《计算机网络协议分析》

实验指导书

暨南大学计算机科学系实验中心

2021 年 08 月

（内部教学，请勿外传）

前言

《网络协议分析》课程是针对计算机网络工程专业的本科生而设置的一门课程，它具有很强的理论性和实践性。本实验指导书是专门为《网络协议分析》理论课程配套的、指导学生完成相关实验及操作而编写的。

本实验指导书按照 TCP/IP 的层次结构对网络互连中的主要协议进行分析，由下而上的设计了 14 个实验，涉及协议分析软件的使用、数据链路层协议分析、网络层协议分析、传输层协议分析、应用层协议分析等，共五个部分。希望学生们通过以上实验进一步加深对网络协议的理解和掌握协议分析的方法。

根据不同的要求,可以在本指导书的范围内选择相应的实验内容，组合成满足不同需求的实验指南。如 16 学时的实验可采用：以太网链路层帧格式分析实验、ICMP 协议分析实验、IP 协议分析实验、ARP 协议分析实验、TCP 协议分析实验、UDP 协议分析实验、FTP 协议分析实验、HTTP 协议分析实验等 8 个实验组合；8 学时的实验可采用：以太网链路层帧格式分析实验、IP 协议分析实验、TCP 协议分析实验、FTP 协议分析实验等 4 个实验组合；其余的实验可以作为任选实验或者课下作业。

特别说明：

1、本指导书中给出的实验网络物理模型，不需要学生动手搭建，所有网络物理模型都基于现有的实验室运行环境。

2、本指导书中网络物理模型中所用到的交换机和路由器均为锐捷设备，这里只是为举例方便。如果改换为 CISCO 或者华为等的相应设备，不影响本实验的步骤和结果。

3、由于我系专业实验室的实验环境有限，本指导书中也有些实验暂时还不完全支持，如：VLAN 802.1Q 帧格式分析实验；有些实验中所需要的软件名称和版本与实际环境中稍有差别，不需更改；若有需要重新安装或者改用其它的软件代替的，应该根据当堂实验课的指导老师的安排来进行。

