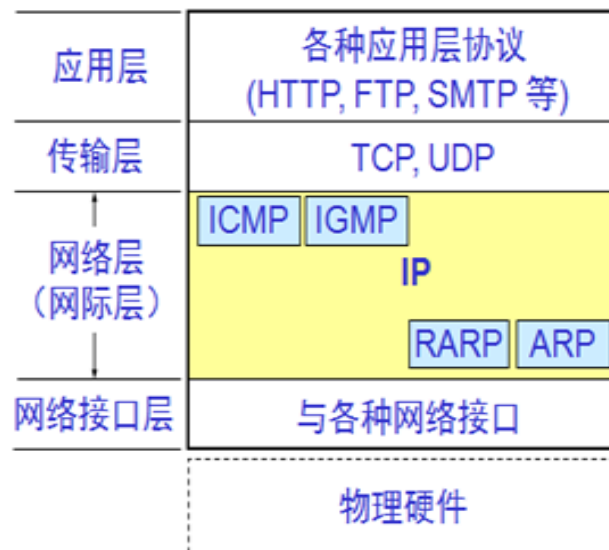
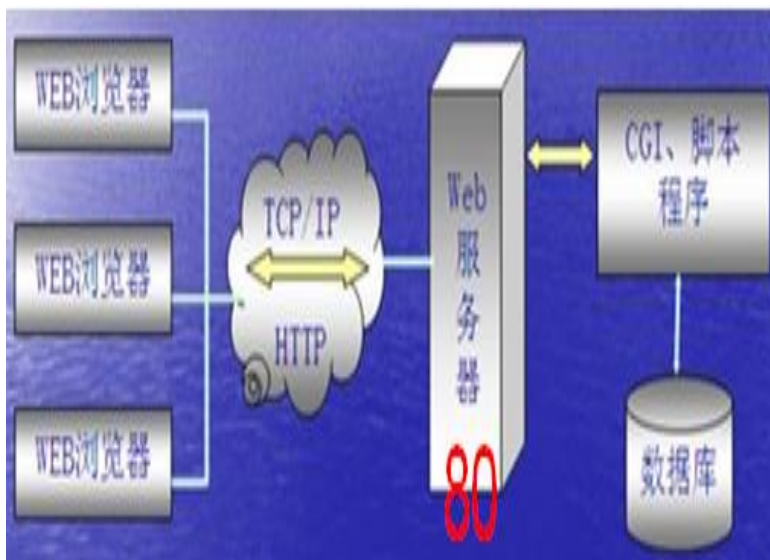
- (4) 分析ARP协议工作原理
- (5) 分析数据链路层工业以太网工作原理（数据帧的语法）



# 实验内容1:网络协议分析与验证

## ■ 4、实验内容

- 学习wireshark或etheral工具使用方法;
- 用户访问[www.baidu.com](http://www.baidu.com)网站首页, 并对完整通信过程抓包;
- 通过对抓取数据包进行分析, 深入理解网络协议工作原理;







# 实验内容1:网络协议分析与验证

## ■ 5、实验原理

- 学习wireshark或etheral工具使用方法（教材第6章）；分析用户客户端浏览器获得[www.baidu.com](http://www.baidu.com)网站首页过程中，网络通信流程。

第一步：调用DNS协议获得域名对应IP地址；

第二步：TCP协议通过三次握手建立TCP连接；

第三步：客户端向WEB服务器发送HTTP请求报文；

第四步：WEB服务器接收到HTTP请求报文并进行处理；

第五步：WEB服务器将[www. baidu. com](http://www.baidu.com)网站首页通过HTTP应答发送给客户端；

第六步：TCP协议通过四次挥手释放TCP连接；

第七步：客户浏览器的对HTTP应答进行解析，并在屏幕上显示解析结果；

对以上过程报文进行捕获，说明DNS协议、ARP协议和HTTP协议工作原理；为什么说在通过过程中会用到DNS、HTTP、TCP、UDP、ICMP、IP、ARP以及数据链路层工业以太网协议等，分析每个协议在此通信过程的作用。



# 实验内容1:网络协议分析与验证

---

## ■ 6、实验要求

- （1）对**DNS**请求报文、**HTTP**请求报文从应用层到数据链路层不同协议单元首部各个字段进行解释说明；
- （2）对**TCP**连接请求报文从传输层到数据链路层不同协议单元首部各个字段进行解释说明；
- （3）对**ARP**请求报文和应答报文从网络层到数据链路层不同协议单元首部各个字段进行解释说明；



