实验 1 五类双绞线的制作

1．1 实验目的

1．了解并掌握五类非屏蔽双绞线的构成。
2．掌握五类双绞线和 RJ-45 连接器的连接方法。
3．掌握五类双绞线的测试方法。

1．2 实验环境

1．每组所用工具及材料：五类非屏蔽双绞线 1 米，RJ-45 连接器 8 个，压线钳一把，测试仪一个。
2．每组一名同学，制作平行线和交叉线。

1．3 实验内容

1．观察五类双绞线和 RJ-45 连接器的构成。
2．制作平行线和交叉线。
3．测试已制作好的五类双绞线。

1．4 背景知识

一、线缆标准

双绞线的做法有两种国际标准：EIA/TIA568A 和 EIA/TIA568B，根据双绞线两端线序的不同，可制作两种双绞线：直通线和交叉线。直通线缆的 RJ-45 连接器两端都遵循 EIA/TIA 568A 或 EIA/TIA 568B 标准，直通线的每组线在两端是一一对应的，颜色相同的线在两端 RJ-45 连接器的相应槽中保持一致。交叉线缆的 RJ-45 连接器一端遵循 EIA/TIA 568A，另一端则采用 EIA/TIA 568B 标准，即 A 端 RJ-45 连接器的 1、2 对应 B 端 RJ-45 连接器的 3、6，A 端 RJ-45 连接器的 3、6 对应 B 端 RJ-45 连接器的 1、2。EIA/TIA 568A 标准描述的线序从左到右为:1-白绿、2-绿、3-白橙、4-蓝、5-白蓝、6-橙、7-白棕、8-棕。EIA/TIA 568B 标准描述的线序从左到右为：1-白橙、2-橙、3-白绿、4-蓝、5-白蓝、6-绿、7-白棕、8-棕。

交叉线线序为：

一端： 白橙 / 橙 / 白绿 / 蓝 / 白蓝 / 绿 / 白棕 / 棕

另一端：白绿 / 绿 / 白橙 / 蓝 / 白蓝 / 橙 / 白棕 / 棕

直通线线序为：

一端： 白橙 / 橙 / 白绿 / 蓝 / 白蓝 / 绿 / 白棕 / 棕

另一端：白橙 / 橙 / 白绿 / 蓝 / 白蓝 / 绿 / 白棕 / 棕

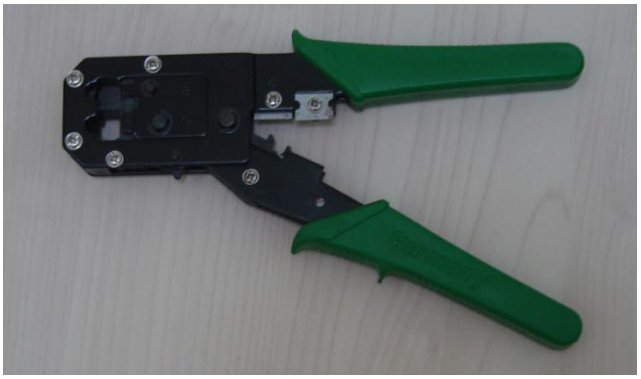
EIA/TIA-568A 线缆标准

顺序	所属线对	颜色	功能
针 1	对 2	白绿	Tx+
针 2	对 2	绿	Tx-
针 3	对 3	白橙	Rx+
针 4	对 1	蓝	在 10BaseT 和 100BaseT 中未使用
针 5	对 1	白蓝	在 10BaseT 和 100BaseT 中未使用
针 6	对 3	橙	Rx-
针 7	对 4	白棕	在 10BaseT 和 100BaseT 中未使用
针 8	对 4	棕	在 10BaseT 和 100BaseT 中未使用

EIA/TIA-568B 线缆标准

顺序	所属线对	颜色	功能
针 1	对 2	白橙	Tx+
针 2	对 2	橙	Tx-
针 3	对 3	白绿	Rx+
针 4	对 1	蓝	在 10BaseT 和 100BaseT 中未使用
针 5	对 1	白蓝	在 10BaseT 和 100BaseT 中未使用
针 6	对 3	绿	Rx-
针 7	对 4	白棕	在 10BaseT 和 100BaseT 中未使用
针 8	对 4	棕	在 10BaseT 和 100BaseT 中未使用

二、工具与材料认识



压线钳

RJ-45 连接器

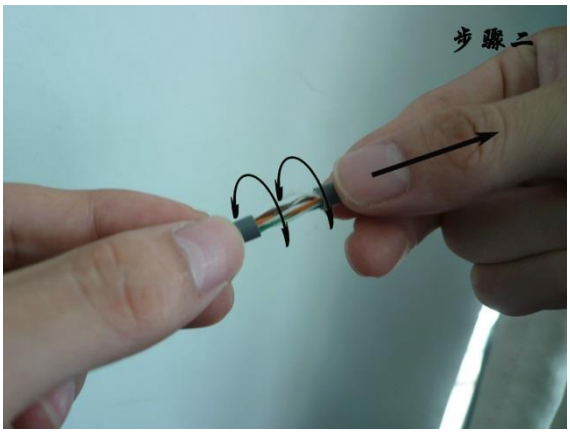
网络电缆测试仪

1．5 实验步骤

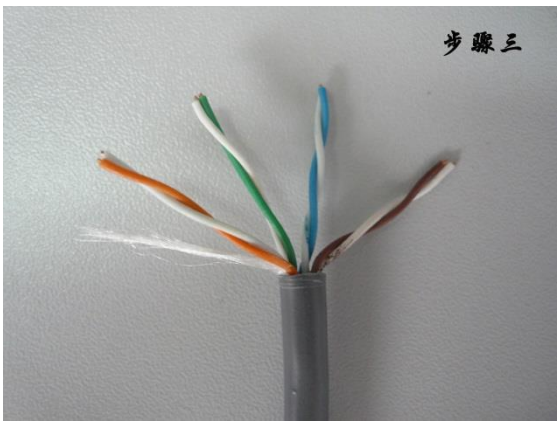
一、平行线的制作

1．用压线钳的剥线刀口将 5 类线的外保护套管划开（小心不要将里面的双绞线的绝缘层划破），刀口距 5 类线的端头至少 2 厘米。

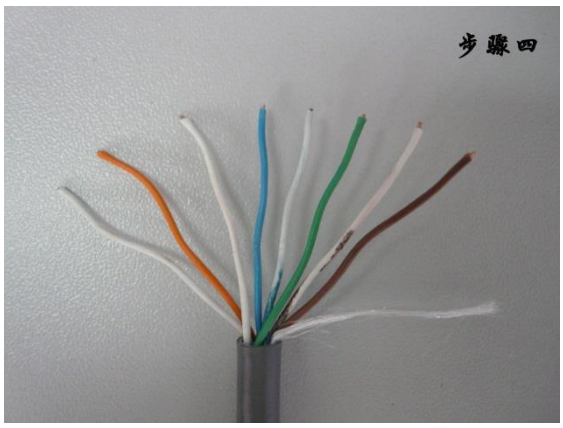
2．将划开的外保护套管剥去（旋转、向外抽）



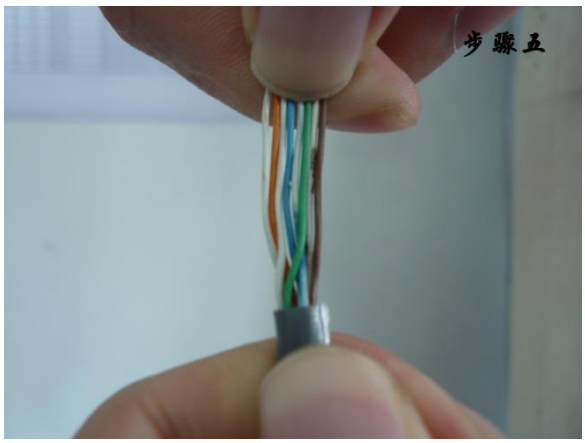
3．露出 5 类线电缆中的 4 对双绞线。



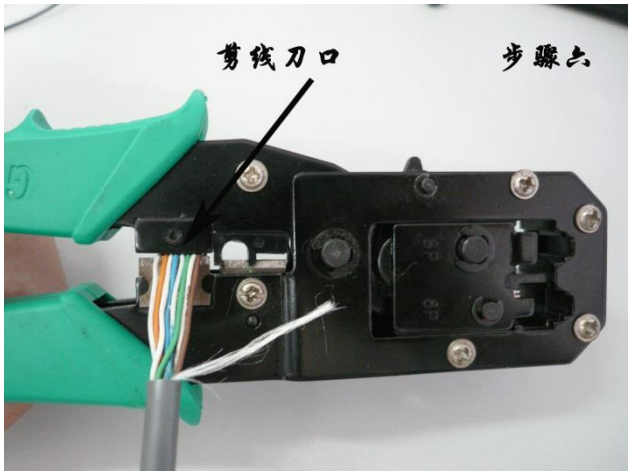
4．按照 T568B 的标准，即白橙、橙色、白绿、蓝色、白蓝、绿色、白棕、棕色线序将导线按规定的序号排好。