4、实验中设备的 ip 地址以实际实验机器的 ip 地址为准，对应指导书中网络实验模型中的 ip 地址。

注：本材料参考重庆邮电大学黄梅根老师编写的《网络协议分析实验指导书》，以及中软吉大编写的《网络协议教学实验教程》，若涉及到版权，请联系我们！

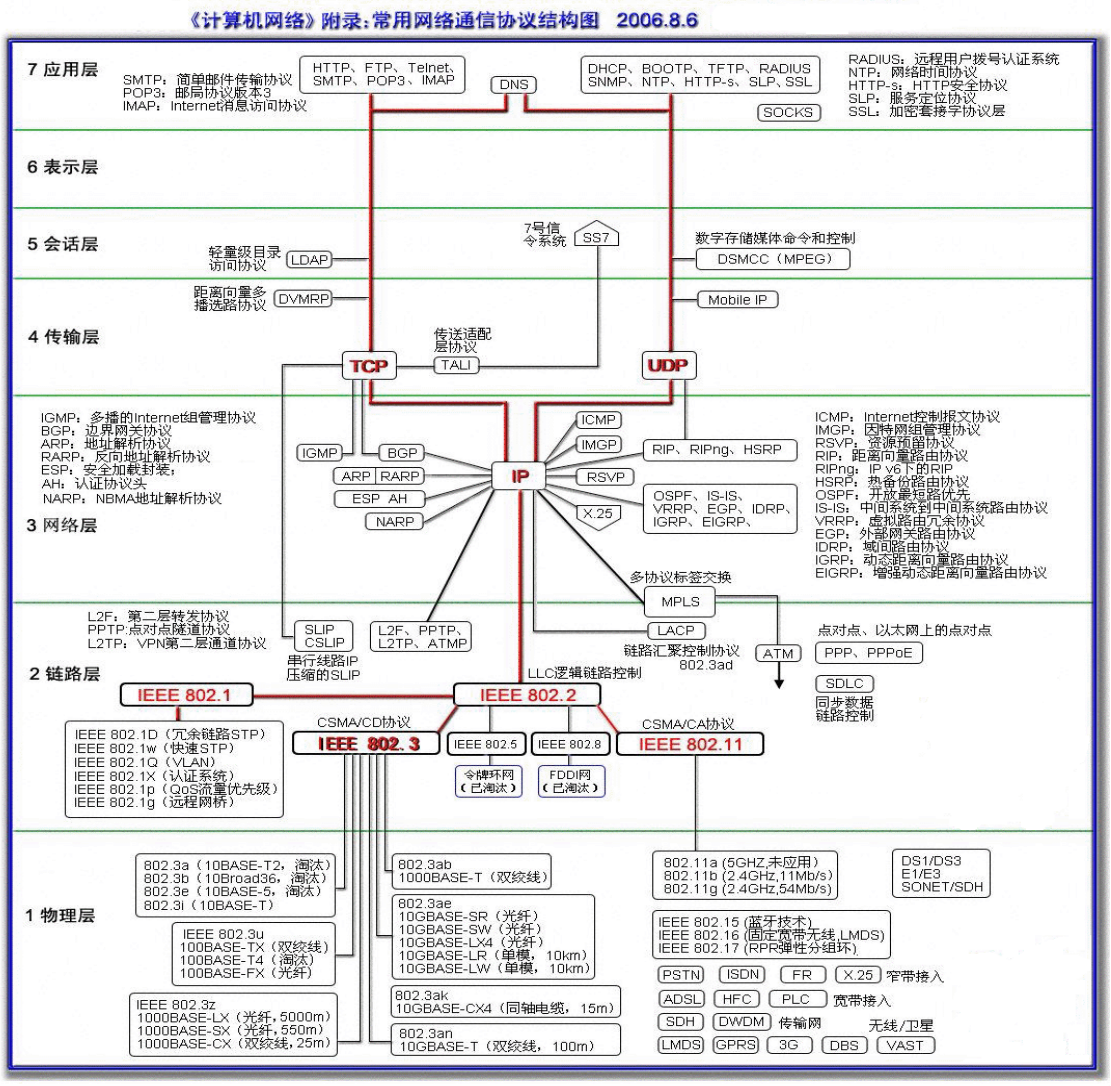
目　录

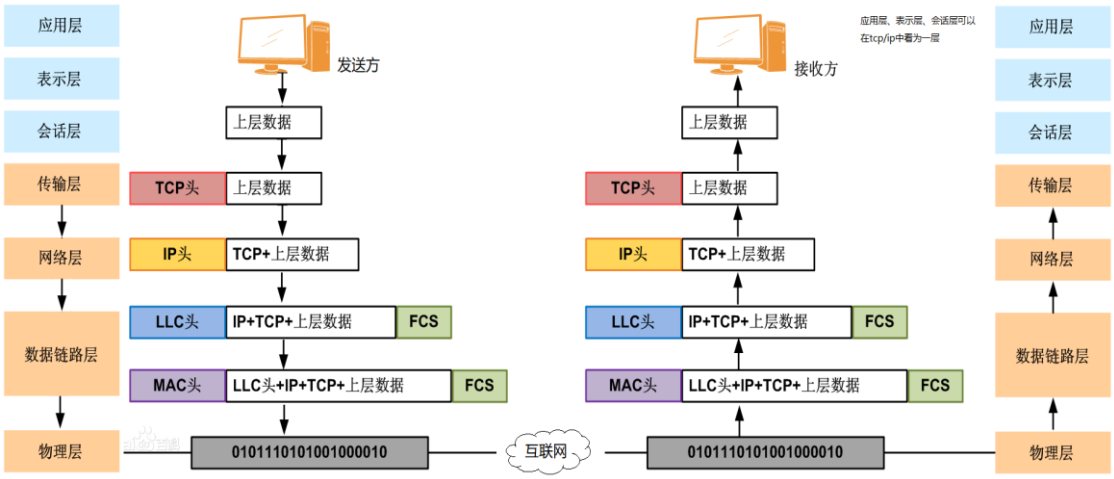
1. 网络协议分析实验环境要求

（1）本指导书按照 TCP/IP 的层次结构对网络互连中的主要协议进行分析。本章实验的基本思路是使用协议分析工具从网络中截获数据报，对截获的数据报进行分析。通过试验，使学生了解计算机网络中数据传输的基本原理，进一步理解计算机网络协议的层次结构、协议的结构、主要功能和工作原理，以及协议之间是如何相互配合来完成数据通信功能的。

Windows 环境下常用的协议分析工具有：Snifer Pro、Natxray、Iris、Wireshark 以及 Windows 2000 自带的网络监视器。本书选用 Wireshark 作为协议分析工具。

（2）网络协议图





2.网络协议分析器 Wireshark

Wireshark（前称 Ethereal）是一个网络封包分析软件。网络封包分析软件的功能是撷取网络封包，并尽可能显示出最为详细的网络封包资料。Wireshark 使用 WinPCAP 作为接口，直接与网卡进行数据报文交换。在过去，网络封包分析软件是非常昂贵的，或是专门属于盈利用的软件。Ethereal 的出现改变了这一切。在 GNUGPL 通用许可证的保障范围底下，使用者可以以免费的途径取得软件与其源代码，并拥有针对其源代码修改及客制化的权利。Ethereal 是全世界最广泛的网络封包分析软件之一。

下载地址地址：https://www.wireshark.org/download.html，在官网我们既可以下载到最新的发布版本软件安装文件，也可以下载到以前发布的旧版本软件安装文件。Wireshark 支持多个操作系统，在下载安装文件的时候注意选择与自己 PC 的操作系统匹配的安装文件。下载完成后，按照软件提示一路 Next 安装。本节以 Wireshark 3.4.7 版本为依据。

