《TCP\IP 网络编程》实验指导书

湘潭大学信息工程学院

网络工程专业

前言

《TCP\IP 网络编程》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《TCP\IP 网络编程》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 4 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。

8 学时的实验时间分配如下：以太网链路层帧格式分析实验 2 学时、IP 协议分析实验 2 学时、TCP 协议分析实验 2 学时、FTP 协议分析实验 2 学时，总共 4 个实验。

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、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。

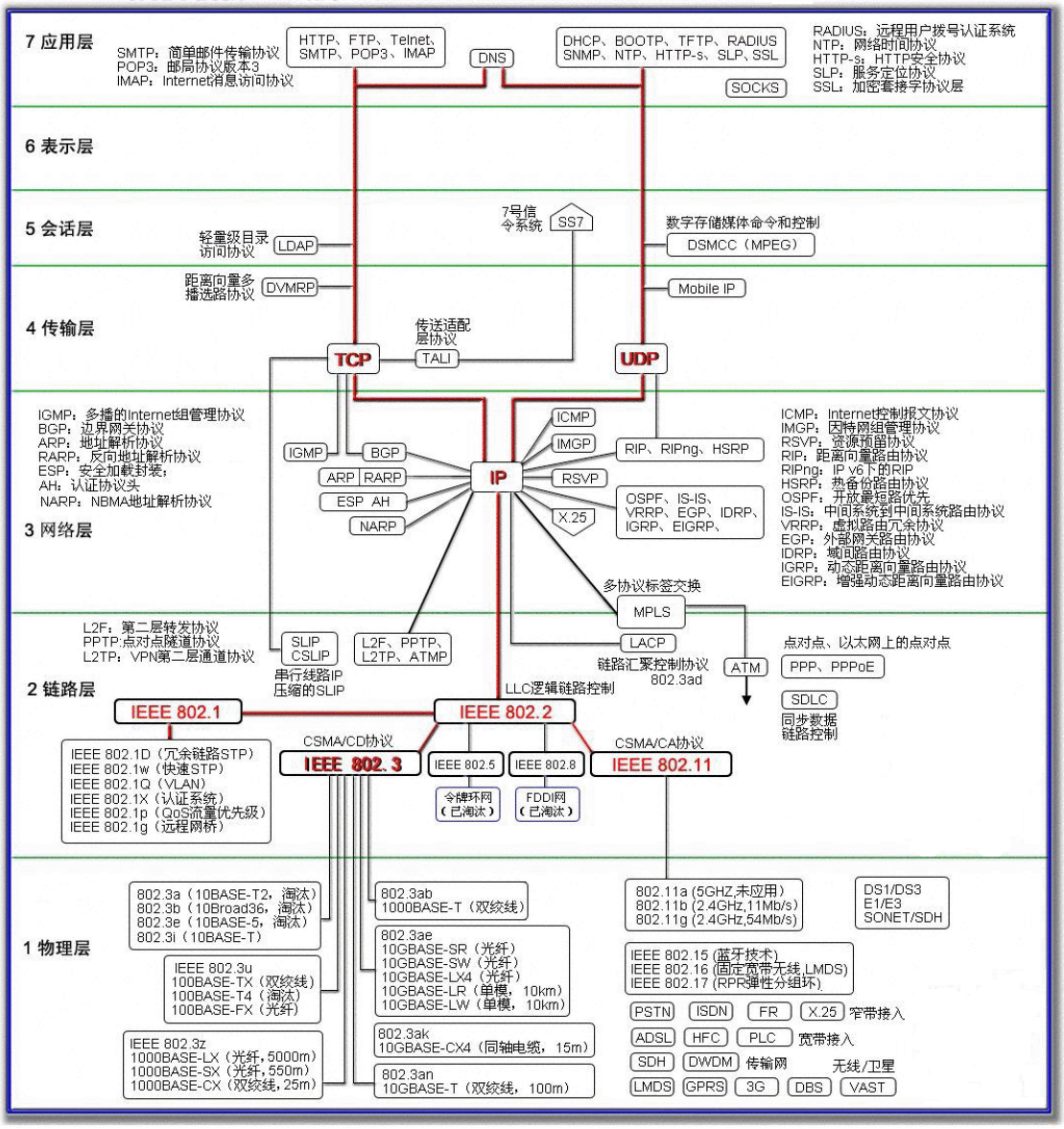
目 录

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、Ethereal 以及 Windows 2000 自带的网络监视器。本书选用 **Ethereal** 作为协议分析工具。

（2）网络协议图



2.网络协议分析器 Ethereal

网络协议分析器网络协议分析器 Ethereal 是目前最好的、开放源码的、获得广泛应用的网络协议分析器,支持 Linux 和 windows 平台。在该系统中加入新的协议解析器十分简单,自从 1998 年发布最早的 Ethereal 0.2 版本发布以来,志愿者为 Ethereal 添加了大量新的协议解析器,如今 Ethereal 已经支持五百多种协议解析。其原因是 Ehereal 具有一个良好的可扩展性的设计结构,这样才能适应网络发展的需要不断加入新的协议解析器。本节以 Ethereal 0.10.14 版本为依据。

Ethereal 的安装比较简单,从网络上下载下载完 Ethereal 安装即可。新版本 Ethereal 已经整合了 winpcap,应用比较方便。

2.1 Ethereal 主窗口简介

图 1 是抓包完成后的 Ethereal 的主窗口。过滤栏以上是 Ethereal 本身的菜单,过滤栏以下是抓获的包经过分析后的显示信息。

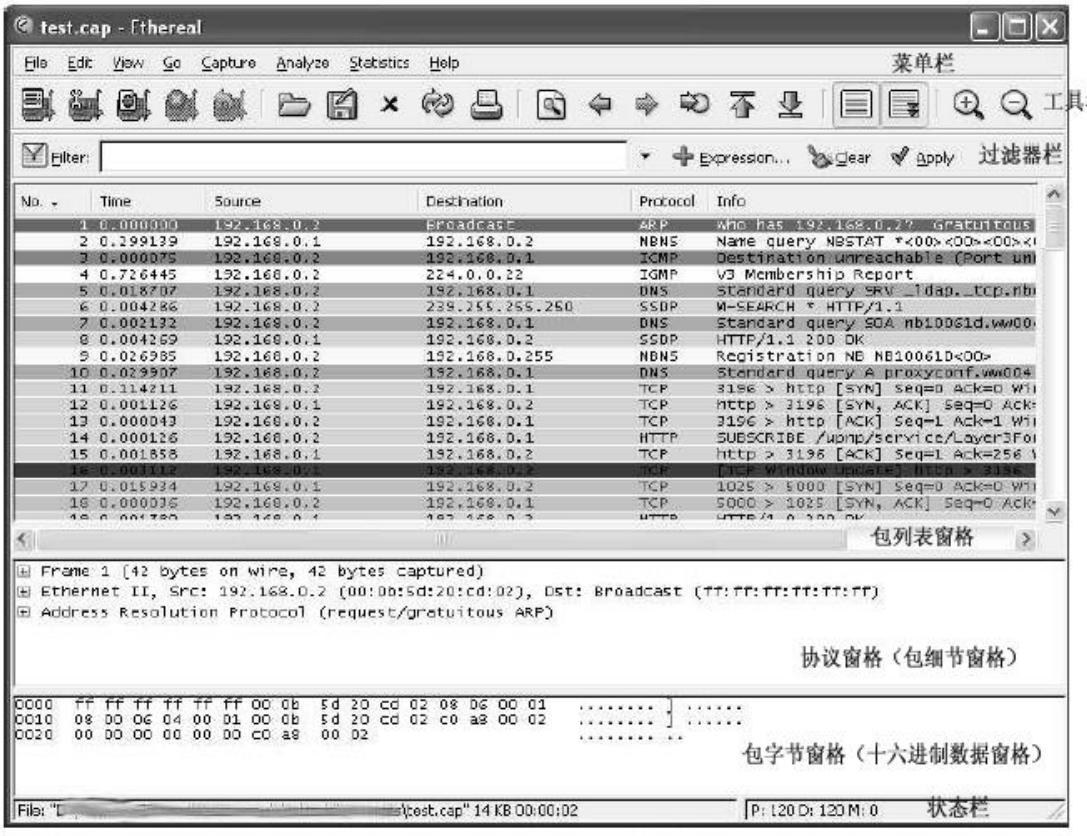


图 1　抓包完成后的 Ethereal 主窗口

其中：

1. 菜单栏通常用来启动 Ethereal 有关操作；
2. 工具栏提供菜单中常用项目的快速访问；
3. 过滤器栏提供一个路径，来直接控制当前所用的显示过滤器；
4. 包列表窗格显示当前抓包文件的全部包的摘要。

包列表的每一行对应抓包文件中的一个包，不同报文有不同的颜色，但是没有明显的规

律。如果你选择了一行，则更详细的信息显示在协议窗格和包字节数据窗格中。

注意：在此窗格里单击某个包，就会在另外的第二个窗口里显示这个包的信息。

当 Ethereal 解析一个包时， 由协议解析器将信息放置到行列中去，比较高级协议会改写较低级协议的信息，你只能看到最高级协议的信息。例如，IP 内部包含有 TCP 的 Ethernet 包，Ethernet 解析器将写出它的数据 （如 Ethernet 地址），而 IP 解析器将用自己的数据改写它 （如 IP 地址），等等。

在包列表窗格中的每一列代表抓获的一个包，每个包的摘要信息包括：

* No ：抓包文件中包的编号。，即使已经用了一个显示过滤器也不会改变。
* Time：包的时间戳，即抓获该包的时间，该时间戳的实际格式可以改变。
* Source：包的源地址。
* Destination：包的目标地址。
* Protocol：包协议的缩写。
* Info：包内容的附加信息，这是一种可用的上下文菜单 （鼠标右键）。

5．包协议窗格 （包细节窗格）

包协议窗格以更详细的格式显示从包列表窗格选中的协议和协议字段。包的协议和字段用树型格式显示，可以扩展和收缩。这是一种可用的上下文菜单，单击每行前的 “＋”就可以展开为以 “－”开头的若干行，单击 “－”又可以收缩。