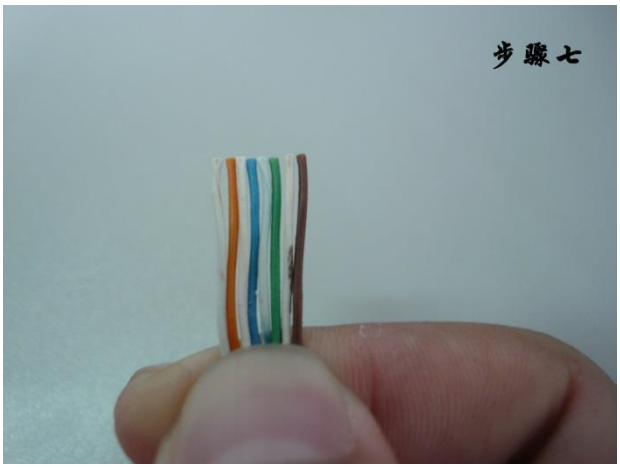
5．将 8 根导线平坦整齐地平行排列，导线间不留空隙。



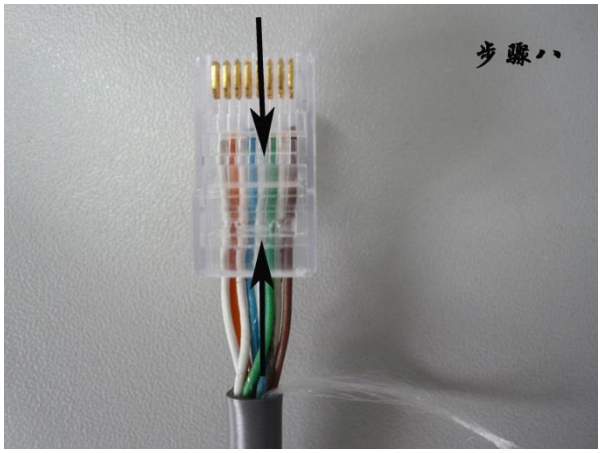
6．准备用压线钳的剪线刀口将 8 根导线剪断。



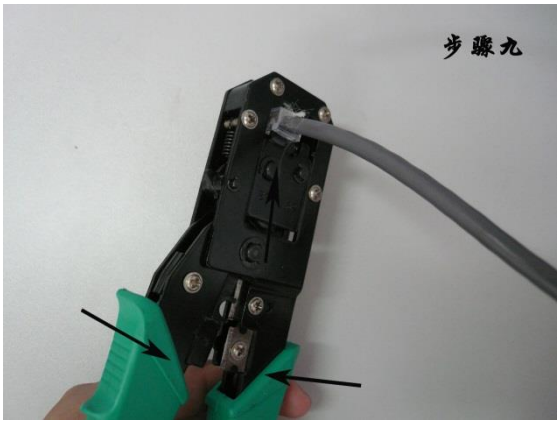
7．剪断电缆线。请注意：一定要剪得很整齐。剥开的导线长度不可太短（1cm～1.2cm）。可以先留长一些。不要剥开每根导线的绝缘外层。



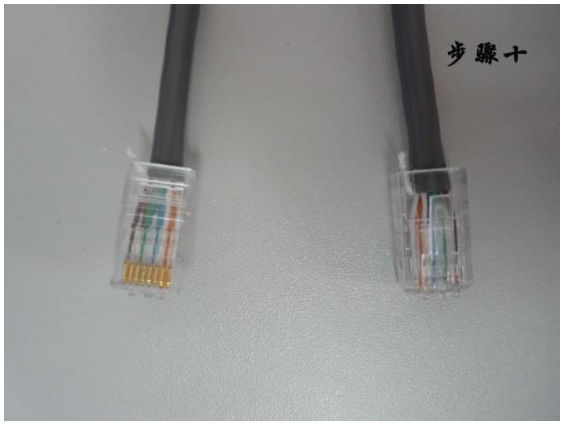
8．将剪断的电缆线放入 RJ-45 插头试试长短（要插到底，电缆线的外保护层最后应能够在 RJ-45 插头内的凹陷处被压实）。反复进行调整。



9．在确认一切都正确后（特别要注意不要将导线的顺序排列反了），将 RJ-45 插头放入压线钳的压头槽内，双手紧握压线钳的手柄，用力压紧。请注意，在这一步骤完成后，插头的 8 个针脚接触点就穿过导线的绝缘外层，分别和 8 根导线紧紧地压接在一起。



10．用同样的方式将双绞线的另一端制作完成。注意两端线序相同。



11.用测试仪测试已做好的网线。如果测线仪两端的指示灯依次亮起，证明双绞线制作正确。

二、交叉线的制作

将双绞线两端的线序分别按照 T568A 和 T568B 的标准，按照上述步骤制作交叉线。

1．6 实验要求

完成本次实验后，通过查找资料对双绞线进行系统地总结，整理并掌握双绞线的性能指标，进而了解并掌握不同的网络环境所应该使用的双绞线的类型。

1．7 思考与讨论

1．两台计算机通过五类双绞线直接连接，双绞线两端应分别使用什么标准？

2．两台计算机通过交换机连接起来，双绞线两端应分别使用什么标准？

实验 2 网络常用命令和网络服务安装

一、网络常用命令

2．1．1 实验目的

1．了解并掌握 Windows XP 常用的网络测试工具的基本功能和使用方法。
2．掌握使用网络工具测试网络状态的方法。
3．掌握科来网络分析系统的安装和使用。

2．1．2 实验环境

1．操作系统：Windows XP
2．科来网络分析系统
3．实验分组：每名同学一组，各自进行实验。

2．1．3 实验内容

1．学习并掌握网络命令：ping、ipconfig、arp、tracert、netstat 的功能和用法。
2．对每个网络命令分别进行参数验证、结果分析和总结。
3．安装科来网络分析系统并熟悉软件的使用。

2．1．4 背景知识

一、ping

1．功能

通过发送数据包，检测两台计算机之间的网络是否连通、网卡配置是否正确、IP 地址是否可用等。根据运行结果，可以初步判断 TCP/IP 参数是否正确，网卡和线路等是否存在故障。

2．命令格式

Ping [-t] [-a] [-l size] [-f] [-i TTL] [-r count] [-n count] [-s count] destination-list

3．参数说明

-t 使当前主机不断地向目标主机发送数据，直到按 Ctrl+C 组合键中断。
-a 显示目标 IP 的主机名称。
-l size 用 size 指定发送到目标主机的数据包的大小，默认是 32 字节，最大值为 65500 字节（Windows 7 操作系统下）。
-f 在数据包中发送“不要分段”标志，使数据包不被路由器分段。
-i TTL 将“生存时间”字段设置为 TTL 指定的值。
-r count 在“记录路由”字段中记录发出和返回数据包的路由。通常情况下，发送的数据包是通过一系列路由才到达目标主机的。
-n count 指定 ping 执行次数，即用 count 指定发送数据包的数目，默认值为 4。
-s count 用 count 指定的跃点数的时间戳。
Destination-list 指定要 ping 的目标主机。