2.1 Wireshark 主窗口简介

Wireshark 主窗口主要有显示过滤器、封包列表、封包详细信息、16 进制数据、地址栏。

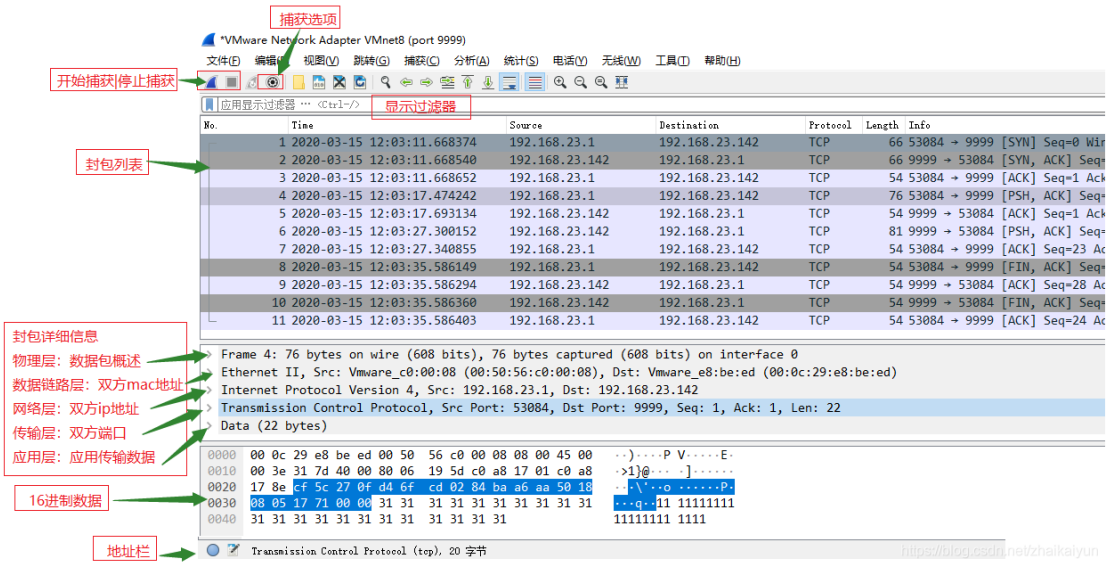


图 1　抓包完成后的 Wireshark 主窗口

其中：

1. Display Filter(显示过滤器)，　用于过滤

2. Packet List Pane(封包列表)，　显示捕获到的封包，　有源地址和目标地址，端口号。　颜色不同，代表

3. Packet Details Pane(封包详细信息)，显示封包中的字段

4. Dissector Pane(16 进制数据)

5. Miscellanous(地址栏，杂项)。

2.2 Wireshark 菜单栏简介

1 “文件”栏

“文件”栏的英文名为“File”，该菜单中包含了打开和合并捕获数据文件项、部分或全部保存/打印/导出捕获数据文件项以及退出应用程序选项等。

2 “编辑”栏

“编辑”栏的英文名为“Edit”，该菜单中包含了查找数据包、设置时间参考、标记数据包、设置配置文件、设置首选项等。需要注意的是，在“编辑”栏中，没有剪切、复制和粘贴等选项。

3 “视图”栏

“视图”栏的英文是“View”，该菜单主要用来控制捕获数据的显示方式。“视图”栏包括了数据包着色选项、缩放字体选项、在新窗口显示数据包选项、展开/折叠数据包细节选项等。

4 “跳转”栏
“跳转”栏的英文是“Go”，该菜单主要用来跳转到指定数据包。

5 “捕获”栏
“捕获”栏的英文是“Capture”，该菜单中包含了开始/停止捕获选项以及编辑包过滤条件选项等。

6 “分析”栏
“分析”栏的英文是“Analyze”，该菜单中包含了显示包过滤宏、启用协议、配置用户指定的解码方式以及追踪 TCP 流等选项。

7 “统计”栏
“统计”栏的英文是“Statistics”，可以显示各种统计窗口，这些统计窗口包括捕获文件的属性选项、协议分级选项以及显示流量图选项等。

8 “电话”栏
“统计”栏的英文是“Telephony”，可以显示与电话相关的统计窗口，这些统计窗口包括媒介分析、VoIP 通话统计选项以及 SIP 流统计选项等。

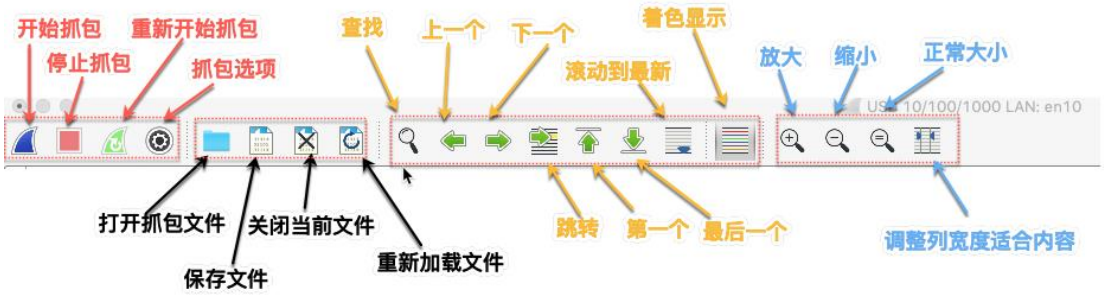
9 “无线”栏
“无线”栏的英文是“Wireless”，该栏用来显示蓝牙和无线网络的统计数据。

10 “工具”栏
“工具”栏的英文是“Tools”，该栏中包含了 Wireshark 中能够使用的工具。

11 “帮助”栏
“帮助”栏的英文是“Help”，该栏用于为用户提供一些基本的帮助，包括了说明文档选项、网页在线帮助选项以及常见问题选项等。

2.3 Wireshark 的工具栏

Wireshark 工具栏提供主菜单中常用的选项的快速访问。



- 打开接口列表对话框
- 打开捕捉选项对话框
- 使用最后一次的捕捉设置立即开始捕捉
- 停止当前捕捉
- 停止当前捕捉并立即重新开始
- 启动打开文件对话框，用于载入文件
- 保存当前文件为任意其他的文件，它将会弹出一个保存对话框（注：如果当前文件是临时未保存文件，图标将会显示为）
- 关闭当前文件。如果未保存，将会提示是否保存
- 重新载入当前文件
- 打印捕捉文件的全部或部分，将会弹出一个打印对话框
- 打开一个对话框，查找包
- 返回历史记录的上一个
- 跳转到历史记录中的下一个包
- 弹出一个设置跳转到指定的包的对话框
- 跳转到第一个包
- 跳转到最后一个包
- 切换是否以彩色方式显示包列表
- 开启/关闭实时捕捉时自动滚动包列表
- 增大字体
- 缩小字体
- 设置缩放大小为 100%
- 重置列宽，是内容适合列宽（使包列表内的文字可以显示）
- 打开对话框，用于创建、编辑捕捉过滤器
- 打开对话框，用于创建、编辑显示过滤器
- 定义以彩色方式显示数据包的规则
- 打开首选项对话框
- 打开帮助对话框