在每个协议行中，会显示一些指定的协议字段：

（1）生成的字段：Ethereal 自己会生成附加的协议字段 （括号括起来者）。这些字段的信息是从抓包文件中已知的与其它字段的上下文推导出来的。例如，Ethereal 分析每个 TCP 流的顺序号/确认号时，就会在 TCP 协议的[SEQ/ACK 分析]中显示出来。

（2）链接： 如果 Ethereal 检测到抓包文件中存在着与其它包的关系，就会产生一个到其它包的链接。链接用蓝色显示，双击它，Ethereal 就跳到相应的包。

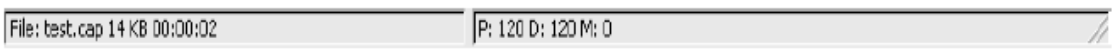
6．包字节窗格 （十六进制数据窗格）

包字节窗格以十六进制形式显示出从包列表窗格中选定的当前包的数据，并以高亮度显示在包协议窗格中选择的字段。在常用的十六进制区内，左边示出包数据的编号，中部为相应的十六进制示出包数据，右边为对应的 ASCII 字符。

7．状态栏

显示当前程序状态和抓获的数据的信息。通常左边显示相关信息的状态，右边显示包的当前数目。

(a)



(b)

图 2 状态栏示例示例

(a) 图示出没有装载抓包文件，即 Ethereal 开始时的情况。

(b) 图为已经装载抓包文件时的状态栏。左边显示关于抓包文件的名字、大小、开始抓包经过的时间等信息。右边显示抓包文件中包的当前数目。显示的数值如下：

* P: 抓获包的数目；
* D: 当前正显示的包的数目；
* M: 已经标记的数目。

2.2 Ethereal 菜单栏简介

1. File 文件菜单

文件菜单包括打开和合并抓包文件，全部或部分存储、打印、输出抓包文件，退出Ethereal。

2. Edit 编辑菜单

编辑菜单包括查询包，时间查询，标记或标识一个或多个包，设置你的选项 （剪切，拷贝，粘贴当前不能实现）

3. View 视图菜单

视图菜单控制抓抓获的包数据的显示，包括对抓获包的着色，字型的缩放，协议窗格中协议树的压缩和展开。

4. Go 指向菜单

以不同方式指向特定的包。

5. Capture 抓包菜单

开始和停止抓包过程以及编辑抓包过滤器。

6. Analyze 分析菜单

包括的选项由操作显示过滤器，允许和不允许对协议解析，配置用户指定的译码器和跟踪一个 TCP 流。

7. Statistics 统计菜单

显示各种统计窗口的菜单项，包括已经抓到的包的摘要，显示协议的分层统计等等。

8. Help 帮助菜单

包括帮助用户的选项，诸如一些基本帮助，所支持的协议列表，手工页面，在线访问一些 web 页面，以及常用的对话框。

2.3 Ethereal 的工具栏

Ethereal 工具栏提供主菜单中常用的选项的快速访问。工具栏不能由用户定制，但是如果屏幕空间需要显示更多的包数据，就可以用视图菜单将它隐蔽。

作为菜单，只有当前程序被选用时该选项才是可用的，其它选项变成灰色 （如果尚未装载数据就不能存入抓包文件）。图 3 为各种工具图标的名称。

图 3 各种工具图标的名称

* 接口：单击此图标，出现一个抓包选项表对话框；
* 选项：引出一个抓包选项对话框；
* 开始：根据选项在最近时间开始抓包；
* 停止：停止当前运行的抓包过程；
* 重开始：为了方便起见，停止当前运行的抓包过程，重新开始；
* 打开：出现打开文件对话框，让你打开一个抓包文件来观察；
* 存储为：让你将当前的抓包文件存储为你希望的文件。弹出“Save Capture File As”对话框；
* 关闭：关闭当前的抓包文件，如果没有存储该包被会询问是否存储；
* 重载：允许重装当前的抓包文件；
* 打印：引出打印对话框，允许全部或部分打印包文件中的包；
* 查询包：引出查询一个包的对话框；
* 向后：在包历史中向回跳；
* 向前：在包历史中向前跳；
* 指定包：引出对话框，跳到指定编号的包；
* 到首包： 跳到包文件中第一个包；
* 到末包：跳到包文件中最后一个包；
* 着色：对包列表中抓获的色，用不同颜色显示；
* 放大：放大打开的包数据 （增大字型）；
* 取消放大：取消包数据放大。

2.4 Ethereal 的网络数据抓包过程

Ethereal 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。

使用 Ethereal 进行网络协议分析时应当注意：必须有管理员权限才能开始抓包过程；必须选择正确的网络接口来抓获包数据；必须在网络的正确的位置抓包才能看到想看到的业务流量。

1. 通过抓包接口开始抓包. 通过抓包接口开始抓包

可以通过工具栏的接口选项，或者“Capture”菜单的“Interfaces”选项选择抓包菜单后，Etherea 弹出抓包接口对话框，如图 4 所示。但需注意，作为抓包接口对话框，只在数据抓包前显示，会消耗很多系统资源，要尽快关闭对话框以防止过多的系统装载。

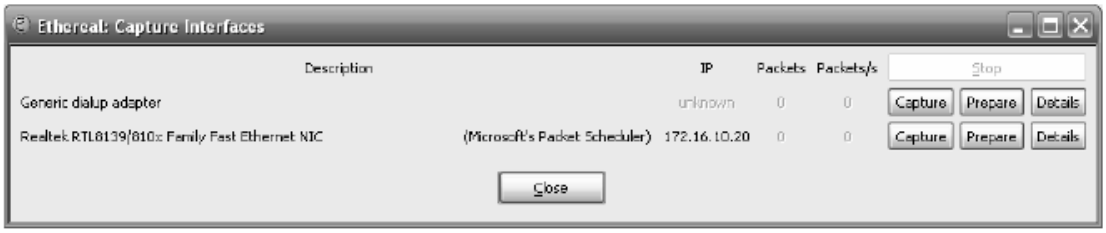


图 4 抓包接口对话框

图中 Gneric dialup adapter 为拨号适配器，第二行为快速以太网网卡。工具栏框中的

各个选项叙述于下：

* IP：Ethereal 可能从这个接口分辨第一个 IP 地址，如果分辨不出地址，就会显示“unknown ”，如果解析出不止一个 IP 地址，则只显示第一个；
* Packets：从对话框打开后从该接口侦测到的包数。如果最近一秒没有侦测到包，则 Packets 变为灰色；
*Packets/s：在最近一秒侦测到的包数，如果没有侦测到包，则在最近一秒变为灰色；
* Stop：停止当前抓包运行；
* Capture：利用最后抓包设置立即在该接口开始抓包；
* Prepare：打开该接口的抓包选项对话框；
* Close：关闭对话框。

如果选择 Capture，则立即开始抓包，并显示图 5 的抓包过程数据报文统计：

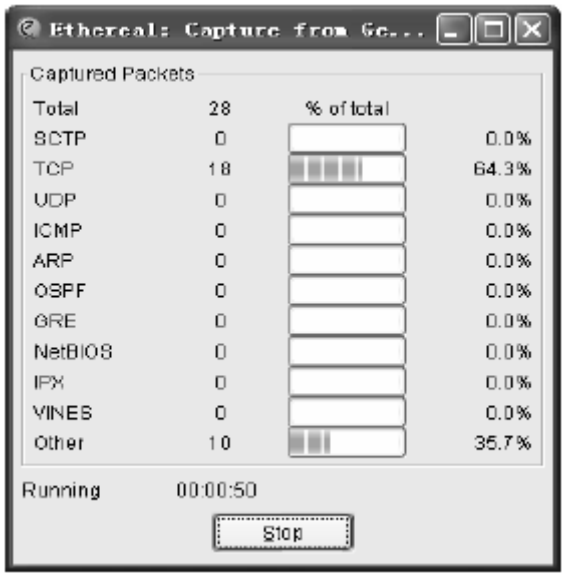


图 5 抓包过程数据报文统计

抓到足够的包后，单击 Stop 停止抓包。即可显示如图 1 的抓包完成后的 Ethereal 主窗口。

2．通过．通过 capture 菜单选项抓包

Ethereal 的抓包 （capture）选项，如图 6 所示。

图 6 Capture 选项

（1）单击 Capture 选抓包过滤器 Capture Filters... ，弹出过滤器窗口，如图 7 所示。

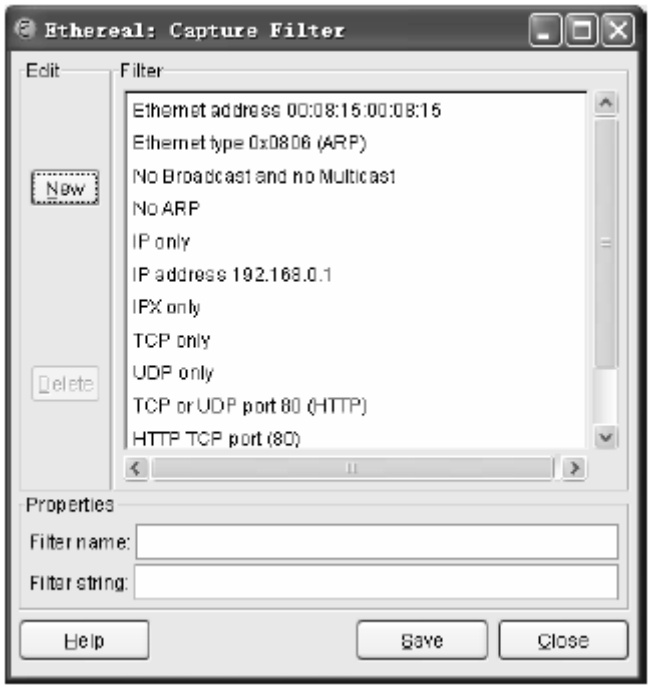


图 7　Capture 过滤器选项

（2）在 Filter 栏中选择某项过滤器名称，如“No Broadcast and no Multicast ”或“TCP only”，则在 Filter name 和 Filter string 文本框中显示你的选项。