二、ipconfig

1．功能

用于显示当前 TCP/IP 参数，如果所在的局域网使用动态主机地址配置协议，通过该命令可以了解到本地计算机是否成功地租用到一个 IP 地址，并显示 IP 地址的相应参数。

2．命令格式

Ipconfig [/all/renew[adapter]|/release[adapter]]

3．参数说明

不带任何参数的命令执行后，只显示 IP 地址、子网掩码和默认网关值，同时显示适配器的名称。

[/all] 显示 TCP/IP 完整的信息，本地网卡的物理地址以及主机名称。

[/release[adapter]] 该参数只在向 DHCP 服务器租用其 IP 地址的计算机上起作用，该参数将所有接口的租用 IP 地址重新交付给 DHCP 服务器。

[/renew[adapter]] 该参数是使本地计算机设法与 DHCP 服务器联系，并租用一个 IP 地址。

三、ARP

1．功能

用于显示、添加和删除 ARP 缓存中的内容。

2．命令格式

arp –s inet-addr eth-addr [if-addr]

arp –d [inet-addr [if-addr]]

arp –a [inet-add] [-N if-addr]

3．参数说明

-a 通过查询当前协议数据显示当前 ARP 缓存表，即显示 IP 地址和物理地址的对应关系。

-d 删除 ARP 高速缓存中的当前内容。

-s 手工向 ARP 高速缓存中写入内容。

inet-addr IP 地址。

eth-addr 物理地址。

四、tracert

1．功能

用于显示数据包访问网络中某个节点时所经过的路径，进行路由跟踪，以及到达每个节点所需的时间，并可以用来分析网络和排查网络故障。

2．命令格式

Tracert [-d] [-h maximum-hops] [-j host-list] [-w timeout] [target_name]]

3．参数说明

-d 不将地址解析为主机名

-h maximum-hops 用 maximum-hops 指定搜索到目的地址的最大跳数。

-j host-list 按照主机列表中的地址释放源路由。

-w timuout 用 timeout 指定超时时间间隔，单位为毫秒。

target_name 目标主机。

五、netstat

1．功能

用于显示当前网络连接以及每个网络接口设备的状态信息。

2．命令格式

netstat [-a] [-e] [-n] [-s] [-p proto] [-r]

3．参数说明

-a 显示当前的 TCP 连接的端口号，以及计算机侦听到的 TCP 和 UDP 端口号。

-e 显示以太网统计信息。

-n 以数字表格形式显示地址和端口信息。

-s 显示每个协议的使用状态。默认情况下显示 TCP、UDP、ICMP、和 IP 协议的统计信息。

-p proto 显示 proto 指定的特定协议的具体使用信息。
-r 显示本机的 IP 路由表内容，该参数与 route print 命令等价。

2．1．5 实验步骤

（一）、Windows XP 网络命令

1．通过以下命令检测网络连通性

（1）ping 本机 IP 如果本机协议参数配置正确，计算机应返回 ping 命令的正确响应信息。如果没有应答，则表示本地计算机配置或安装存在问题。

（2）ping <局域网内其他 IP> 如果收到正确的响应信息，表示本地网络中的网卡和传输介质运行正确。如果收到错误的应答信息，则表明可能会有如下问题之一：

- 子网掩码不正确，应重新配置。
- 网卡配置错误，应查看网卡指示灯有无闪烁，检查网卡设置和驱动程序。
- 网络连接有问题，检查网线的连通性和集线器、交换机的连接。

（3）ping <网关 IP> 如果收到正确的应答信息，则表示局域网中的网关路由器正常运行。

（4）ping <一个远程域名> 如果正确说明域名服务器参数设置正确，并表示该机可以正常访问因特网了。否则，说明域名服务器的 IP 配置不正确或域名服务器有故障。