2.4 Wireshark 的网络数据抓包过程

Wireshark 的抓包有如下特征：

＊ 可以从不同类别的网络硬件抓包，如 Ethernet、 Token Ring、ATM 等；

＊ 停止抓包时不同的触发器相似：如抓获数据的总数、抓包时间，抓获包的数目；

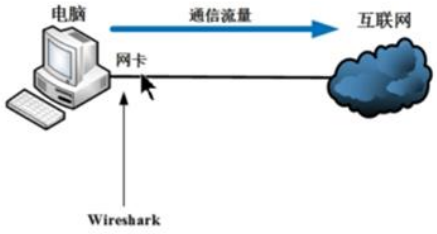
＊ 抓包过程中同时显示编译后 （解析）的包。

＊ 根据包过滤器的条件，从抓获的全部数据中进行过滤，减去符合条件的包。

抓包原理

(1) 网络原理

(a)本机环境：直接抓本机网卡进出流量



网卡(NIC)是局域网（LAN,全称是：Local Area NetWork）中连接计算机和传输介质的接口，它工作在物理层(L1）。它是处于主机箱内的一块网络接口板，因为它的存在，从而使得本机能够与外部局域网进行连接通信。任何一台计算机，想要进行上网、通信功能，就必须使用网卡。网卡的书面语是网络适配器/网络接口卡。LAN（局域网）可以使用以太网帧格式的以太网（Ethernet）协议标准进行通信。同时在网络中还可以使用支持该标准协议的交换机、路由器等。在使用线缆连接局域网 LAN 时候，个人计算机可以使用以太网(Ethernet）双绞线连接到交换机，然后交换机连接到路由器，而最终路由器处理跨越异构子网和发送至互联网进行通信。以太网上传输的数据在数据链路层（TCP/IP 网络模型或 OSI（Open Systems Interconnection）开发系统互联-网络模型）以数据帧（以太网帧-Ethernet II 格式）的形式存在。当本机发送数据时候，会将数据帧/MAC 帧并行写到网卡的缓存中，然后网卡对缓存中要传输的数据进行编码,并最终转换为传输媒介 UTP 线缆上的电气信号进行网络传输。

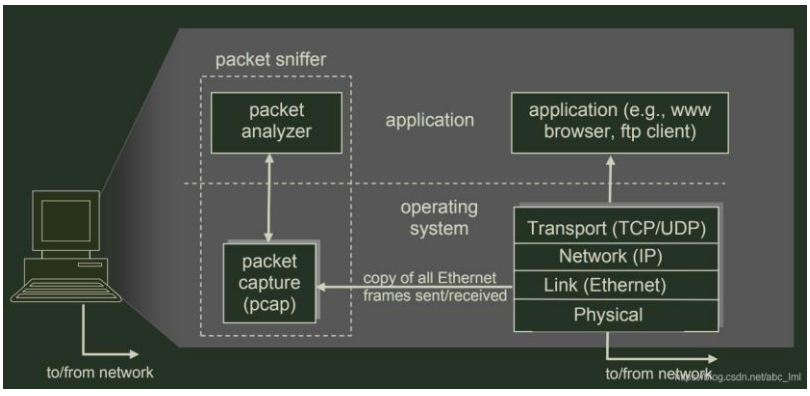
Wireshark 可以抓取你的电脑接受或发送的信息, 它获取的是你电脑应用或协议收\发的包的副本。下图展示的就是原理图，主要由两部分构成：packet capture library 和 packet analyzer。其中：

- packet capture library:

  可以获取你电脑收/发的所有的数据链路层帧的副本

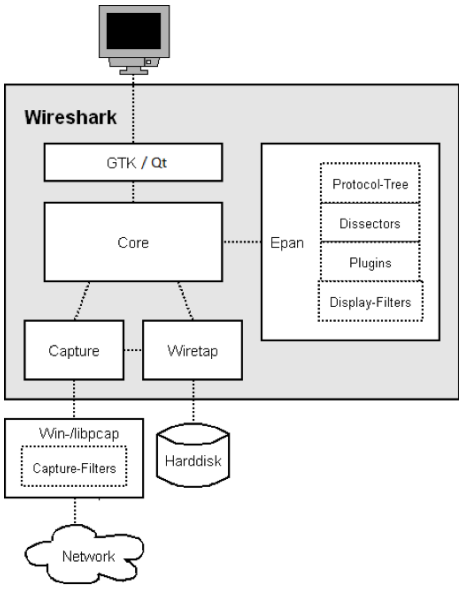
- packet analyzer:

  展示协议信息中所有字段的内容，所以它“知道”所有协议的信息交换的字段，例如以太网帧、IP、TCP、HTTP 等。



(2) 总体结构

wireshark 的总体结构如下图所示



主要功能模块包括：

模块名	功能	源码子目录
GTK/Qt	处理所有的用户输入/输出(所有的窗口,对话框等等)	/ui GTK: /ui/gtk Qt: /ui/qt
Core	主要的"粘合代码"(glue code),它把其他的块组合到一起	/
Epan (Ethereal Packet Analyzer)	协议树(Protocol-Tree) - 保存捕获文件的协议信息数据	/epan
	解析器(Dissectors) - 多种协议的解析器	/epan/dissectors
	插件(Plugins) - 一些用插件实现的协议解析器	/plugins
	显示过滤器(Display-Filters) - 显示过滤器引擎	/epan/dfilter
Wiretap	wiretap 库用于读/写 libpcap 格式或者其他文件格式的捕获文件	/wiretap
Capture	抓包引擎相关接口	/

Dumpcap	抓包引擎. 这是唯一需要提升权限来执行的部	/
WinPcap/libpcap	(不是 Wireshark 包的一部分) - 依赖于平台的包捕获库,包含捕获过滤器引擎.这就是我们为什么有不同的显示和捕获 两套过滤语法的原因 - 因为用了两种不同的过滤引擎	-