也可以在 Filter name 框中键入过滤器名字,在 Filter string 框中键入过滤器字符串，单击 New，一个过滤器就建立好了。

单击 Capture 选 Options，弹出图 8 所示过滤器选项窗口，指明网络适配器，抓包模式，包字节限制，过滤条件等有关抓包的系统配置的启用和设置。

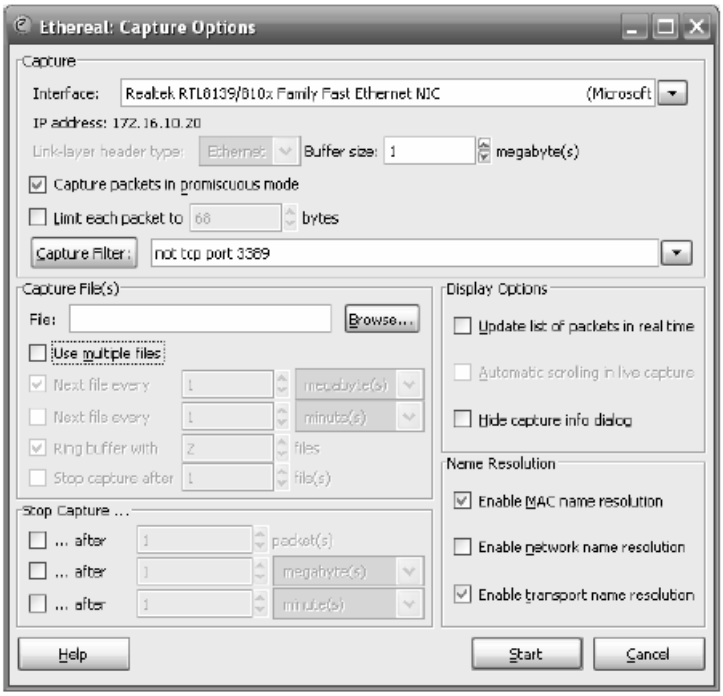


图 8　过滤器选项窗口

（3）Ehereal 的抓包过滤器

抓包过滤器用来只抓取你感兴趣的包。如果你想抓取某些特定的数据包时，有两种方法可供选择。

第一种方式是先定义好抓包过滤器，结果是只抓到你设定好的那些类型的数据包；

第二种方式是，先把本机收到或者发出的包全部抓下来，再使用的显示过滤器，只显示你想要的那些类型的数据包，这种方式比较常用，建议实验时大家采用。

（4 ）最后单击 Start，即可开始抓包，并弹出本机收到的数据报文统计信息。

此后的操作与通过接口抓包相同，单击 Stop 即可停止抓包，并显示对截获到的报文进行分析后的界面。

2.5 由 Ethereal 协议窗口分析协议的格式

Ethereal 抓包后的界面有三个部分，上部为报文列表窗口，显示的是对抓到的每个数据报文进行分析后的总结型信息，包括编号、时间、源地址、目标地址、协议、信息。中部为协议树窗口，显示的是数据报文的协议信息。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。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。

在抓包完成后，显示过滤器可以用来找到你感兴趣的包，也可根据协议、是否存在某个域、域值、域值之间的关系来查找你感兴趣的包。

1.. Etheral 的显示过滤器

可以使用下面的操作符来构造显示过滤器：

eq == 等于：如 ip.addr==10.1.10.20

ne != 不等于：如 ip.addr!=10.1.10.20

gt > 大于：如 frame.pkt_len>10

lt < 小于：如 lt < frame.pkt_len<10

ge >= 大等于：如 frame.pkt_len>=10

le <= 小等于：如 frame.pkt_len<=10

也可以使用下面的逻辑操作符将表达式组合起来：

and &&逻辑与：如 ip.addr=10.1.10.20&&tcp.flag.fin

or || 逻辑或：如 ip.addr=10.1.10.20||ip.addr=10.1.10.21

xor ^^ 异或：如 tr.dst[0:3] == 0.6.29 xor tr.src[0:3] == not

! 逻辑非：如 !llc

例如：你想抓取 IP 地址是 192.168.2.10 的主机所收或发的所有的 HTTP 报文，则显示过滤器 （Filter ）为：ip.addr=192.168.2.10 and http

图 9 组合过滤器设置

注意：当在 Filter 的输入，显示绿色背景时 （图 9 上图）说明表达式是正确的，显示红色背景时 （图 9 下图）说明表达式是错误的。

又例如，你只想查看使用 tcp 协议的包，在 Ethereal 窗口 Filter 栏中输入 tcp，然后回车，Ethereal 就会只显示 tcp 协议的包。

2．实例分析

下面的分析示例是通过上网查询 “TCP/IP”，然后运行 ethereal 抓包。

抓包过程为：单击 Capture－按默认过滤器－Start－抓包 2 分钟－Stop，获得图 10 的结果。

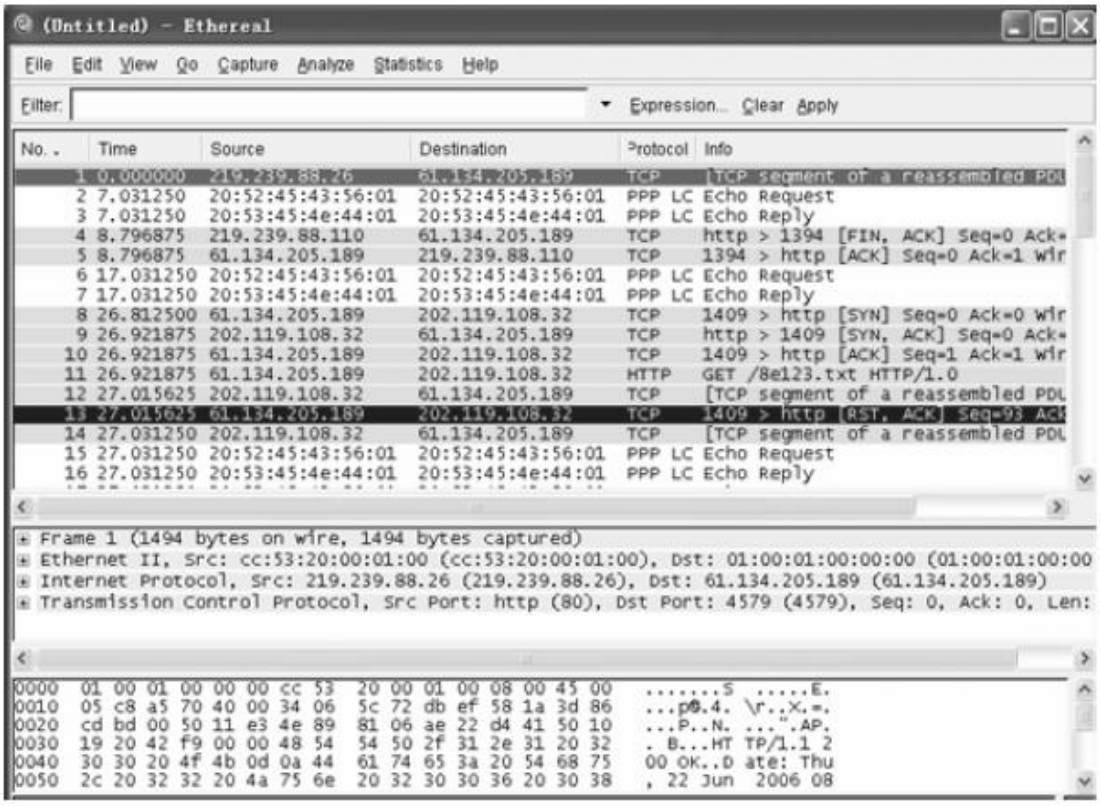


图 10 上网查询抓包结果

由于 Ethereal 已经对抓包结果做了分析，所以，通过协议窗口可以获得 IP 协议数据报格式和 TCP 协议报文格式的具体数据。在图 10 中，各个窗口都可以用拖拉方法拉大或缩小，即可与十六进制窗口相结合，清楚地看到各个字段的数据。其方法如下：

（1）最初协议窗口显示了协议信息，单击第一条信息，则十六进制窗口的中对应的信息变为黑底白字，如图 11 所示：

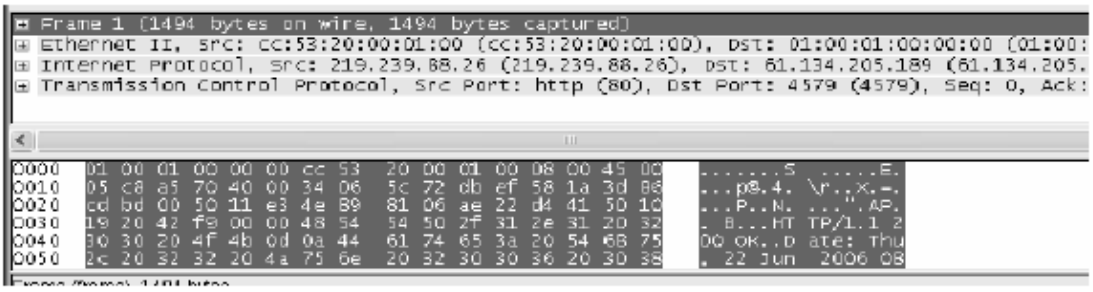


图 11 单击 frame 1 1494 字节改变颜色

（2）每条信息头部有一个 “＋”号，单击“＋”则变为“－”，具体的协议信息即展开并显示在协议窗口内，图 12 所示为 Internet protocol 协议展开的图示：

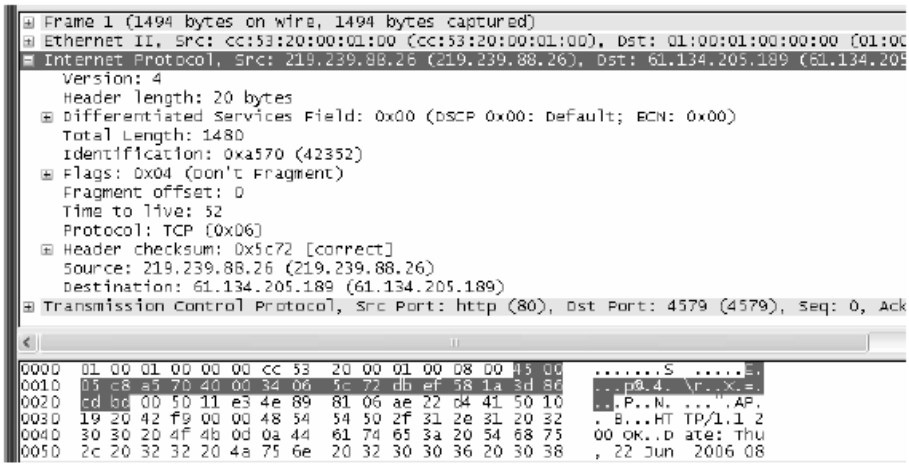


图 12 单击 IP 协议的展开图

由图 12 可见，IP 协议源地址为 219.239.88.26，目标地址为 61.134.205.189，版本为 IPV4，报头长度为 20 字节。对应的十六进制数据为 45 00 05 c8 a5 70 40 00 34 06 5c 72 db ef 58 1a 3d 86 cd b0。协议窗口中还有 3 个带 “＋”的信息行，将 Differentiated Service Field（不同的服务字段）、标志行 （Flags ）和报头校验和行展开，则可以看到具体字段的数据。