2．用 ipconfig 命令查看本机的协议参数。

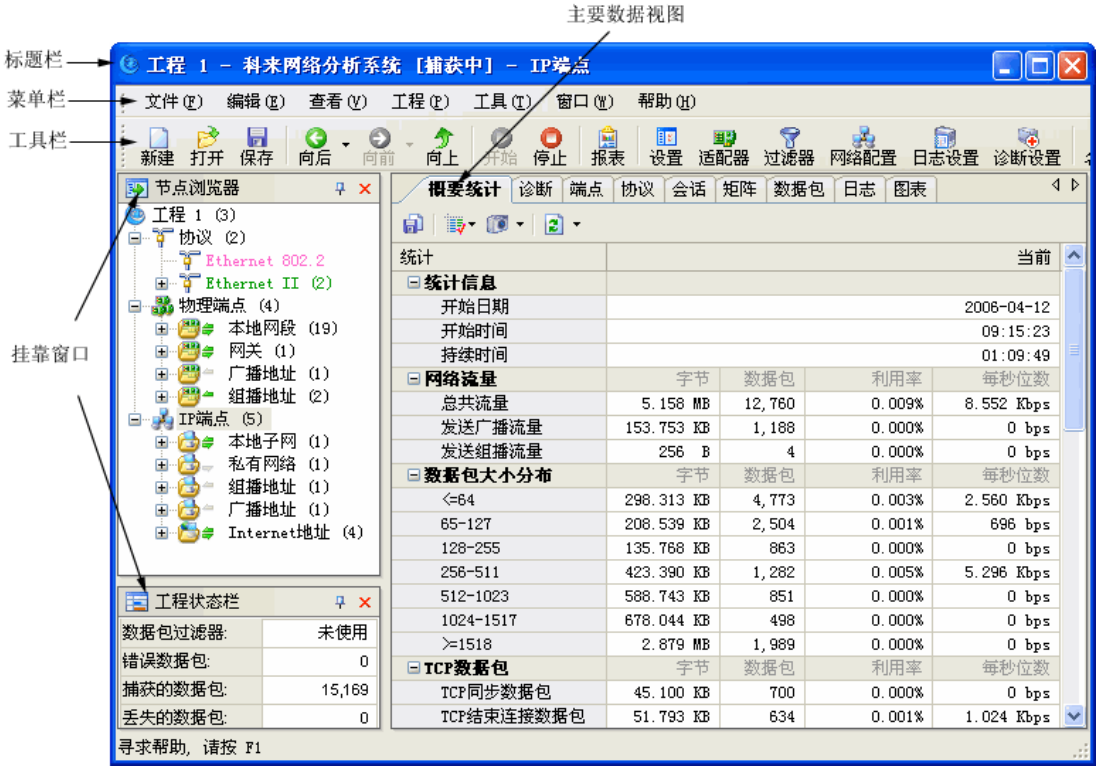
3．用 arp 命令查看、添加和删除 arp 高速缓存中的项目。

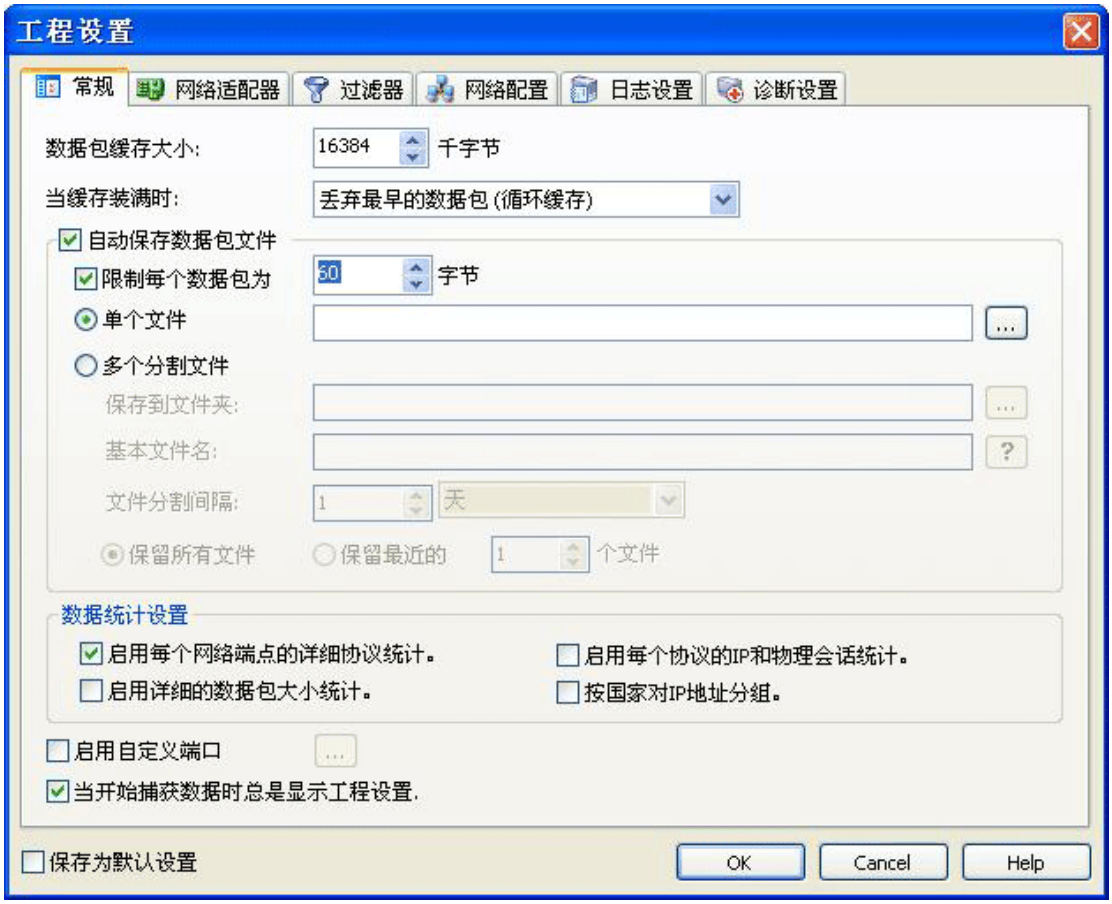
4．用 tracert 命令跟踪一个站点所经过的路由信息。

5．用 netstat 命令查看本机的网络连接和接口状况。

（二）、科来网络分析系统的使用

1．熟悉并掌握科来网络分析系统的界面、功能和用法。





以上界面是科来网络分析系统的两个主要界面，其他详细内容和使用方法可参见科来网络分析系统《用户使用手册》和《快速入门指南》，也可以直接访问科来软件的网站，该网站提供了很多技术解决方案和技术难题解答等，网址：http://www.colasoft.com.cn/。

2．开启科来网络分析系统，进行捕获。

3．用 ping 命令，ping 临近的计算机。

4．将捕获的数据包保存下来，观察捕获到的数据包的情况。

2．1．6 实验要求

完成本次实验后，通过查找资料，总结常用的网络命令的使用方法和适用场合，以及解决不同的网络问题需要使用哪种网络命令。了解并掌握科来网络分析系统的使用方法。

2．1．7 思考与讨论

1．说明以上五个网络命令在计算机网络中都有什么作用？

2．通过用科来网络分析系统捕获数据包，回答下列问题

（1）你捕获了多少数据包？

（2）在你捕获的数据包中有几个 IP 地址？这些 IP 地址与你希望的网络请求一致么？

二、网络服务安装

2．2．1 实验目的

1．了解并掌握 DNS 和 IIS 的安装方法。

2．掌握 DNS 和 IIS 的基本配置方法以及验证 DNS、IIS 的方法。

2．2．2 实验环境

1．操作系统：Windows XP

2．所需软件：Windows XP 操作系统光盘内容已复制到 F 盘下“Windows XP”文件夹下，安装 DNS 和 IIS 服务所需文件（192.dns、boot、cache.dns、dns.exe、dnsmgr.dll、dnsperf.dll、dnsperf.h、dnsperf.ini、netdns.inf、place.dns）已拷贝到 F 盘“配置 dns 和 iis 所需文件”文件夹下。

3．实验分组：两名同学一组，安装和配置 DNS 和 IIS，在客户端进行验证，然后一起观察验证结果。

2．2．3 实验内容

1．安装并配置 DNS 服务器和 IIS。

2．配置 WWW 和 FTP 服务，验证 DNS、WWW 和 FTP 服务的运行。

2．2．4 实验步骤

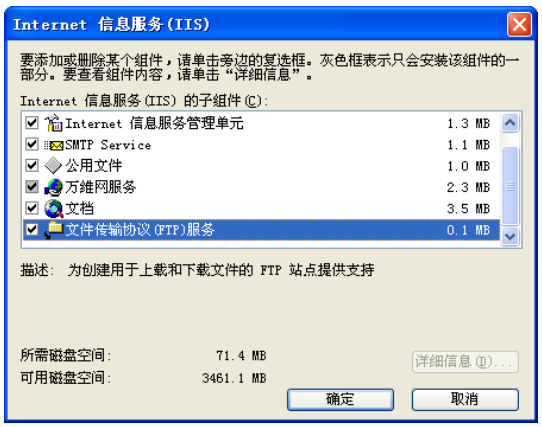
（一）、安装 DNS 和 IIS 服务器

1．将文件 netdns.inf 拷贝到 C:\windows\inf 下。

2.打开 C:\windows\inf【该文件夹初始为隐藏】下的文件 netoc.inf，在 SNMP 下增加一行“DNS”，然后保存

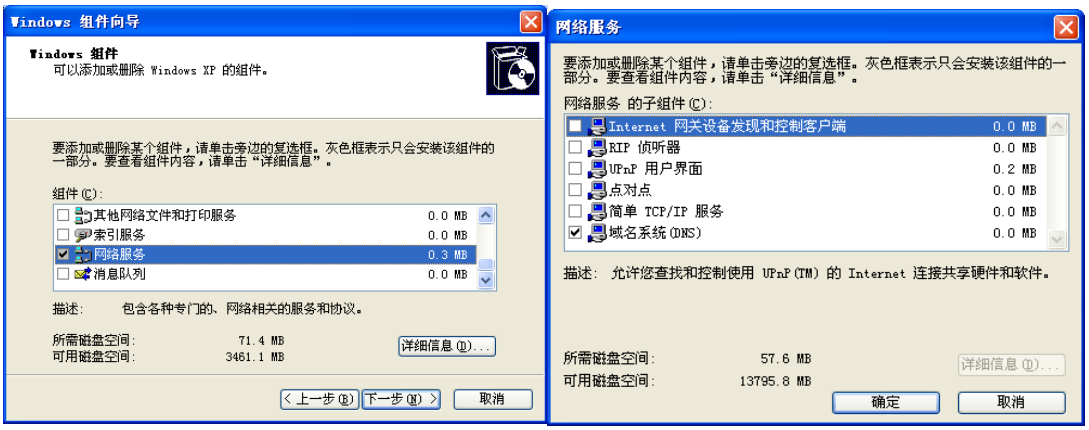
[Optional Components]
NetOC ;Top level option
NetServices
FileAndPrint
SNMP
DNS

3．打开控制面板----添加或删除程序----添加/删除 Windows 组件，选择“**Internet 信息服务（IIS）**”，再单击下面的“**详细信息**”选择需要的项目，在右图点“确定”。