2.5 Wireshark 表达式规则

表达式规则

1. 协议过滤

比如 TCP，只显示 TCP 协议。

2. IP 过滤

比如 ip.src ==192.168.1.102 显示源地址为 192.168.1.102，

ip.dst==192.168.1.102, 目标地址为 192.168.1.102

3. 端口过滤

tcp.port ==80, 端口为 80 的

tcp.srcport == 80, 只显示 TCP 协议的愿端口为 80 的。

4. Http 模式过滤

http.request.method=="GET", 只显示 HTTP GET 方法的。

5. 过滤 MAC

太以网头过滤

eth.dst == A0:00:00:04:C5:84 // 过滤目标 mac

eth.src eq A0:00:00:04:C5:84 // 过滤来源 mac

eth.dst==A0:00:00:04:C5:84

eth.dst==A0-00-00-04-C5-84

eth.addr eq A0:00:00:04:C5:84 // 过滤来源 MAC 和目标 MAC 都等于 A0:00:00:04:C5:84 的

less than 小于 < lt

小于等于 le

等于 eq

大于 gt

大于等于 ge

不等 ne

6. http 模式过滤

例子:

http.request.method == “GET”

http.request.method == “POST”

http.request.uri == “/img/logo-edu.gif”

http contains “GET”

http contains “HTTP/1.”

// GET 包

http.request.method == “GET” && http contains “Host: “

http.request.method == “GET” && http contains “User-Agent: “

// POST 包

http.request.method == “POST” && http contains “Host: “

http.request.method == “POST” && http contains “User-Agent: “

// 响应包

http contains “HTTP/1.1 200 OK” && http contains “Content-Type: “

http contains “HTTP/1.0 200 OK” && http contains “Content-Type: “

7. TCP 参数过滤

tcp.flags 显示包含 TCP 标志的封包。

tcp.flags.syn == 0x02　显示包含 TCP SYN 标志的封包。

tcp.window_size == 0 && tcp.flags.reset != 1

常用的过滤表达式

常见用显示过滤需求及其对应表达式：

（1）数据链路层：

筛选 mac 地址为 04:f9:38:ad:13:26 的数据包----eth.src == 04:f9:38:ad:13:26

筛选源 mac 地址为 04:f9:38:ad:13:26 的数据包----eth.src == 04:f9:38:ad:13:26

（2）网络层：

筛选 ip 地址为 192.168.1.1 的数据包----ip.addr == 192.168.1.1

筛选 192.168.1.0 网段的数据---- ip contains "192.168.1"

筛选 192.168.1.1 和 192.168.1.2 之间的数据包----ip.addr == 192.168.1.1 && ip.addr == 192.168.1.2

筛选从 192.168.1.1 到 192.168.1.2 的数据包----ip.src == 192.168.1.1 && ip.dst == 192.168.1.2

（3）传输层：

筛选 tcp 协议的数据包----tcp

筛选除 tcp 协议以外的数据包----!tcp

筛选端口为 80 的数据包----tcp.port == 80

筛选 12345 端口和 80 端口之间的数据包----tcp.port == 12345 && tcp.port == 80

筛选从 12345 端口到 80 端口的数据包----tcp.srcport == 12345 && tcp.dstport == 80

（4）应用层：

特别说明----http 中 http.request 表示请求头中的第一行（如 GET index.jsp HTTP/1.1），http.response 表示响应头中的第一行（如 HTTP/1.1 200 OK），其他头部都用 http.header_name 形式。

筛选 url 中包含.php 的 http 数据包----http.request.uri contains ".php"

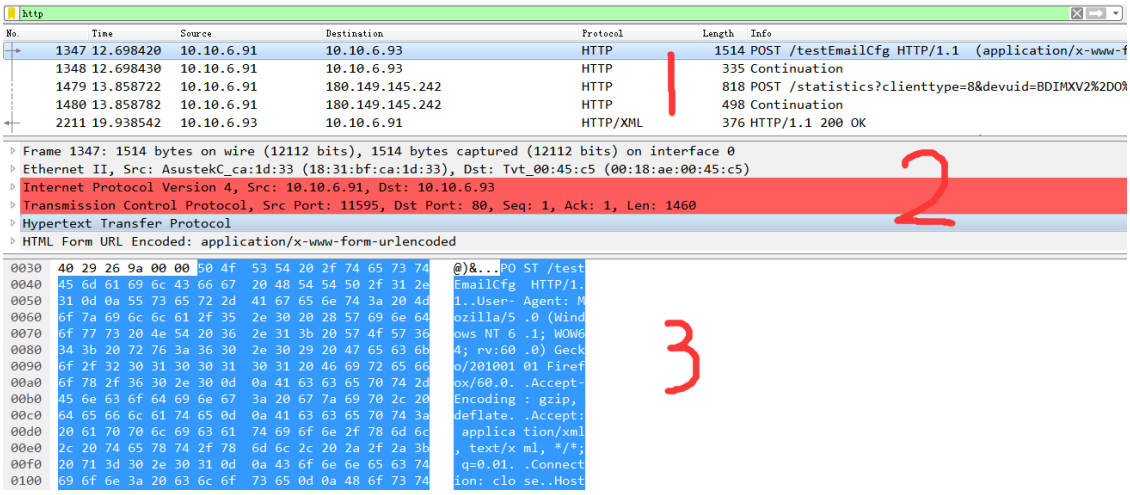
筛选内容包含 username 的 http 数据包----http contains "username"

显示 post 请求方式的 http 封包---http.request.method== "POST"

显示请求的域名为 tracker.1ting.com 的 http 封包---http.host == "tracker.1ting.com"

2.6 由 Wireshark 协议窗口分析协议的格式

Wireshark 抓包后的界面有三个部分，如下图：



上部为封包列表的面板中显示，编号，时间戳，源地址，目标地址，协议，长度，以及封包信息。具体为：

1. No:代表数据包标号。
2. Time：在软件启动的多长时间内抓到。
3. Source：来源 ip。
4. Destination: 目的 ip。
5. Protocol：协议。
6. Length:数据包长度。
7. info：数据包信息。