# 实验内容1:网络协议分析与验证

---

## ■ 6、实验要求

- (4) 通过对捕获的数据包进行分析, 提供证据, 说明如何获得以下信息:
  - 1) [www.baidu.com](http://www.baidu.com) 对应的IP地址;
  - 2) 网关IP地址和MAC地址;
  - 3) 发送方和接收方TCP协议协商的初始序号? 发送数据的实际起始序号是多少?
  - 4) HTTP协议协商的版本号是多少? 该版本号HTTP协议工作特点是什么?
  - 5) 一个TCP连接从建立到释放, 总共发送和接收了多少字节数据?
  - 6) 针对一个TCP连接, 提供该连接建立三次握手报文段和四次挥手报文段, 为什么说该证据是针对一个TCP连接?



# 实验内容1:网络协议分析与验证

---

## ■ 6、实验要求

- (5) 以HTTP请求报文为例子，当WEB服务器接收到该报文后，接收方从数据链路层到应用层如何知道不同层数据字段的长度，开始和起始位置。
- (6) 从应用层到数据链路层有哪些校验字段，分别采用什么方法计算校验码，其校验范围分别是什么，不同层重复的校验是多余的吗？
- (7) 如果在本次实验过程，对抓取的报文进行分析，发现DNS和ARP协议没有工作，为什么？如何解决该问题？在解决该问题过程中用到两个网络命令，分别是什么，写出这两个命令具体应用。
- (8) 如果在本次实验过程，用户在客户端DOS>ping [www.baidu.com](http://www.baidu.com),连续发送了三次ICMP ECHO请求报文，但显示第一次接收ICMP ECHO应答报文超时，说明网络不同；但后面两次ICMP ECHO应答报文接收正常，又说明网络是连通的，为什么？



# 实验内容1:网络协议分析与验证

## ■ 7、实验步骤

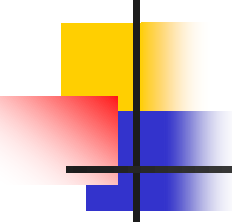
- (1) 安装WINPCAP组件;
- (2) 安装wireshark抓包工具;
- (3) 启动wireshark抓包工具, 并激活的网络接口上开始抓包;
- (4) 用户在浏览器地址栏输入: [www.baidu.com](http://www.baidu.com)回车, 直到百度首先在浏览器上显示为止;
- (5) 抓包结束, 开始对报文分析, 对实验要求内容找到报文证据。

## ■ 8、助教检查点

检查点1: 抓到DNS请求报文和对应的DNS应答报文;

检查点2: 抓到ARP请求报文和对应的ARP应答报文;

检查点3: 抓到一个TCP连接建立三次握手报文段; 抓到检查点3对应的TCP连接四次挥手释放报文段;



---

# 实验内容2：网络广播报文发送编程

## 实验六：P274



# 实验内容2:网络广播报文发送

---

- 1、实验要求
  - 两个同学一组;
  - 提交文档: 实验报告
- 2、实验环境
  - WIN XP
  - C, C++, VC++, VISUAL STUDIO;



# 实验内容2:网络广播报文发送

---

## ■ 3、实验内容

- 编写程序，发送三层广播报文；
- 在另一台利用抓包工具，抓取广播报文，并对报文首部进行分析；

## ■ 4、实验要求

- (1) 从抓取的报文中过滤出源IP = 发送方IP地址的某一个报文（可以手动或者采用过滤器）；
- (2) 分析广播报文传输层采用UDP/TCP，理解广播或者组播为什么不是TCP？
- (3) 抓取发送的广播报文，找出通信的五元组信息和数据帧首部信息，分析目的IP地址、源IP地址、协议类型、目的MAC地址、源MAC地址等与单播UDP用户数据报的不同。





# 助教检查点及记录分数

助教实验检查点：

检查点1：抓取发送的第一个广播报文，找出通信的五元组信息和数据帧首部信息，分析目的IP地址、源IP地址、协议类型、目的MAC地址、源MAC地址等与单播UDP用户数据报的不同。

- 两个同学为一组；
- 当完成一个检查点时，主动要求助教检查，助教对检查间完成情况进行记录，并记录好完成时间。



# 实验报告

---

- 按照格式要求，撰写2次实验的报告，并发送至课程群公告中指定的邮箱。
  - 2个报告放在一个文件中，按照统一要求命名
  - 实验报告雷同者均为0分
  - 截至日期为11月25日