（3）TCP 协议的展开

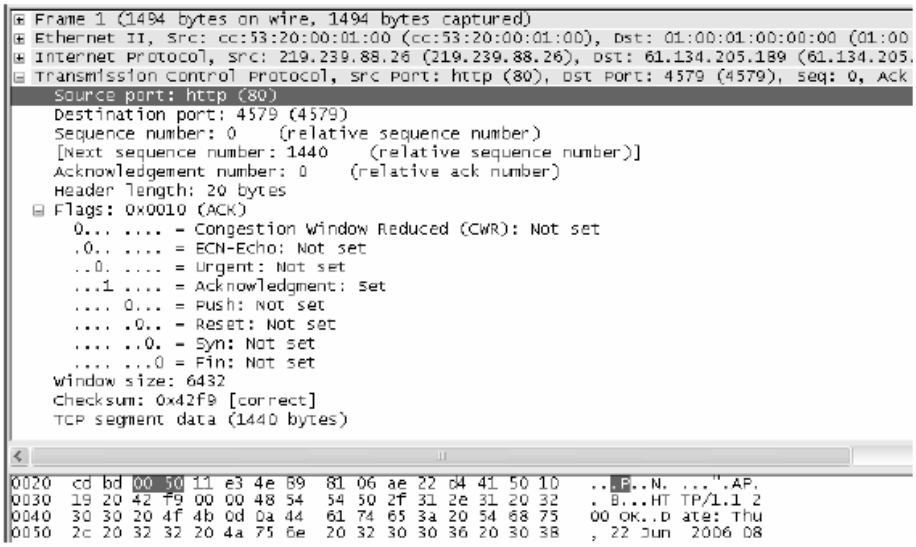


图 13 TCP 协议的展开图

图 13 为 TCP 协议的展开图，由图可见源端口号为 http（80），对应的十六进制为 00 50，目标端口号为 4579，顺序号为 0，下一顺序号为 1440，确认号为 0，报头长 20 字节，其后还可以看到保留位和 6 个控制位的设置情况等等。

TCP/IP 协议的报文格式此处没有列出，请读者自己对照，即可得知 Ethereal 已经对抓包结果做了准确的分析。

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。

以太网链路层帧格式分析实验

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 1 坚持的 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。

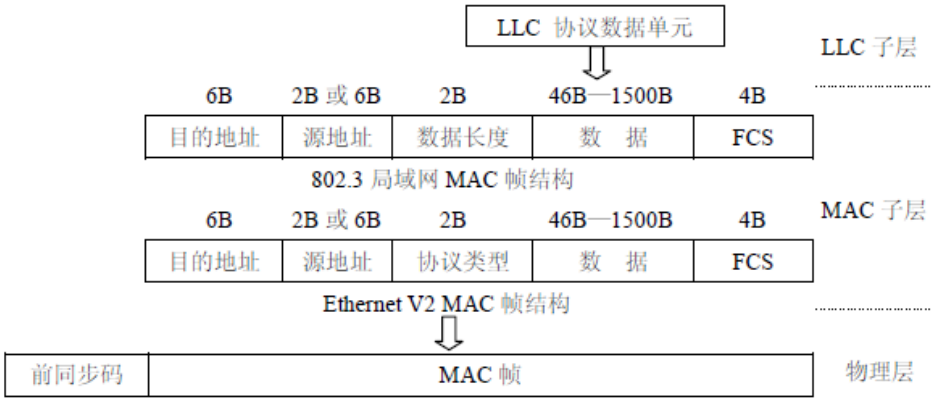


图 14 802.3 和 Ethernet V2 MAC 帧结构

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，一台锐捷 S2126G 交换机连接了 2 台 PC 机，分别命名为 PC1、PC2，交换机命名为 Switch。

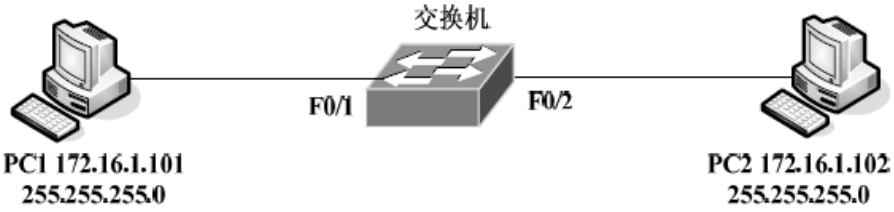


图 15 Ethernet 链路层帧结构实验连接图

（3）实验分组

每四名同学为一组，其中每两人一小组，每小组各自独立完成实验。

3．实验步骤

步骤 1：按照如图 15 所示连接好设备，配置 PC1 和 PC2 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 PC1 或 PC2。）

步骤 2：在：PC1 和 PC2 上运行 Ethereal 截获报文，为了只截获和实验内容有关的报文，将 Ethereal 的 Captrue Filter 设置为 “No Broadcast and no Multicast ”；

步骤 3：在： PC1 的“运行”对话框中输入命令 “Ping 172.16.1.102”，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，观察这些协议之间的关系。

_____

_____

2）在网络课程学习中，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？

_____

_____

_____

_____

步骤 5：在： PC1 和 PC2 上运行 Ethereal 截获报文，然后进入 PC1 的 Windows 命令行窗口，执行如下命令：

net send 172.16.1.102 Hello

这是 PC1 向 PC2 发送消息的命令，等到 PC2 显示器上显示收到消息后，终止截获报文。注意 PC1 和 PC2 的信使服务应启动。

找到发送消息的报文并进行分析，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	
User Datagram Protocol 协议树中	Source 字段值	
	Destination 字段值	
应用层协议树	协议名称	
	包含 Hello 的字段值	

4. 网络层协议分析

该层是网络互联层，负责相邻计算机之间的通信。该层上的主要协议是 IP 协议，此外，这一层还包括三个子协议：ICMP 协议、ARP 协议和 RARP 协议。

* 互联网控制信息协议 （ICMP，Internet Control Message Protocol）

ICMP 是 TCP/IP 协议簇的的一个子协议，它和 IP 协议属于同一层， 但 ICMP 数据报是被封装在 IP 数据报中发送的。ICMP 协议通常被用于在 IP 主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。该协议经常被用作调试和监视网络。

* 网际协议 （IP，Internet Protocol）

这个协议是 TCP/IP 协议中最主要的协议之一,他负责处理来之传输层的分组发送请求和输入的数据报文。该层以上各层的协议都要使用 IP 协议。

* 地址解析协议 （ARP ）和反地址解析协议 （RARP，Reverse Address Resolution Protocol）

它们分别负责实现从 IP 地址到物理地址 （如以太网网卡 MAC 地址）和从物理地址到 IP 地址的映射。

IP 协议分析实验

1. IP 协议介绍

（1）IP 地址的编址方法

IP 地址是为每个连接在互联网上的主机分配的唯一识别的 32 位标识符。IP 地址的编址方法共经历了三个阶段：

* 分类的 IP 地址

这是一种基于分类的两级 IP 地址编址的方法。

表 8 IP 地址的分类

IP 地址 类型	第一字节 十进制范围	二进制 固定最高位	二进制 网络位	二进制 主机位
A 类	1-126	0	8 位	24 位
B 类	128 －191	10	16 位	16 位
C 类	192 －223	110	24 位	8 位
D 类	224 －239	1110	组播地址	
E 类	240 －254	1111	保留试验使用	

如表 8 所示，IP 地址分为 A，B，C，D，E 五类，其中 A、B、C 类地址为可分配主机地址，而 D 类地址为组播地址，E 类地址保留以备将来的特殊使用。IP 地址采用点分十进制方式记录，每个地址表被视为 4 个以点分隔开的十进制整数，每个整数对应一个字节。

A、B、C 三类地址由两部分组成：网络地址和主机地址，这三类地址的网络地址部分的长度不一样。每个 A 类地址的网络中可以有 1600 万台主机；每个 B 类地址的网络中可以有 65534 台主机；每个 C 类地址的网络中可以有 254 台主机。

这样对于一个共有几十台计算机的局域网来说即使分配一个 C 类地址也是一种浪费。为此，提出了子网和子网掩码的概念。

* 划分子网的 IP 地址

子网就是将一个 A 类、B 类或 C 类网络分割成许多小的网络，每一个小的网络就称为子网。划分子网采用 “网络号”＋“子网号”＋“主机号”三级编址的方法。在划分了子网的网络地址中，子网掩码用于确定网络地址。

子网掩码是一个和 IP 地址对应的 32 位二进制数。子网掩码中与 IP 地址的网络地址对应的部分为 1，与主机地址对应的部分为 0。这样把网络接口的 IP 地址与该接口上的掩码相与就得到该接口所在网络的网络地址，而把该 IP 地址与掩码的反码相与则可得到主机地址。

* 无分类域间路由选择 CIDR

无分类域间路由选择 CIDR 是根据划分子网阶段的问题提出的编址方法。IP 地址采用“网络前缀”＋“主机号”的编址方式。目前 CIDR 是应用最广泛的编址方法，它消除了传统的 A、B、C 类地址和划分子网的概念，提高了 IP 地址资源的利用率，并使得路由聚合的实现成为可能。