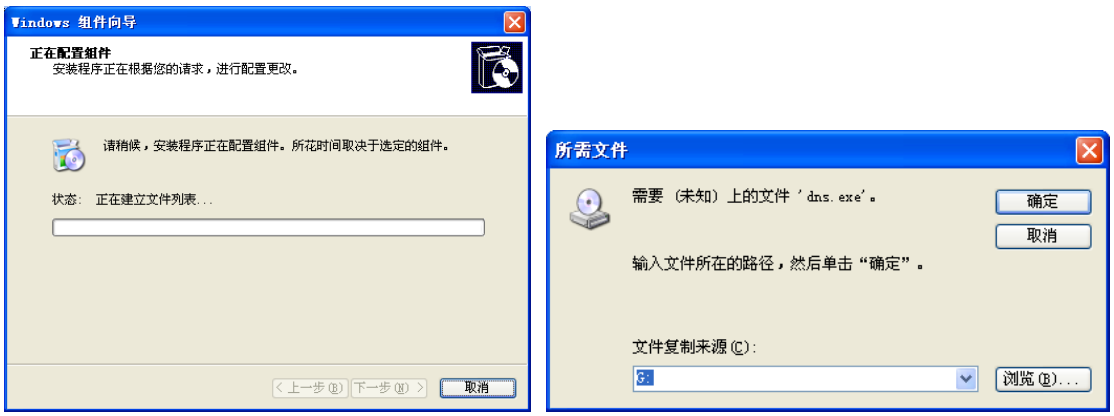


4．选择 DNS 服务：在“**Windows 组件向导**”窗口，选择“**网络服务**”，再点击下面的“**详**

细信息”，在弹出的“**网络服务**”窗口中只选择“**域名系统**”，其他不选。然后点“**确定**”，返回到“**Windows 组件向导**”窗口。



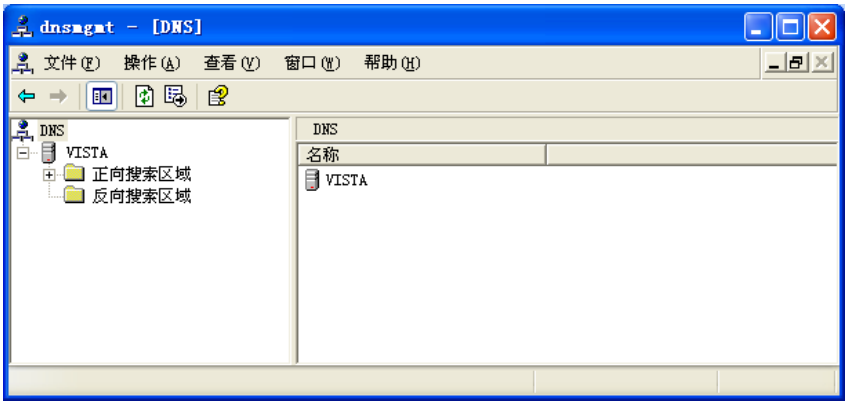
5．在“**Windows 组件向导**”窗口点“**下一步**”，出现下面右侧窗口，点击“**浏览**”，将路径指向保存上述文件的位置。点确定。则 DNS 安装完成。



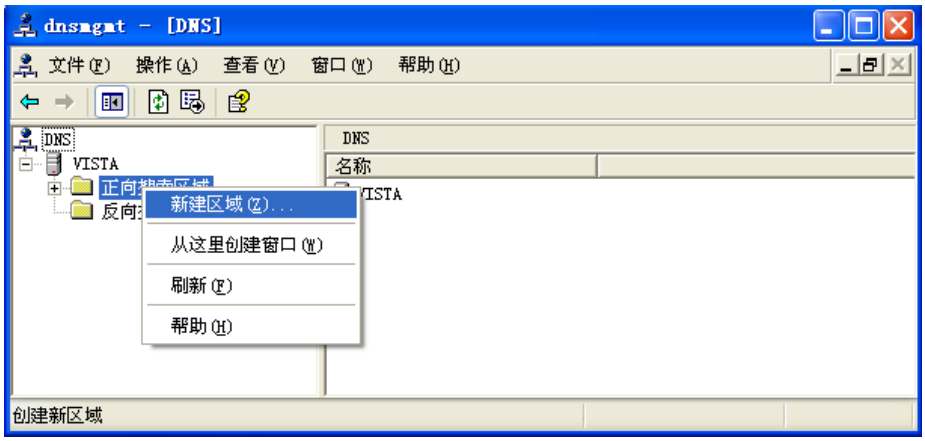
6．开始安装 IIS，系统提示插入 Windows XP 光盘，点确定后开始安装。直至安装完成。（**所需文件在自建的目录以及 Windows XP 的 I386 目录下可以找到**）