你可以看到不同的协议用了不同的颜色显示。你也可以修改这些显示颜色的规则， View ->Coloring Rules

中部为协议树窗口，显示的是选定的数据包的分协议层展示。在报文列表窗口选择不同条目则协议树窗口的 内容随之改变为相应的协议信息。这个面板是我们最重要的，用来查看协议中的每一个字段。

各行信息分别为：

Frame: 物理层的数据帧概况

Ethernet II: 数据链路层以太网帧头部信息

Internet Protocol Version 4: 互联网层 IP 包头部信息

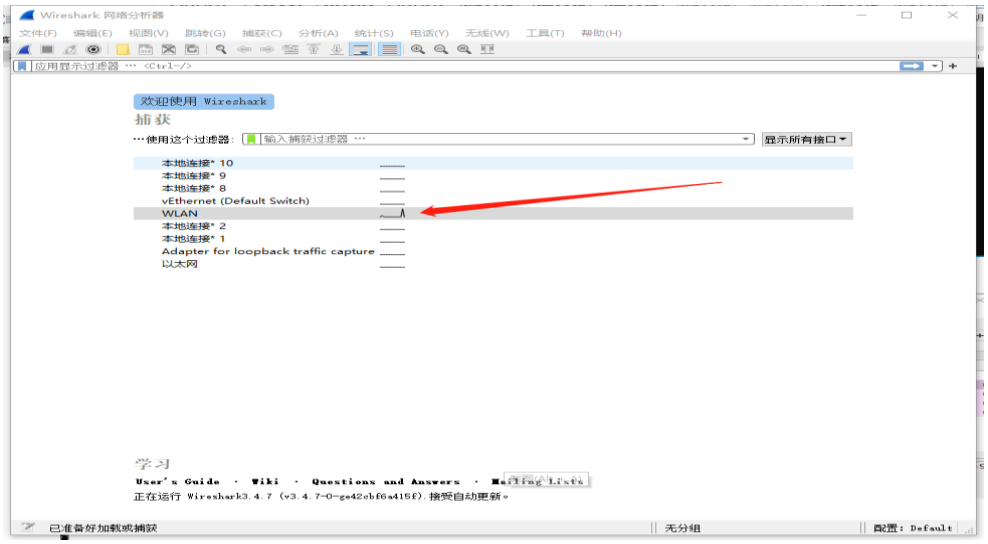
Transmission Control Protocol: 传输层 T 的数据段头部信息，此处是 TCP

Hypertext Transfer Protocol: 应用层的信息，此处是 HTTP 协议

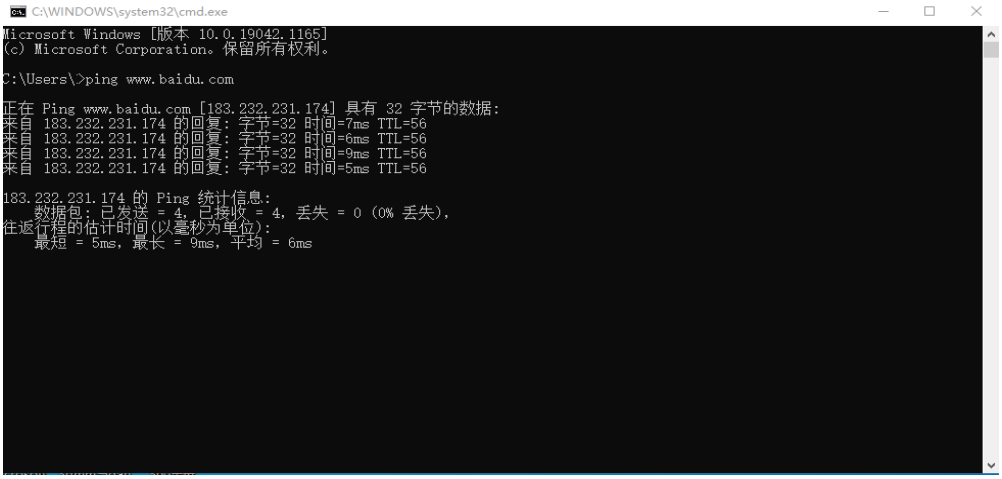
下部为 16 进制报文窗口，可以显示报文在物理层的数据形式。其中左侧是十六进制表示，右侧是 ASCII 码表示。