（2）IP 报文格式

IP 报文由报头和数据两部分组成，如图 23 所示：

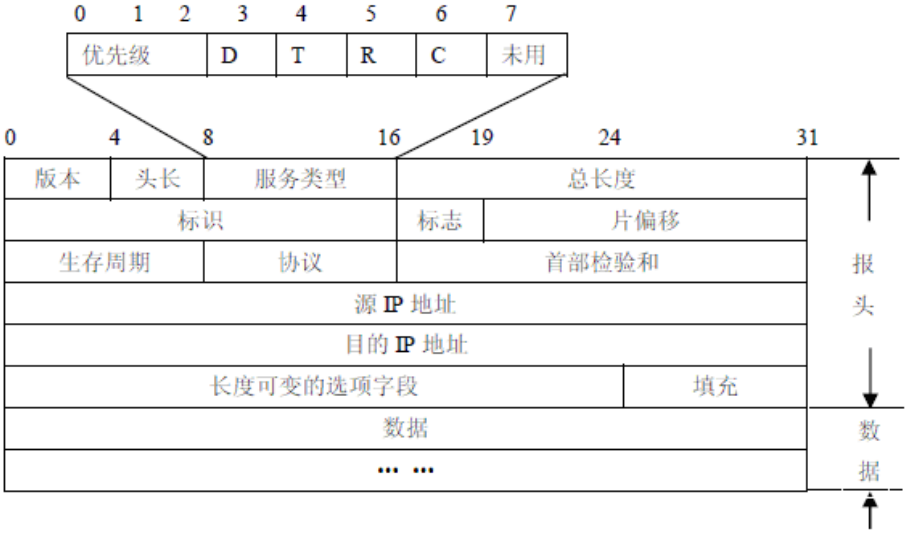


图 23　IP 报文格式

其中主要字段的意义和功能如下：

* 版本：指 IP 协议的版本；
* 头长：是指 IP 数据报的报头长度，它以 4 字节为单位。IP 报头长度至少为 20 字节，如果选项部分不是 4 字节的整数倍时，由填充补齐；
* 总长度：为整个 IP 数据报的长度；
* 服务类型：规定对数据报的处理方式；
* 标识：是 IP 协议赋予数据报的标志，用于目的主机确定数据分片属于哪个报文；
* 标志：为三个比特，其中只有低两位有效，这两位分别表示该数据报文能否分段和是否该分段是否为源报文的最后一个分段；
* 生存周期：为数据报在网络中的生存时间，报文每经过一个路由器时，其值减 1，当

生存周期变为 0 时，丢弃该报文；从而防止网络中出现循环路由；

* 协议：指 IP 数据部分是由哪一种协议发送的；

* 校验和：只对 IP 报头的头部进行校验，保证头部的完整性；

* 源 IP 地址和目的 IP 地址：分别指发送和接收数据报的主机的 IP 地址。

（3）IP 数据报的传输过程

在互联网中，IP 数据报根据其目的地址不同，经过的路径和投递次数也不同。当一台主机要发送 IP 数据报时，主机将待发送数据报的目的地址和自己的子网掩码按位 “与”，判断其结果是否与其所在网络的网络地址相同，若相同，则将数据报直接投递给目的主机，否则，将其投递给下一跳路由器。

路由器转发数据报的过程如下：

① 当路由器收到一个数据报文时，对和该路由器直接相连的网络逐个进行检查，即用目的地址和每个网络的子网掩码按位 “与”，若与某网络的网地址相匹配，则直接投递；否则，执行 2。

② 对路由表的每一行，将其中的子网屏蔽码与数据报的目的地址按位 “与”，若与该行的目的网络地址相等，则将该数据报发往该行的下一跳路由器；否则，执行 3。

③ 若路由表中有一个默认路由，则将数据报发送给路由表所指定的默认路由器。否则，报告转发出错。

2．实验环境与说明

（1）实验目的

使用 Ping 命令在两台计算机之间发送数据报，用 Ethereal 截获数据报，分析 IP 数据报的格式，理解 IP V4 地址的编址方法，加深对 IP 协议的理解。

（2）实验设备和连接

实验设备和连接图如图 24 所示，一台锐捷 R1760 路由器连接 2 台 PC 机，分别命名为 PC1、PC2。

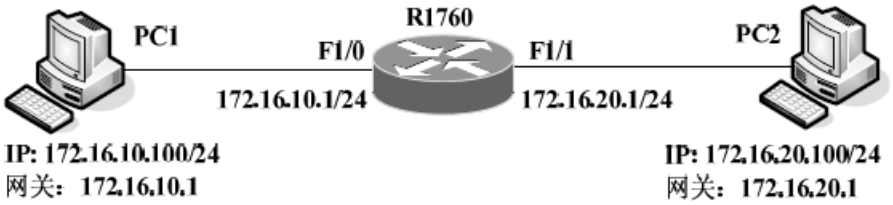


图 24 IP 协议分析实验连接图

（3）实验分组

每四名同学为一组，其中每两人一小组，每小组各自独立完成实验。

3．实验步骤

步骤 1：按照如图 24 所示连接好设备；

步骤 2：完成路由器和 PC1、PC2 的相关配置，与 4.1 实验步骤 2 相同；（编者注：实验室中任何一台 PC 都可以作为模型中的 PC1。而 PC2 用 202.202.43.125 等另一网段机器代理即可。）

步骤 3：按照 4.1 实验方法，截获 PC1 上 ping PC2 的报文，结果保存为 IP-学号；

步骤 4：任取一个数据报，分析 IP 协议的报文格式，完成下列各题：

1） 分析 IP 数据报头的格式，完成表 9；

表 9 IP 协议报文分析

字段	报文信息	说明
版本		
头长		
服务类型		
总长度		
标识		
标志		
片偏移		
生存周期		
协议		
校验和		
源地址		
目的地址		

2）查看该数据报的源 IP 地址和目的 IP 地址，他们分别是哪类地址？体会 IP 地址的编址方法。

_____

_____

IP 数据报分片实验

1. IP 数据报分片实验原理

我们已经从前边的实验中看到，IP 报文要交给数据链路层封装后才能发送。

理想情况下，每个 IP 报文正好能放在同一个物理帧中发送。但在实际应用中，每种网络技术所支持的最大帧长各不相同。例如：以太网的帧中最多可容纳 1500 字节的数据；FDDI 帧最多可容纳 4470 字节的数据。这个上限被称为物理网络的最大传输单元 （MTU，Maxium Transfer Unit）。

TCP/IP 协议在发送 IP 数据报文时，一般选择一个合适的初始长度。当这个报文要从一个 MTU 大的子网发送到一个 MTU 小的网络时，IP 协议就把这个报文的数据部分分割成能被目的子网所容纳的较小数据分片，组成较小的报文发送。每个较小的报文被称为一个分片 （Fragment）。每个分片都有一个 IP 报文头，分片后的数据报的 IP 报头和原始 IP 报头除分片偏移、MF 标志位和校验字段不同外，其他都一样。图 25 显示了 Ethereal 捕获的 IP 数据报分片的分析情况，可参考。

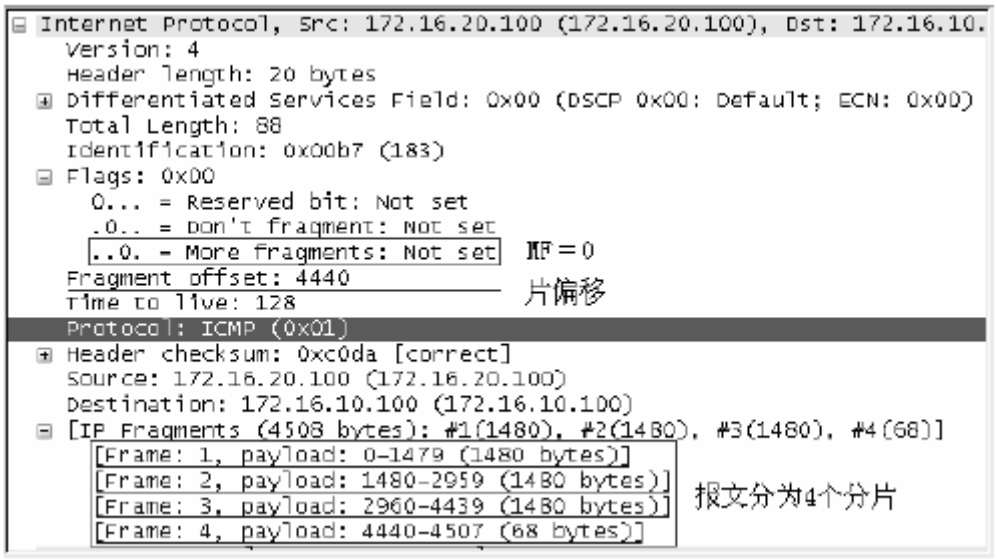


图 25 IP 数据报分片示例

重组是分片的逆过程，分片只有到达目的主机时才进行重组。当目的主机收到 IP 报文时，根据其片偏移和标志 MF 位判断其是否一个分片。若 MF 为 0，片偏移为 0，则表明它是一个完整的报文；否则，则表明它是一个分片。当一个报文的全部分片都到达目的主机时，IP 就根据报头中的标识符和片偏移将它们重新组成一个完整的报文交给上层协议处理。

2．实验环境与说明

（1）实验目的

使用 Ping 命令在两台计算机之间发送发送大于 MTU 的数据报，验证分片过程，加深对 IP 协议的理解。

（2）实验设备和连接

与 5.2.1 和 5.2.2 实验完全相同。

（3）实验分组

每四名同学为一组，其中每两人一小组，每小组各自独立完成实验。

3．实验步骤

步骤 1：按照 4.1 和 4.2 实验连接好设备，完成路由器和 PC1、PC2 的相关配置；（编者注：实验室中任何一台 PC 都可以作为模型中的 PC1。而 PC2 用 202.202.43.125 等另一网段机器代理即可。）

步骤 2：在 PC1、PC2 两台计算机上运行 Ethereal，为了只截获和实验有关的数据报，设置 Ethereal 的截获条件为对方主机的 IP 地址，开始截获报文；

步骤 3：在 PC1 上执行如下 Ping 命令，向主机 PC2 发送 4500B 的数据报文：

Ping -l 4500 -n 2 172.16.20.100

步骤 4：停止截获报文，分析截获的报文，回答下列问题：

1）以太网的 MTU 是多少？

_____

2）对截获的报文分析，将属于同一 ICMP 请求报文的分片找出来，主机 PC1 向主机 PC2 发送的 ICMP 请求报文分成了几个分片？

_____

3）若要让主机 PC1 向主机 PC2 发送的数据分为 3 个分片，则 Ping 命令中的报文长度应为多大？为什么？

_____

_____

_____

4 ）将第二个 ICMP 请求报文的分片信息填入表 5.10：

表 10 ICMP 请求报文分片信息

分片序号	标识(Identification)	标志(Flag)	片偏移(Fragment Offset)	数据长度

5.传输层协议分析

TCP/IP 的传输层有两个协议，即：传输控制协议 TCP（Transmission Control Protocal）和用户数据报 （User Datagram Protocol ）。在 TCP 体系中，根据所使用的协议是 TCP 或 UDP，传输的数据单元分别称之为 TCP 报文段或 UDP 数据报。