（二）、配置 DNS

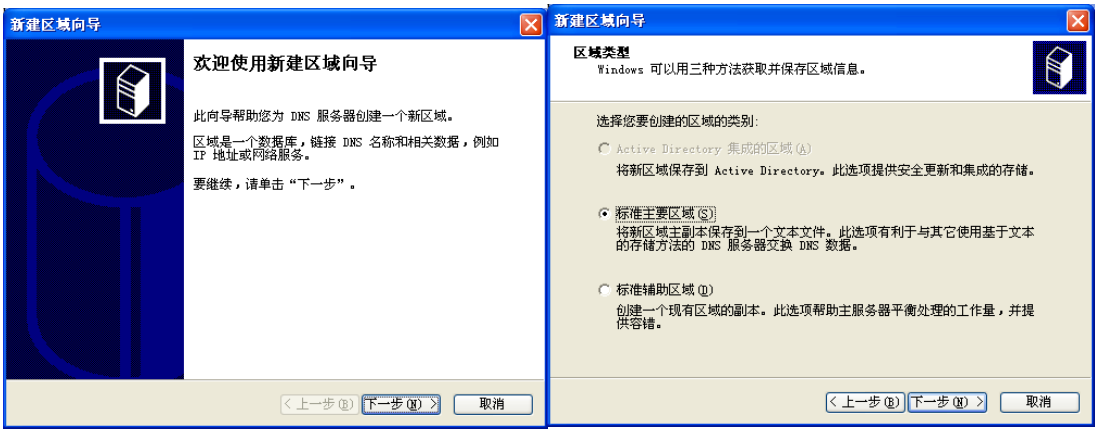
1．在“控制面板----管理工具”中打开“DNS”，如下图



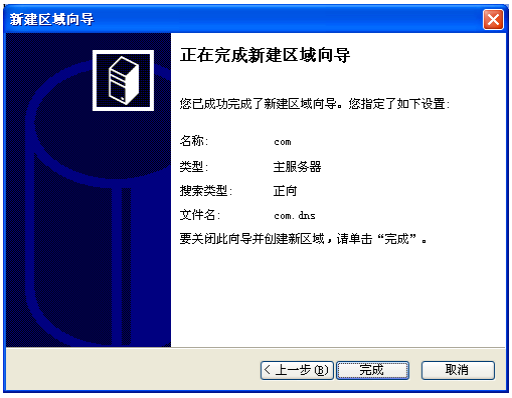
2．右键单击“正向搜索区域”，在出现的菜单中点“新建区域”。



出现如下左图所示，点下一步，出现如下右图所示。

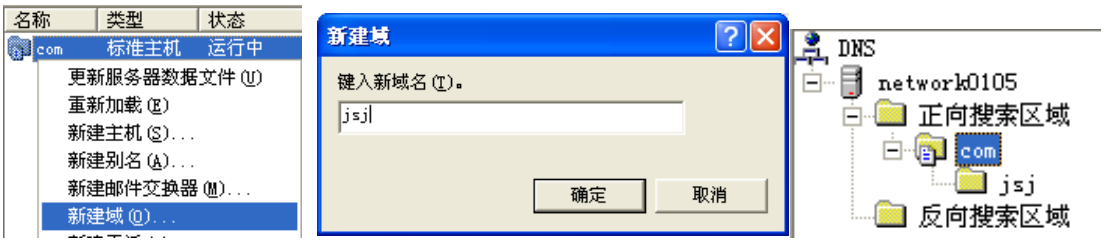


默认选择“标准主要区域”，点下一步，出现如下左图所示，在名称处输入“com”，点下一步，出现如下右图，再点下一步，出现完成窗口，点击完成即可。

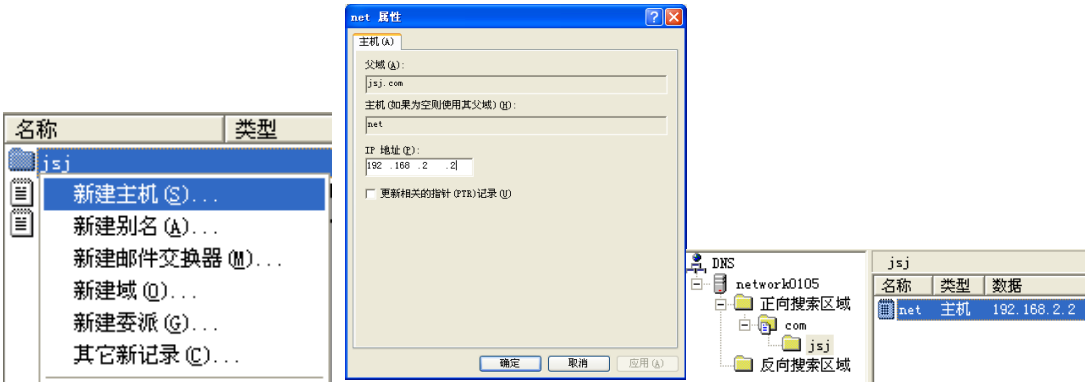


3．以上操作完成后的结果如下图所示

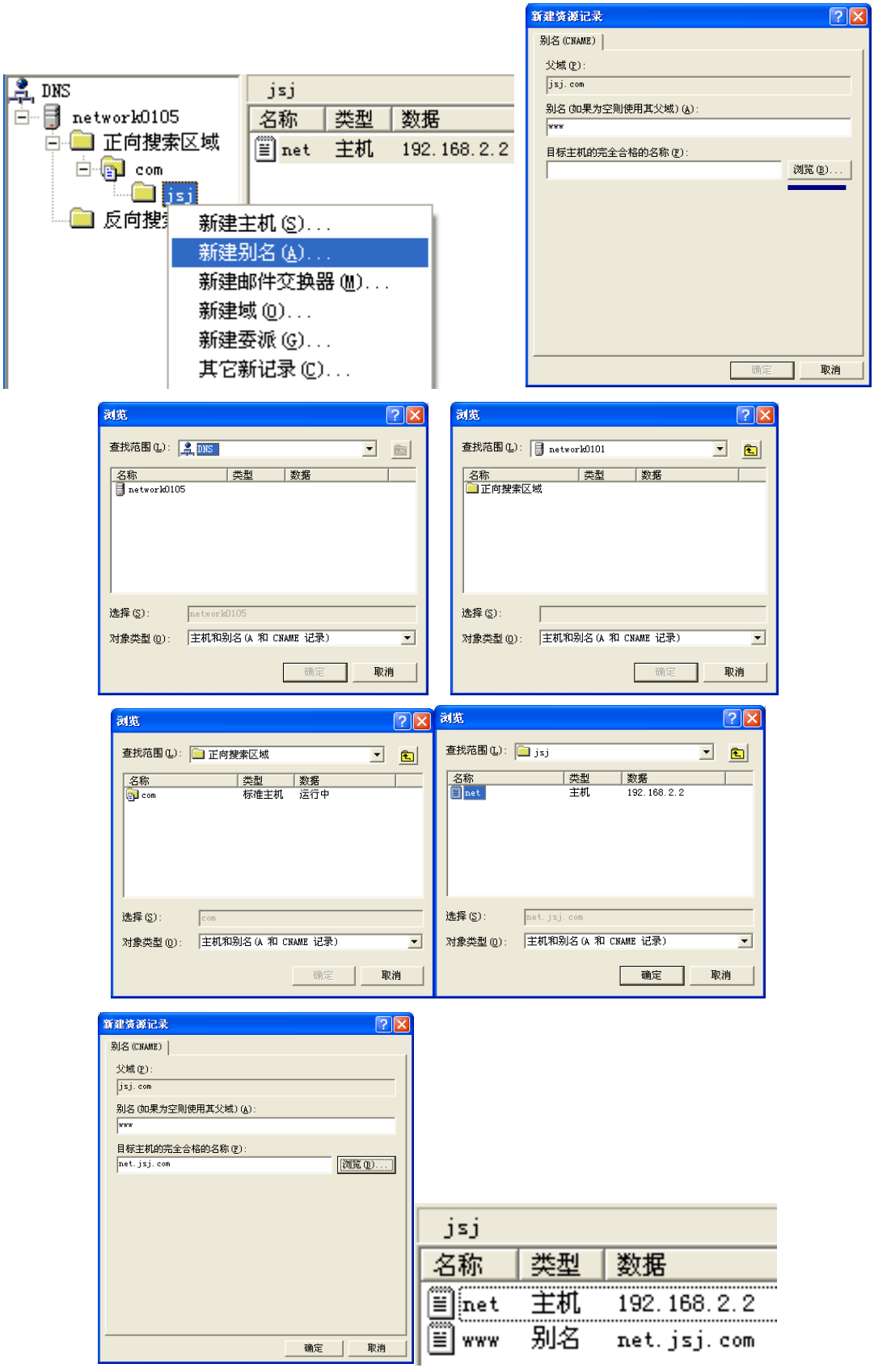
4．在“com”处单击右键，出现菜单，如下左图。选择“新建域”，出现如下中图。在名称处输入“jsj”，确定后，出现下右图。



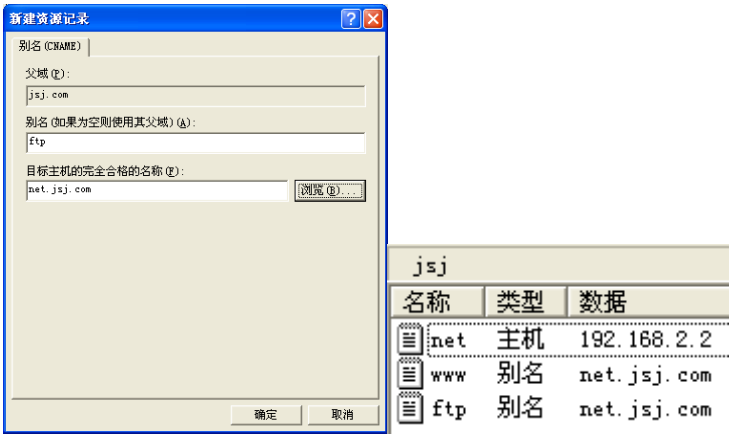
5．在如下左图中“jsj”处点右键，选新建主机，在中图中，输入“net”和 IP 地址处输入“当前使用的计算机的 IP 地址”。点“添加主机”，单击完成退出。