实例：分析 ping www.biadu.com 命令的数据包

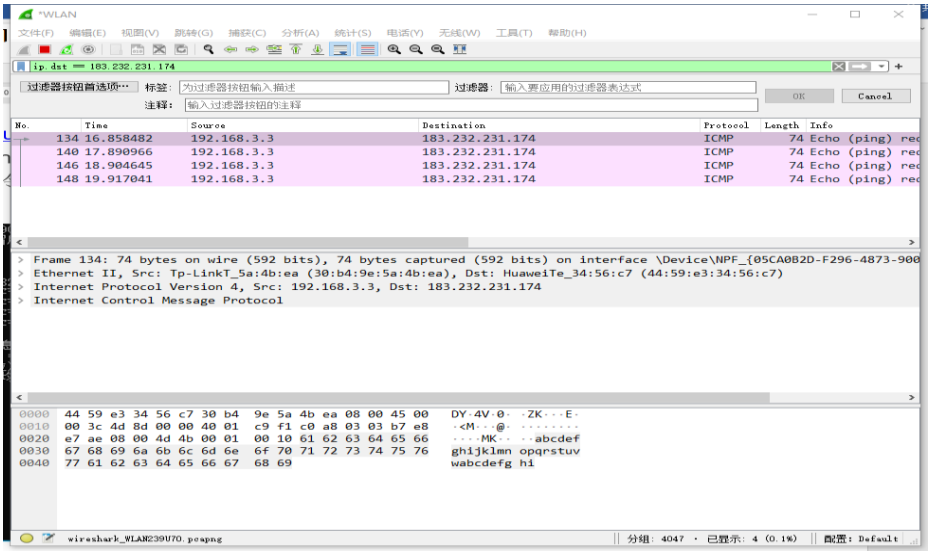
第一步骤：打开 wireshark 软件，选择对应的网卡进行捕获数据。



第二步骤：在 CMD 命令窗口输入 ping www.biadu.com



第三步骤：在过滤器输入过滤条件：ip.dst == 183.232.231.174



3. 数据链路层协议分析

TCP/IP 协议栈分为四层，从下往上依次为网络接口层、网际层、传输层和应用层，而网络接口层没有专门的协议，而是使用连接在 Internet 网上的各通信子网本身所固有的协议。如以太网（Ethernet）的 802.3 协议、令牌环网（TokenRing）的 802.5 协议、分组交换网的 X.25 协议等。

目前 Ethernet 网得到了广泛的应用，它几乎成为局域网代名词。因此，这一部分将对以太网链路层的帧格式和 802.1Q 帧格式进行分析验证，使学生初步了解 TCP/IP 链路层的主要协议以及这些协议的主要用途和帧结构。

3.1 以太网链路层帧格式分析实验

【实验目的】

1. 掌握以太网的报文格式
2. 掌握 MAC 地址的作用
3. 掌握 MAC 广播地址的作用
4. 掌握 LLC 帧报文格式
5. 掌握Wireshark的使用方法
6. 掌握协议栈发送和接收以太网数据帧的过程

【实验原理】

1．以太网简介

IEEE 802 参考模型把数据链路层分为逻辑链路控制子层 （LLC，Logical Link Control）和介质访问控制子层 （MAC，Media Access Control）。与各种传输介质有关的控制问题都放在 MAC 层中，而与传输介质无关的问题都放在 LLC 层。因此，局域网对 LLC 子层是透明的，只有具体到 MAC 子层才能发现所连接的是什么标准的局域网。

IEEE 802.3 是一种基带总线局域网，最初是由美国施乐 （Xerox ）于 1975 年研制成功的，并以曾经在历史上表示传播电磁波的以太 （Ether）来命名。1981 年，施乐公司、数字设备公司（Digital）和英特尔（Intel）联合提出了以太网的规约。1982 年修改为第二版，即 DIX Ethernet V2，成为世界上第一个局域网产品的规范。这个标准后来成为 IEEE 802.3 标准的基础。

在 802.3 中使用 CSMA/CD（Carrier Sense Multiple Access with Collision Detection ）协议。现在流行的以太网的 MAC 子层的帧结构有两种标准，一种是 802.3 标准，另一种是 DIX Ethernet V2 标准。

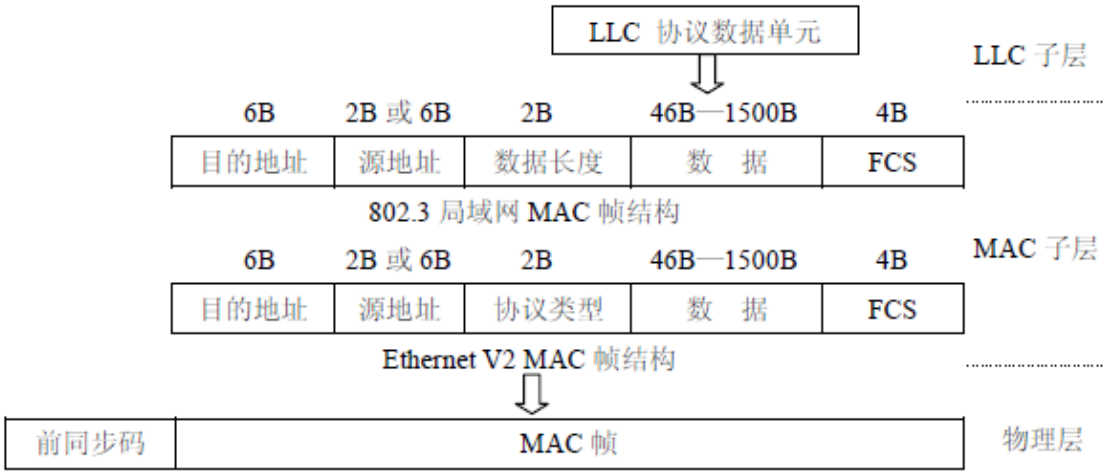


图 14　802.3 和 Ethernet V2 MAC 帧结构

图 14 画出了两种标准的 MAC 帧结构。它们都是由五个字段组成。MAC 帧的前两个字段分别是目的地址字段和源地址字段，长度是 2 或 6 字节。但在 IEEE 802.3 标准规定对 10Mb/s 的基带以太网则使用 6 字节的地址字段。

两种标准的主要区别在于第三个字段 （2 字节）。在 802.3 标准中，这个字段是长度字段，它指后面的数据字段的字节数，数据字段就是 LLC 子层交下来的 LLC 帧，其最小长度 46 字节，最大长度 1500 字节。在 Ethernet V2 标准中，这个字段是类型字段，它指出 LLC 层使用的协议类型。由于数据字段的最大长度为 1500 字节，因此，以太网 V2 标准中将各种协议的代码规定为大于 1500 的数值，这样就不至于发生误解，并借此实现兼容。最后一个字段是一个长度为 4 字节的帧校验序列 FCS，它对前四个字段进行循环冗余（CRC）校验。