TCP 提供面向连接的可靠的传输服务。在传输数据之前必须建立连接，数据传送结束后释放连接。因此，不可避免地增加了很多开销，如确认、流量控制、计时器以及连接管理等。这样不仅使协议数据单元的首部加长，还要占用许多处理器资源。

UDP 在传输数据前不需要建立连接，远程主机的传输层在收到 UDP 数据报后不需要提供任何确认信息。虽然 UDP 提供的是一种不可靠的传输服务，但在某些请况下，UDP 是一种有效率的工作方式。

在一台主机上，常常有多个应用程序运行，为了区分一台主机上的多个应用程序，TCP/IP 协议中引入了端口的概念。每个端口都有一个 16 位的标志符，这个标志符被称为端口号，TCP 和 UDP 都有自己的端口号。

TCP 协议分析实验

1. TCP 协议介绍

TCP 是传输控制协议 （Transmission Control Protocal）的缩写，提供面向连接的可靠的传输服务。在 TCP/IP 体系中，HTTP、FTP、SMTP 等协议都是使用 TCP 传输方式的。

（1）TCP 报文格式

图 28 TCP 报文段格式

TCP 报文分为首部和数据两个部分。如图 28 所示，TCP 报文段首部的前 20 字节是固定的，后面有 4 ×n 字节是可选项。其中：

* 源端口和目的端口：各 2 字节，用于区分源端和目的端的多个应用程序；
* 序号：4 字节，指本报文段所发送的数据的第一字节的序号；
* 确认序号：4 字节，是期望下次接收的数据的第一字节的编号，表示该编号以前的数据

已安全接收。

* 数据偏移：4 位，指数据开始部分距报文段开始的距离，即报文段首部的长度，以 32bit 为单位。
* 标志字段：共有六个标志位：
  ① 紧急位 URG=1 时，表明该报文要尽快传送，紧急指针启用；
  ② 确认位 ACK=1 时，表头的确认号才有效；ACK=0，是连接请求报文；
  ③ 急迫位 PSH=1 时，表示请求接收端的 TCP 将本报文段立即传送到其应用层，而不是等到整个缓存都填满后才向上传递；
  ④ 复位位 RST=1 时，表明出现了严重差错，必须释放连接，然后再重建连接；
  ⑤ 同步位 SYN=1 时，表明该报文段是一个连接请求或连接响应报文，
  ⑥ 终止位 FIN=1 时，表明要发送的字符串已经发送完毕，并要求释放连接。
* 窗口：2 字节，指该报文段发送者的接收窗口的大小，单位为字节；
* 校验和：2 字节，对报文的首部和数据部分进行校验；
* 紧急指针：2 字节，指明本报文段中紧急数据的最后一个字节的序号，和紧急位 URG 配合使用；
* 选项：长度可变，若该字段长度不够四字节，有填充补齐。

（2）TCP 连接的建立

TCP 连接的建立采用 “三次握手”的方法。

一般情况下，双方连接的建立由其中一方发起。如图 29(a)所示：

* 主机 A 首先向主机 B 发出连接请求报文段，其首部的 SYN 同步位为 1，同时选择一个序号 x；
* 主机 B 收到此连接请求报文后，若同意建立连接，则向主机 A 发连接响应报文段。在响应报文段中，SYN 同步位为 1，确认序号为 x+1，同时也为自己选择一个序列号 y；
* 主机 A 收到此确认报文后，也向主机 B 确认，这时，序号为 x+1，确认序号为 y+1 。

当连接建立后，A、B 主机就可以利用 TCP 进行数据传输了。

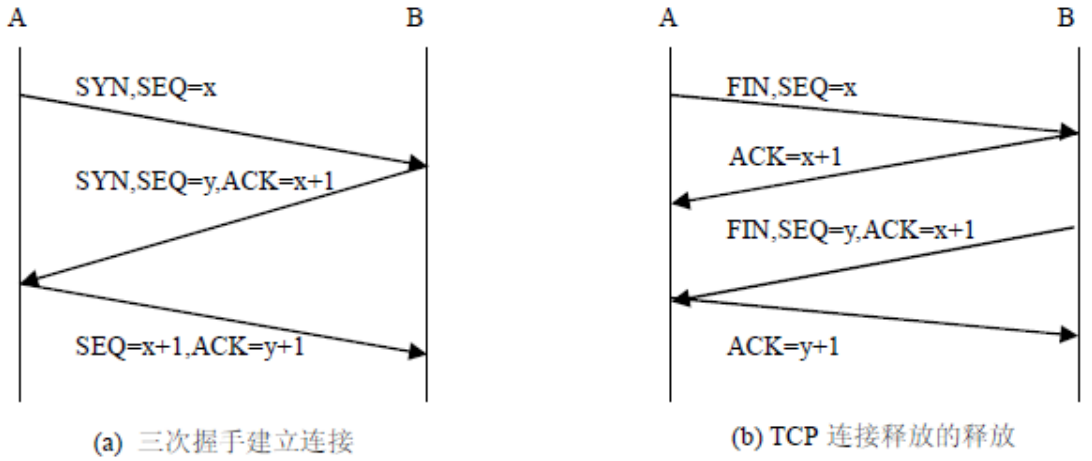


图 29 TCP 的连接和释放

（3）TCP 连接的释放

在数据传输结束后，任何一方都可以发出释放连接的请求，释放连接采用所谓的 “四次握手”方法。如图 29(b)所示，假如主机 A 首先向主机 B 提出释放连接的请求，其过程如下：

* 主机 A 向主机 B 发送释放连接的报文段，其中，FIN 终止位为 1，序号 x 等于前面已经发送数据的最后一个字节的序号加 1；

* 主机 B 对释放连接请求进行确认，其序号等于 x+1。这时从 A 到 B 的连接已经释放，连接处于半关闭状态，以后主机 B 不再接收主机 A 的数据。但主机 B 还可以向主机 A 发送数据，主机 A 在收到主机 B 的数据时仍然向主机 B 发送确认信息。
* 当主机 B 不再向主机 A 发送数据时，主机 B 也向主机 A 发释放连接的请求；
* 同样主机 A 收到该报文段后也向主机 B 发送确认。

（4 ）TCP 数据传输

TCP 可以通过检验序号和确认号来判断丢失、重复的报文段，从而保证传输的可靠性。TCP 将要传送的报文看成是由一个个字节组成的数据流，对每个字节编一个序号。在连接建立时，双方商定初始序号（即连接请求报文段中的 SEQ 值）。TCP 将每次所传送的第一个字节的序号放在 TCP 首部的序号字段中，接收方的 TCP 对收到每个报文段进行确认，在其确认报文中的确认号字段的值表示其希望接收的下一个报文段的第一个数据字节的序号。

由于 TCP 能提供全双工通信，因此，通信中的每一方不必专门发送确认报文段，而可以在发送数据时，捎带传送确认信息，以此来提高传输效率。

2. 实验工具软件简介

（1）3CDaemon 软件

3CDaemon 是 3Com 公司推出的功能强大的集 FTP Server、TFTP Server、Syslog Server 和 TFTP Client 于一体的集成工具，界面简单，使用方便。

这里主要介绍实验中需要用到的 FTP Server 功能。

* 主界面如图 30 所示，左窗格第二项为 FTP Server；

图 30 3CDaemon 主界面

* 配置 FTP Server 功能：选中左窗格功能窗口，打开 FTP Server 按钮，单击窗格中的 Configure FTP Server 按钮，打开 3CDaemon Configuration 配置窗口，如图 31 所示，配置 FTP Server 功能。

这里需要设置的就是 “Upload/Download ”路径，作为 FTP Server 的文件夹，其它选

项可以使用系统缺省设置。设置完成后，单击确认按钮，设置生效。

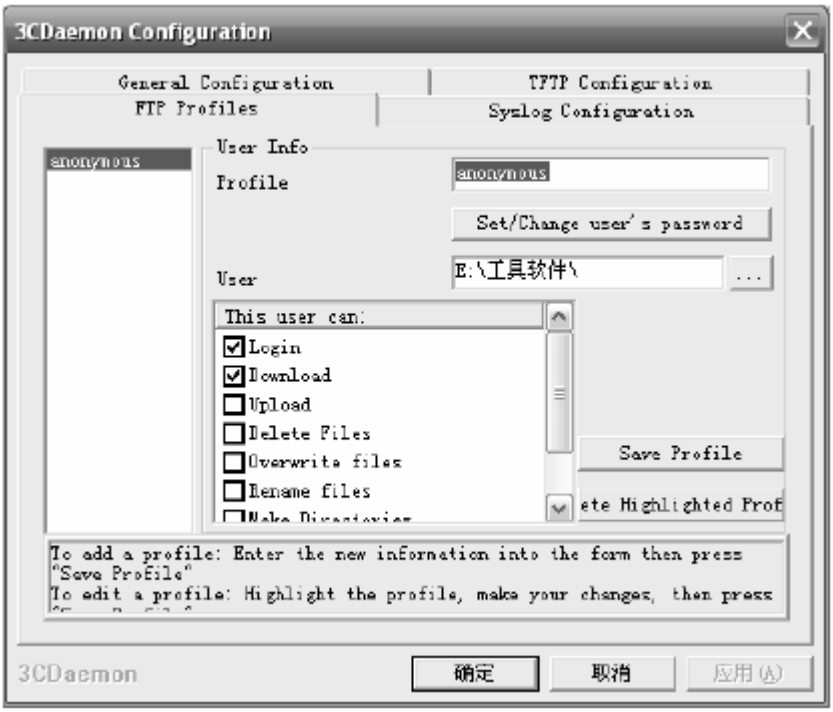


图 31 3CDaemon Configuration 配置窗口

在实验中，我们使用 3CDaemon 系统内置的匿名帐户 “anonymous”登陆 FTP 服务器，客户端使用微软 FTP 客户端命令，关于 Ftp 命令的说明可以参考本章 5.5.2 FTP 协议分析一节的实验工具软件介绍。