6．按下列步骤为该主机添加两个别名（www 和 ftp），步骤如下图。

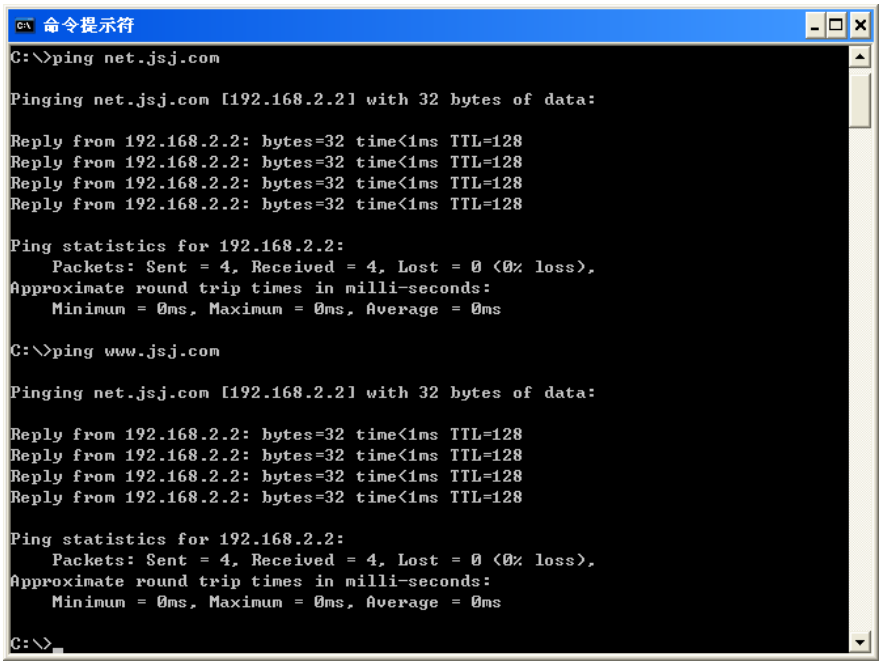


新建完成后如上图所示，接着按照相同的步骤新建另一个别名，完成后如下图所示。



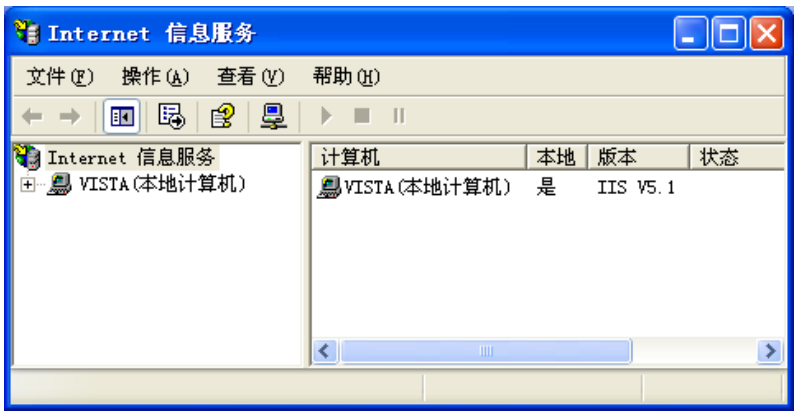
7．打开“控制面板----网络连接”，右键点本地连接，在 Internet 协议(TCP/IP)中修改 dns 设置，改成当前使用的计算机的 IP 地址并保存。

8．在 dos 窗口，执行 ping net.jsj.com、ping www.jsj.com 和 ftp.jsj.com，返回信息如下图，则表示配置正确。至此完成了 dns 的初步配置。



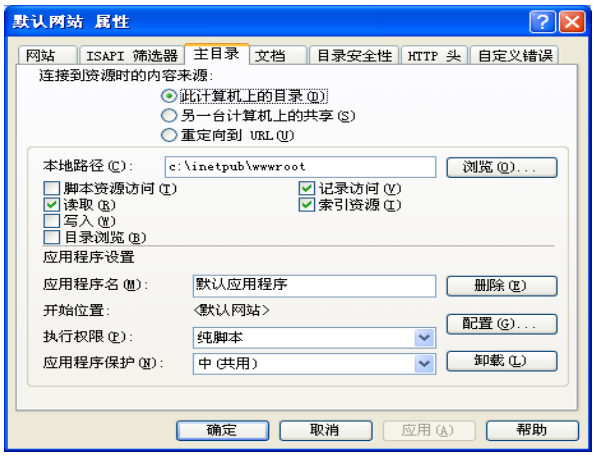
（三）、配制 www 和 ftp 服务器

1．在“控制面板----管理工具”中，打开“Internet 信息服务”，如下图



2．设置 www 服务的属性：展开目录，右键点“网站”下的“默认网站”，在出现的菜单中

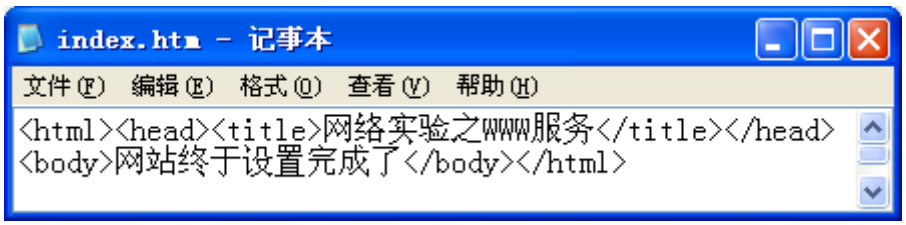
选择“属性”，出现如下图所示。在该窗口中可以控制用户访问时是否可以写入，是否可以读取。还可在文档标签下选择首页文件格式的读取顺序。本实验按照默认值进行，不需要作任何修改，关闭该窗口。



3．设置 ftp 服务的属性：右键单击“ftp 站点”下的“默认 ftp 站点”，选择“属性”，出现如下所示窗口。将主目录标签下的读取、写入、记录访问选中并保存。

（四）、验证 www 和 ftp 服务器

1．编辑一个简单的网页，命名为 index.htm，保存到“C:\Inetpub\wwwroot”下。文件命名为“index.htm”。



2．在 IE 浏览器地址栏输入 http://www.jsj.com 回车后，出现如下图所示。则 www 服务器安

装配置完成。

3．ftp 服务器验证，先从 windows 里复制一个文件到“C:\Inetpub\ftproot”下，打开浏览器，在地址栏输入“ftp://ftp.jsj.com”，出现内容后，再从资源管理器中复制一个文件，粘贴到 IE 窗口中。如下图，证明 ftp 服务器安装配置完成。

2．2．5 实验要求

完成本次实验后，通过查找资料，整理并总结架设 WWW 服务器、FTP 服务器、DNS 服务器可以使用的软件的种类和用法，了解并掌握三种服务器中的各种设置。

2．2．6 思考与讨论

1．通过 ping www.jsj.com 命令，说明 DNS 的作用。

2．如何控制 FTP 服务器的读写功能？

实验 3 以太网帧结构和 ARP 协议分析

一、以太网帧结构

3．1．1 实验目的

掌握以太网的帧结构，理解以太网帧中各字段的含义和作用。

3．1．2 实验环境

1．连网的 Windows XP 主机两台，PC1 安装有科来网络分析系统，PC2 安装 IIS。
2．实验分组：两名同学一组，轮换进行实验。

3．1．3 实验内容

用科来网络分析系统捕获并分析以太网的帧结构。

3．1．4 实验步骤

1．在 PC1 上删除本机的 ARP 表项。
2．在 PC1 上启动科来网络分析系统，开始捕获数据包。
3．立刻访问 PC2 的 Web 页面【利用实验三中建立的 WWW 服务器进行本实验】。
4．停止捕获。
5．分析捕获到的数据包。
（1）在捕获到的数据包中，找到每个数据包的数据帧，查看每个数据帧的首部各字段的内容并进行记录；
（2）根据所学的内容和每个数据帧首部字段的 MAC 地址信息，判断数据帧的方向；
（3）观察数据帧的大小，检查每个帧的大小是否符合协议要求。

3．1．5 实验要求

完成本次实验后，进一步掌握科来网络分析系统在网络分析中的作用和使用方法，理解并掌握了以太网帧结构、以太网帧中各字段的含义和作用，进一步了解并熟悉了科来网络分析系统的用法。

3．1．6 思考与讨论

1．查看捕获到的数据帧，目的地址为 PC2 的数据帧中长度最小的是多大？查看这种帧的各个域，查看先导域（前同步码）是否包括在记录的数据中？捕获到的数据帧从哪个字段开始，到哪个字段结束？是否包含帧校验序列？是否可以验证 EthernetV2 标准中规定的最小帧长为 64 字节？
2．查找捕获的帧中长度最长的帧。确定这些帧中最长的帧是多少字节？为什么？
3．找到捕获的数据帧中由 PC1 发出的 ARP 请求帧，辨认其目的地址域和源地址域，查看目的 MAC 地址是多少？用 IPconfig -all 命令查看 PC2 的 MAC 地址，看是否与该帧中的源地址一致？
4．对比封装 ARP 分组的帧和其他帧（封装 IP 分组的帧），它们的类型字段分别是多少？

二、ARP 协议分析

3．2．1 实验目的

掌握 ARP 命令的用法，理解 ARP 协议原理，理解 ARP 协议的分组格式。

3．2．2 实验环境

1．安装科来网络分析系统的连网的 Windows XP 主机两台。

2．实验分组：两名同学一组，轮流进行实验。

3．2．3 实验内容

用 ARP 命令查看本机 ARP 缓存中的内容，ARP 命令的参数的使用，捕获 ARP 分组，分析分组格式和首部各字段的含义。

3．2．4 实验步骤

1．观察 ARP 缓存表的内容

通过命令 arp –a 查看本机 ARP 缓存的内容，分析每个项目的含义。在命令窗口执行命令 ping 临机 IP，再观察 ARP 缓存的内容，理解 ARP 缓存的作用和生成过程。