为了使发送方和接收方同步，MAC 帧在总线上传输时还需要增加 7 个字节的前同步码字段和 1 字节的起始定界符 （它们是由硬件生成的），其中前同步码是 1 和 0 的交替序列， 供接收方进行比特同步之用；紧跟在前同步码之后的起始定界符为 10101011，接收方一旦接 收到两个连续的 1 后，就知道后面的信息就是 MAC 帧了。需要注意的是前同步码、起始定 界符和 MAC 帧中的 FCS 字段在网卡接收 MAC 帧时已经被取消，因此，在截获的数据报中 看不到这些字段。

注意：由于 802.3 标准在 MAC 帧中封装 802.2 帧，相比 Ethernet V2 增加了 8 个字节的开销，而且实践表明，这样做过于繁琐，使得其在实际中很少得到使用。因此，本节实验中重点分析 Ethernet V2 MAC 帧格式，802.3MAC 帧不作具体讨论。

2．实验环境与说明

（1）实验目的

了解 EthernetV2 标准规定的 MAC 帧结构，初步了解 TCP/IP 的主要协议和协议的层次结构。

（2）实验设备和连接

实验设备和连接图如图 15 所示，一台交换机连接了 2 台 PC 机，分别命名为主机 A、主机 B。

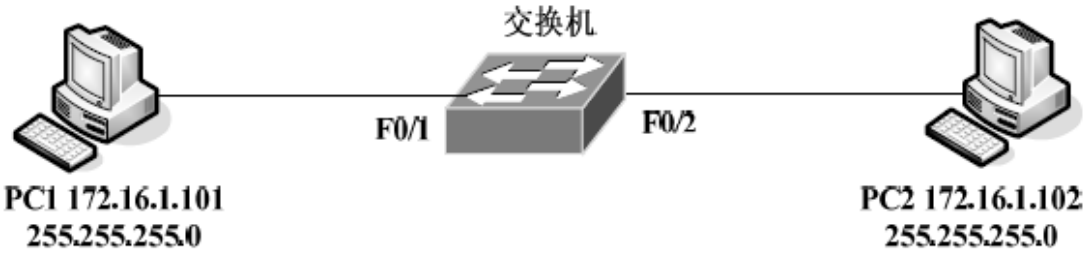


图 15 Ethernet 链路层帧结构实验连接图

（3）实验分组

每六名同学为一组，其中每两人一小组，每小组各自独立完成实验。将主机 A 和 B 作为一组，主机 C 和 D 作为一组，主机 E 和 F 作为一组。现仅以主机 A、B 所在组为例，其它组的操作参考主机 A、B 所在组的操作。将主机 A 和 B 作为一组，主机 C 和 D 作为一组，主机 E 和 F 作为一组。现仅以主机 A、B 所在组为例，其它组的操作参考主机 A、B 所在组的操作。

【实验步骤】

练习一、领略真实的 MAC 帧

步骤 1：使用 ipconfig/all 命令查看主机 A 和主机 B 的 IP 地址；（编者注：实验室中任何一台 PC 都可以作为模型中的主机 A 或主机 B）

步骤 2：在：主机 A 和主机 B 上运行 Wireshark 截获报文，为了只截获和实验内容有关的报文，将 Wireshark 的 Captrue Filter 设置为 “icmp”；

步骤 3：主机 A ping 主机 B，在： 主机 A 的“运行”对话框中输入命令 “Ping 主机 B IP 地址”，单击 “确定”按钮；

步骤 4：停止截获报文：将结果保存为 MAC-学号，并对截获的报文进行分析：

1）列出截获的报文中的协议类型，观察这些报文之间的关系。

_____

_____

_____

_____

2）在理论课程原理学习中我们知道，EthernetV2 规定以太网的 MAC 层的报文格式分为 7 字节的前导符、1 字节的帧首定界、6 字节的目的 MAC 地址、6 字节的源 MAC 地址、2 字节的类型、46～1500 字节的数据字段和 4 字节的帧尾校验字段。分析一个 Ethernet V2 帧，查看这个帧由几部分组成，缺少了哪几部分？为什么？

_____

_____

对捕获的报文进行分析，查看主窗口中数据报文列表窗口和协议树窗口信息，填写下表：

表 1　报文分析

此报文类型		
此报文的基本信息（数据报文列表窗口中的 Information 项的内容）		
Ethernet II 协议树中	Source 字段值	
	Destination 字段值	
Internet Protocol 协议树中	Source 字段值	
	Destination 字段值	

记录实验结果

	本机 MAC 地址	源 MAC 地址	目的 MAC 地址
主机 A			
主机 B			

思考问题：

1、 MAC 地址应用于 TCP/IP 协议模型的哪一层？

2、 如何区分以太网的两种标准帧格式？

练习二、编辑并发送 MAC 广播帧

本练习将主机 A、B、C、D、E、F 作为一组进行实验。

步骤1：主机 E 启动协议编辑器。

步骤2：主机 E 编辑一个 MAC 帧：

目的 MAC 地址：FFFFFF-FFFFFF

源 MAC 地址：主机 E 的 MAC 地址

协议类型或数据长度：大于 0x0600

数据字段：编辑长度在 46—1500 字节之间的数据

（注查看 MAC 地址的命令是 ipconfig/all）

步骤3：主机 A、B、C、D、F 启动Wireshark，打开捕获窗口进行数据捕获并设置过滤条件（源AC 地址为主机 E 的 MAC 地址）。

步骤4：主机 E 发送已编辑好的数据帧。

步骤5：主机 A、B、C、D、F 停止捕获数据，察看捕获到的数据中是否含有主机 E 所发送的数据帧。

- 结合练习三的实验结果，简述 FFFFFF-FFFFFF 作为目的 MAC 地址的作用。

思考问题：

1、 主机 A、B、C、D、F 是否可以收到主机 E 的广播帧？

2、 说明 MAC 广播帧的范围？