3．实验环境与说明

（1）实验目的

学习 3CDaemon FTP 服务器的配置和使用，分析 TCP 报文格式，理解 TCP 的连接建立、和连接释放的过程。

（2）实验设备和连接

实验设备和连接图如图 32 所示，一台锐捷 S2126G 交换机连接了 2 台 PC 机，分别命名为 PC1、PC2，交换机命名为 Switch。

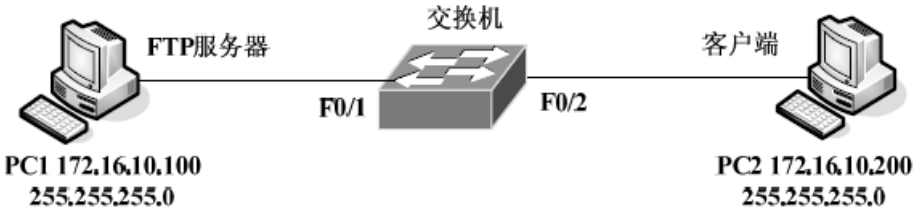


图 32 TCP 协议分析实验连接图

（3）实验分组

每四名同学为一组，其中每两人一小组，每小组各自独立完成实验。

4．实验步骤

步骤 1：按照如图 32 所示连接好设备，配置 PC1 和 PC2 的 IP 地址，验证连通；（编者

注:实验室中任何一台 PC 都可以作为模型中的 PC1 和 PC2;用Ｓｅｒｖ-Ｕ软件代替 3CDaemon 软件即可。)

步骤 2：按照上面 3CDaemon 软件的介绍方法在 PC1 上建立 FTP 服务器；

步骤 3：在 PC1 和 PC2 中运行 Ethereal，开始截获报文，为了只截获到与我们实验有关的内容，将截获条件设置为对方主机的 IP 地址，如 PC1 的截获条件为“host 172.16.10.200 ”；

步骤 4：在： PC2 上打开命令行窗口，执行如下操作：

```
C:\Documents and Settings\Administrator>ftp
ftp> open
To 172.16.10.100
Connected to 172.16.10.100.
220 3Com 3CDaemon FTP Server Version 2.0
User (172.16.10.100:(none)): anonymous
331 User name ok, need password
Password:
230-The response '' is not valid.
230-Next time, please use your email address as password.
230 User logged in
ftp> quit
221 Service closing control connection
C:\Documents and Settings\Administrator>
```

步骤 5：停止截获报文，将截获的结果保存为 FTP-学号，按下列要求分析截获的结果；

1）结合本节 TCP 协议介绍部分的内容，分析 TCP 连接建立的 “三次握手”过程，找到对应的报文，填写表 12（传输方向填写 PC2=>PC1 或 PC2<=PC1 ）。

表 12 TCP 连接建立报文分析

报文号	传输方向	源端口	目的端口	序　号	确认序号	同步位 SYN	确认位 ACK

注意:Ethereal 协议树中 TCP 协议下的“SEQ/ACK analysis”的内容 （这不是 TCP 报文的真实内容,而是 Ethereal 给我们提供信息),找到 TCP 数据传输报文的序号和确认报文

2）从 FTP-学号的报文中的第一个 FIN=1 的 TCP 报文开始分析 TCP 连接释放的 “四次握手”过程，填写表 13。

表 13 TCP 连接连接释放报文分析

报文号	传输方向	源端口	目的端口	序　号	确认序号	终止位 FIN	同步位 SYN	确认位 ACK

6. 应用层协议分析

网络体系结构中的最高层是应用层，它包括了所有的高层协议，并且随着网络应用的日益推广，不断有新的协议加入。TCP/IP 体系的应用层协议主要有：

＊ 域名服务 DNS （Domain Name System），用于实现互联网中主机域名到 IP 地址的映射功能；

＊ 文件传输协议 FTP（File Transfer Protocol），用于实现互联网中交互式文件传输；

＊ 超文本传输协议 HTTP（Hyper Text Transfer Protocol），用于 WWW 服务。

＊ 电子邮件协议 SMTP （Simple Mail Transfer Protocol）和 POP3 （Post Office Protocol），用于实现电子邮件的传送和读取功能；

＊ 远程终端协议 TELNET，用于实现互联网中远程登录功能；

计算机通信的对象是应用层中的应用进程，在 TCP/IP 体系中，两个应用进程采用客户服务器方式进行通信。客户服务器方式描述进程之间服务和被服务关系。当 A 进程需要 B 进程的服务时，A 是客户，B 是服务器。也许在下次通信时，B 需要 A 的服务，此时，B 是客户而 A 是服务器。客户与服务器的通信关系一旦建立，通信就可以是双向的，客户和服务器都可以发送和接收信息。

FTP 协议分析实验

1. FTP 协议简介协议简介

FTP 是文件传输协议 （File Transfer Protocol）的简称。

FTP 基于 TCP 协议，它通过两个 TCP 连接来传输一个文件，一个是控制连接，另一个是数据连接。相应的，在进行文件传输时，FTP 需要两个端口，分别用于控制连接端口 （用于给服务器发送指令以及等待服务器响应）和数据传输端口 （在客户机和服务器之间发送一个文件或目录列表）。

两种连接的建立都要经过一个 “三次握手”的过程，同样，连接释放也要采用 “四次握手”方法。控制连接在整个回话期间一直保持打开状态。数据连接是临时建立的，在文件传送结束后被关闭。

FTP 的连接模式有两种，PORT 和 PASV。PORT 模式是一个主动模式，PASV 是被动模式，这里都是相对于服务器而言的。

当 FTP 客户以 PORT 模式连接服务器时,它首先动态地选择一个端口号连接服务器的 21 端口,注意这个端口号一定是 1024 以上的,因为 1024 以前的端口都已经预先被定义好，被一些典型的服务使用或保留给以后会用到这些端口的资源服务。经过 TCP 的三次握手后，控制连接被建立。这时客户就可以利用这个连接向服务器发送指令和等待服务器响应了。当需要从 （或向）服务器传送数据时，客户会发出 PORT 指令告诉服务器用自己的那个端口来建立一条数据连接 （这个命令由控制连接发送给服务器），当服务器接到这一指令时，会使用 20 端口连接客户指定的端口号，用以数据传送。

当 FTP 客户以 PASV 模式连接服务器时，控制连接的建立过程与 PORT 模式相同，不同的是，在数据传送时，客户不向服务器发送 PORT 指令而是发送 PASV 指令告诉服务器自己要连接服务器的某一个端口，如果这个服务器上的这个端口是空闲的可用的，那么服务器会返回 ACK 的确认信息，此后，数据连接被建立并返回客户机所要的信息；如果服务器的

这个端口被另一个资源所使用，那么服务器返回 UNACK 的信息，FTP 客户会再次发送 PASV 命令，这也就是所谓的连接建立的协商过程。

需要强调的是微软自带的 FTP 客户端命令，不支持 PASV 模式。

2. 实验工具软件简介

（1）Serv-U 软件

Serv-U 是一种被广泛运用的 FTP 服务器端软件，支持 9x/ME/NT/2K 等全 Windows 系列。FTP 服务器用户通过它用 FTP 协议能在 internet 上共享文件。它设置简单，功能强大，性能稳定。此外，Serv-U 并不是简单地提供文件的下载，还为用户的系统安全提供了相当全面的保护。

本次实验中，我们使用 Serv-U FTP Server 6.2.0.1 汉化版软件作为 FTP 服务器。有关 Serv-U 的系统配置请阅读软件的帮助文档。

（2）微软 FTP 客户端命令

实验中，我们使用 Windows 自带的 FTP 命令和 IE 浏览器来作为 FTP 的客户端。下面简单的介绍一下常用 FTP 客户端命令。

FTP 的命令格式：ftp [-v] [-d] [-i] [-n] [-g] [-w:windowsize] [主机名/IP 地址]

其中：

-v 不显示远程服务器的所有响应信息；

-n 限制 ftp 的自动登录；

-i 在多个文件传输期间关闭交互提示

-d 允许调试、显示客户机和服务器之间传递的全部 ftp 命令；

-g 不允许使用文件名通配符；

-w：windowsize 忽略默认的 4096 传输缓冲区。

使用 FTP 命令登录成功远程 FTP 服务器后进入 FTP 子环境，在这个子环境下，用户可以使用 FTP 的内部命令完成相应的文件传输操作。

FTP 常用内部命令如下：

* open host[port]：建立指定 ftp 服务器连接，可指定连接端口。

*user user-name[password][account]：向远程主机表明身份，需要口令时必须输入。

* append local-file [remote-file]：将本地文件追加到远程系统主机，若未指定远程系统文件名，则使用本地文件名。

* cd remote-dir：进入远程主机目录。

* cdup：进入远程主机目录的父目录。

* cd [dir]：将本地工作目录切换至 dir。

* dir [remote-dir][local-file]：显示远程主机目录，并将结果存入本地文件。

* get remote-file[local-file]：将远程主机的文件 remote-file 传至本地硬盘的 local-file。

* ls [remote-dir][local-file]：显示远程目录 remote-dir，并存入本地文件 local-file。

* put local-file [remote-file]：将本地文件 local-file 传送至远程主机。

* mput local-file：将多个文件传输至远程主机。

* nlist [remote-dir][local-file] ：显示远程主机目录的文件清单，存入本地硬盘 local-file。

* bye 或 quit：退出 ftp 会话过程。

3．实验环境与说明

（1）实验目的

学习 Serv-U FTP Server 服务软件的基本配置和 FTP 客户端命令的使用，分析 FTP 报文格式和 FTP 协议的工作过程。

（2）实验设备和连接

实验设备和连接图如图 40 所示，一台锐捷 S2126G 交换机连接了 2 台 PC 机，分别命名为 PC1、PC2，交换机命名为 Switch。

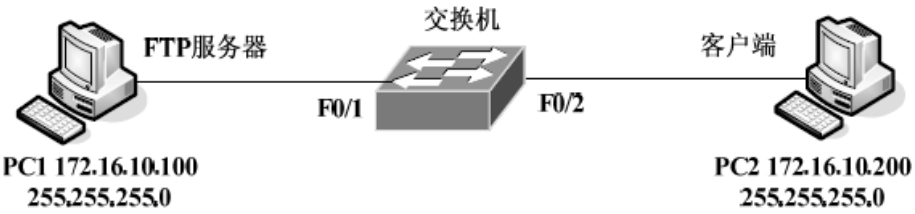


图 40 FTP 协议分析实验连接图

（3）实验分组

每四名同学为一组，其中每两人一小组，每小组各自独立完成实验。

4．实验步骤

步骤 1：按照如图 40 所示连接好设备，配置 PC1 和 PC2 的 IP 地址，验证连通；（编者注：实验室中任何一台 PC 都可以作为模型中的 PC1 和 PC2。）

步骤 2：在上安装 Serv-U FTP Server，启动后出现图 41 所示界面。

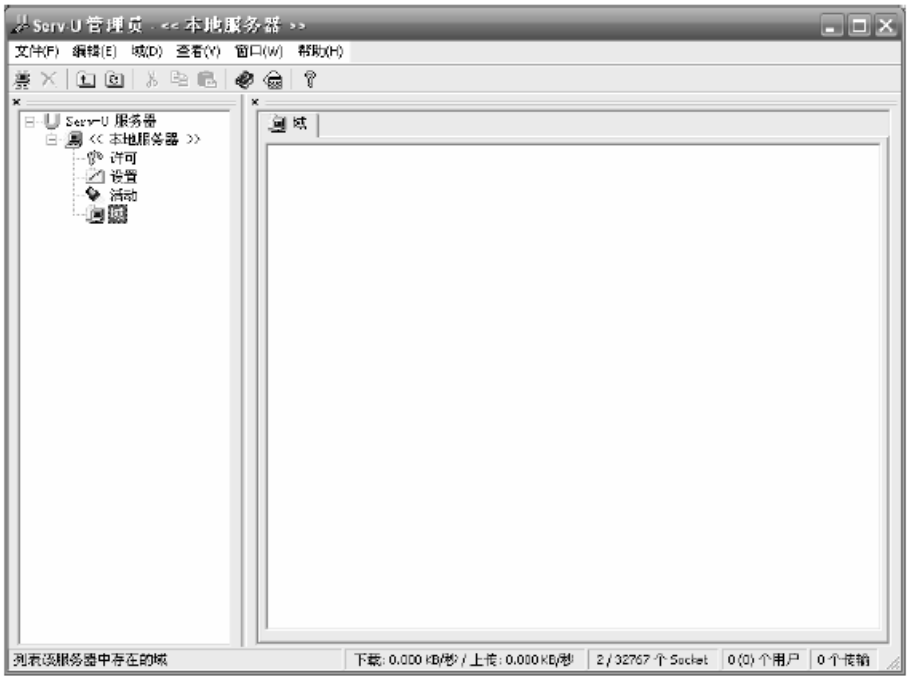


图 41 Serv-U FTP Server 主界面

点击左窗格目录树 Ser-U 服务器－本地服务器－域，右键菜单，选择新建域 （或者选择窗口菜单域－新建域），打开添加新建域向导，完成如下操作：

添加域 IP 地址：172.16.10.100；添加域名：test.com；设置域端口号：21

（默认）；设置域类型：存储于.INI 文件 （默认）。完成后界面如图 5.42 所示：

图 42 Serv-U FTP Server 域设置界面

完成上述操作后，还需要创建用于实验的用户帐号。点击左窗格用户，打开添加新建用户向导：添加用户名：test1；添加密码：123；设置用户主目录 （登陆文件夹）；设置是否将用户锁定于主目录：是（默认）。完成后界面如图 43 所示：

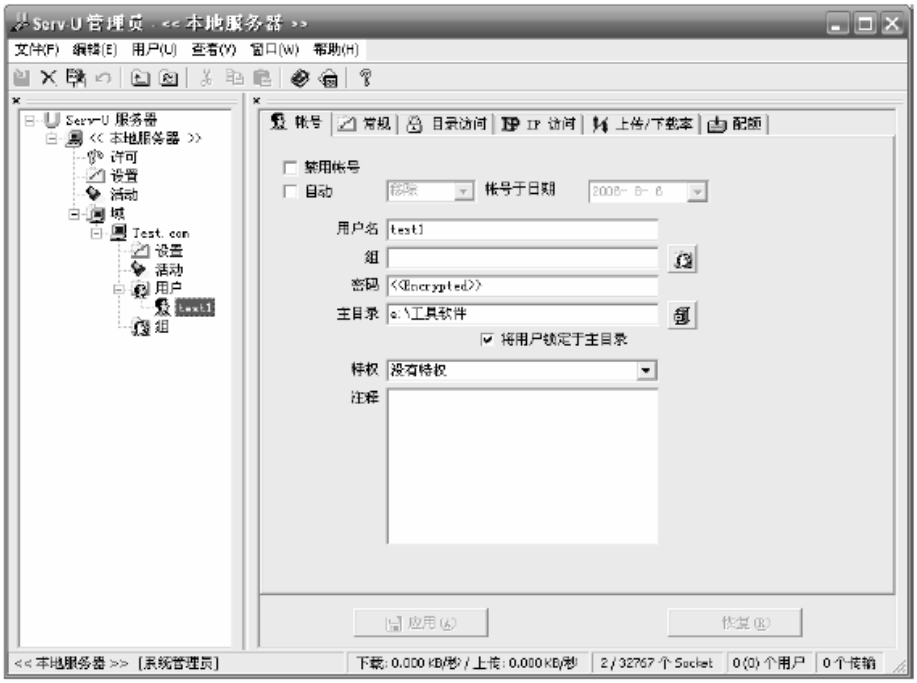


图 43 Serv-U FTP Server 用户设置界面

新建的用户只有文件读取和目录列表权限，为完成实验内容，还需要为新建的用户设置目录访问权限，方法为打开用户设置界面，点击目录访问标签按钮，按照图 44 所示进行配

置：

图 44 用户目录访问设置界面

FTP 服务器的配置就此完成，对 Serv-U FTP Server 的其它功能有兴趣的话可以参考相关帮助文档；

步骤 3：在 PC1 和 PC2 上运行 Ethereal，开始截获报文。

步骤 4：在 PC2 命令行窗口中登录 FTP 服务器，根据步骤 2 中的配置信息输入用户名和口令，参考命令如下：

```
C:\ >ftp
ftp> open
To 172.16.10.100                          //登录 ftp 服务器
Connected to 172.16.10.100.
220 Serv-U FTP Server v6.2 for WinSock ready...
User(none): test1                         //输入用户名
331 User name okay, need password.
Password:123                              //输入用户密码
230 User logged in, proceed.              //通过认证，登录成功
ftp> quit                                 //退出 FTP
221 Goodbye!
```

步骤 5：停止截获报文，将截获的报文保存为 FTP-1-学号。

步骤 6：在 PC1 和 PC2 上再次运行 Ethereal，开始截获报文。

步骤 7：在 PC2 上打开浏览器窗口，地址栏输入 ftp:// 172.16.10.100；由于未启用匿名帐户，连接断开并提示图 5.45 所示对话框。

图 45FTP 文件夹错误

此时，单击右键快捷菜单选择登陆，在图 46 所示登陆对话框中输入用户名和密码，登陆 FTP 服务器；

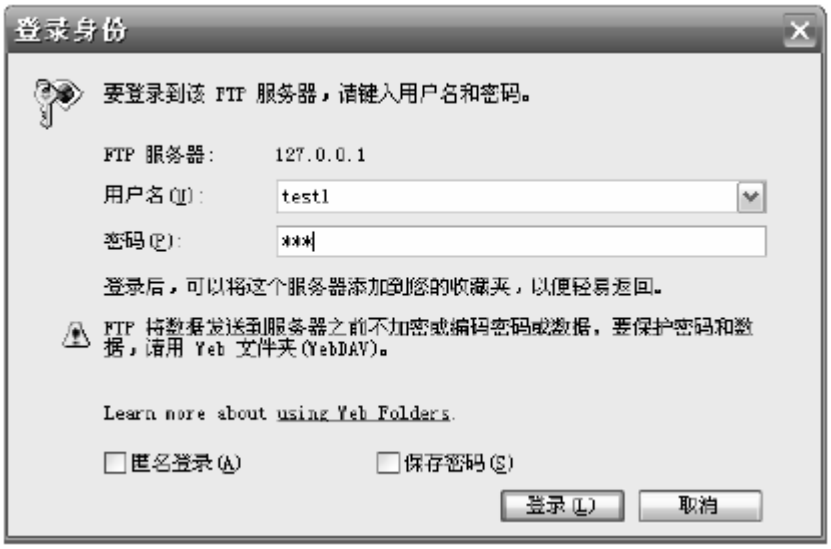


图 46 FTP 登陆对话框

步骤 8：在浏览器显示的用户目录下创建一个名为 ftp-学号的文件夹，并将本地的一个文本文件 f1.txt 粘贴到新建文件夹下，停止截获报文，将截获的报文保存为 FTP-2-学号。分析两次截获的报文，回答如下问题。

1）对 FTP-1-学号进行分析，找到 TCP 三次握手后第一个 FTP 报文，分析并填写表 17。

表 17 FTP 报文格式分析

源 IP 地址		源端口	
目标 IP 地址		目标端口	
FTP 字段	字段值		字段所表达的信息
Response Code			
Response Arg			

2）在 FTP-1-学号中找出 FTP 指令传送和响应的报文，填写表 18；

表 18 FTP 指令和响应过程分析

过程	指令/响应	报文号	报文信息
User	Request		
	Response		
Password	Request		
	Response		
Quit	Request		
	Response		

3）对第二次截获的报文进行综合分析，观察 FTP 协议的工作过程。特别观察两种连接的建立过程和释放过程，以及这两种连接建立和释放的先后顺序，将结果填入表 19。

表 19 FTP 传送过程中的报文

文类型	所包括的报文序号号	客户端口号	服务器端口
控制连接的建立			
数据连接的建立			
FTP 数据传送			
FTP 指令传送和响应			
数据连接的释放			
控制连接的释放			

4 ）第二次截获的报文中，FTP 客户是以 PORT 模式还是 PASV 模式连接服务器？你是如何判断的？

_____

_____

5）FTP 中的匿名帐户是_____；