2．观察 ARP 缓存生存时间

反复用命令 arp –a 查看 ARP 缓存，通过计时观察动态 ARP 缓存的生存时间。

3．观察本机 ARP 缓存生成过程

在命令行下用 arp –d 命令删除 PC1 上的所有 arp 表项，然后用 ping 临机 ip，用该命令来触发 arp 过程。通过科来网络分析系统捕获分组可以观察 arp 过程。此时在 PC1 和 PC2 上，在命令行下用 arp –a 命令即可观察到对方的 MAC 地址。根据观察到的现象理解 arp 过程。

4．观察 ARP 分组格式

启动科来网络分析系统，开始捕获，在命令窗口执行命令 ping 临机 ip，命令执行完成后，停止捕获，观察 ARP 分组的内容。

3．2．5 实验要求

完成本次实验后，整理 arp 命令的用法，各个参数的作用，进一步理解并掌握了 ARP 缓存的生成过程、ARP 缓存的含义、ARP 分组的格式以及首部字段的含义。

3．2．6 思考与讨论

1．实验过程观察到了动态 ARP 缓存经过一定时间自动删除，如何生成静态 ARP 缓存？

2．ARP 缓存中各个项目的含义是什么？类型字段的类型及含义分别是什么？

实验 4 ICMP 协议分析

4．1 实验目的

掌握 ICMP 协议的工作原理，理解 ICMP 分组结构。

4．2 实验环境

1．安装科来网络分析系统的连网的 Windows XP 主机两台。

2．实验分组：两名同学一组，轮流进行实验。

4．3 实验内容

用 ping 命令和科来网络分析系统分析 ICMP 包的基本结构以及回显请求与应答消息、目标不可达、超时等消息的 ICMP 报文的异同。

4．4 实验步骤

在两台 PC 机上启动科来网络分析系统，开始抓包。

1．回显请求及应答消息。

1）在 PC1 上运行命令：ping 临机 IP。

2）命令执行后，停止抓包，分析 ICMP 报文，查看报文结构和首部格式以及首部中各字段的内容。

3）说明 ICMP 报文首部各字段的含义以及所捕获的数据报属于什么报文。

4）对 PC2 上捕获到的包进行分析，说明 ICMP 报文首部各字段的含义以及所捕获的数据报属于什么报文。

2．超时消息。

1）在 PC1 上运行命令：ping 不存在的或者没有开机的计算机的 IP。

2）停止抓包，分析 ICMP 报文，查看报文结构和首部格式以及首部中各字段的内容。

3）说明 ICMP 报文首部各字段的含义以及所捕获的数据报属于什么报文。

4）对 PC2 上捕获到的包进行分析，说明 ICMP 报文首部各字段的含义以及所捕获的数据报属于什么报文。

3．端口不可达消息。

在 PC2 上启动 TFTP 服务器软件。

在 PC1 上启动科来网络分析系统，开始抓包。

在 PC1 的命令窗口运行命令：tftp –I PC2 的 IP get 文件名（该文件可能不存在）；停止抓包可以看到如图所示结果：

编号	绝对时间	源	目标	协议	大小	解码	概要
1	20:16:29.356739	192.168.0.9:3128	192.168.0.12:tftp	TFTP	64	编号=0...	读请求,文件: x.tzt,类型: octet
2	20:16:29.357710	192.168.0.12	192.168.0.9	ICMP	88	编号=0...	目标端口不可达
3	20:16:29.357776	192.168.0.9:3128	192.168.0.12:tftp	TFTP	64	编号=0...	读请求,文件: x.tzt,类型: octet
4	20:16:29.358632	192.168.0.12	192.168.0.9	ICMP	88	编号=0...	目标端口不可达
5	20:16:29.358671	192.168.0.9:3128	192.168.0.12:tftp	TFTP	64	编号=0...	读请求,文件: x.tzt,类型: octet
6	20:16:29.359508	192.168.0.12	192.168.0.9	ICMP	88	编号=0	目标端口不可达

ICMP - 因特网控制消息协议[ICMP - Internet Control Messages Protocol]: [34/8]

类型[Type]: 3 （目的不可达） [34/1]

代码[Code]: 3 （端口不可达） [35/1]

校验和[Checksum]: 0x7E8A （正确） [36/2]

图中显示 ICMP 报文首部中的类型为 3，表示目的不可达；代码为 3，表示端口不可达。

4．5 实验要求

完成本次实验后，通过查找资料，整理并总结 ICMP 报文的各字段的意义，ICMP 各种消息的作用，进一步掌握网络连通性的测试方法。

4．6 思考与讨论

1．通过查资料，请描述协议不可达报文的结构以及首部字段的含义。

2．总结 ICMP 类型与代码，简单描述其含义。

实验 5 IPv4 协议分析

一、IPv4 数据报首部

5．1．1 实验目的

掌握 IPv4 协议原理，理解 IPv4 分组首部结构及各字段的含义。

5．1．2 实验环境

1．连接外网的 Windows XP 主机一台，并安装有科来网络分析系统。
2．通过科来网络分析系统捕获一段时间内的 IPv4 分组。
3．实验分组：一名同学一组。

5．1．3 实验内容

1．用科来网络分析系统捕获数据包。
2．分析捕获到的 IP 数据包中首部各个字段的意义。

5．1．4 实验步骤

1．打开科来网络分析系统，开始捕获数据包。
2．用浏览器访问百度，用 ping 命令探测临机、网关和百度。
3．停止捕获，观察捕获到的数据包。
4．将访问百度以及 ping 临机、网关和百度的 IP 数据包首部中各字段的值记录在下表中，需要记录 IP 数据报的版本号、首部长度、总长度、标识、标志、片偏移、生存时间、上层协议、源地址和目的地址。

版本号	首部长度	总长度	标识	标志	片偏移	生存时间	上层协议	源地址	目的地址

5．比较所记录的各字段的值，理解首部字段的含义和作用。

5．1．5 实验要求

完成本次实验后，仔细观察所捕获的数据包，对网络层数据包首部的各字段进行整理，说明参数之间的关联性，进而加深理解网络层的工作过程。

5．1．6 思考与讨论

1．在连续捕获到的数据包中，IPv4 首部哪些字段的值是不变的？说明原因。
2．在连续捕获到的数据包中，IPv4 首部哪些字段的值是变化的？说明原因。

二、IPv4 数据报分段

5．2．1 实验目的

理解并掌握 IP 协议首部与分段有关的字段的含义和作用。

5．2．2 实验环境

1．软硬件环境：安装科来网络分析系统的连网的 Windows XP 主机一台。
2．实验分组：每名同学一组。

5．2．3 实验内容

用 PING 命令发送设置不分段的数据包，发送可分段数据包，捕获数据包，分析首部相关字段的内容，理解这些字段的含义和作用。

5．2．4 实验步骤

（一）、确认分段标志位
1．打开科来网络分析系统，开始捕获数据包。
2．在命令窗口执行 ping –f　www.baidu.com 命令，设置 DF 值为 1，即不分段。
3．停止捕获，观察捕获的数据包中 DF 字段的值。
（二）、IPv4 分段与重组
1．打开科来网络分析系统，开始捕获数据包。
2．在本机运行命令：“ping –l 3000 网关 IP”，向局域网网关发送较大的 ping 分组。
2．停止捕获后，分析捕获到的数据包，观察分组的分段与重组，记录如下内容：

1）应答分组的返回时间比起通常的 ping 应答要长一些，并且有可能刚开始几个 ping 请求会得不到应答，为什么？

2）在科来网络分析系统中可以看到每个 ping 请求都被分成了 3 个 IPv4 分段，将截图放到实验记录中，并回答下列问题。

（1）三个段的标识字段的值是多少？说明什么？

（2）片偏移字段的值依次是多少？是否可以确保在乱序到达时也能正确重组出原来的分组？

（3) 第一个分段的最后一个字母、第二个分段的第一个字母和最后一个字母、第三个分段中的第一个字母分别是什么？

5．2．5 实验要求

完成本次实验后，对捕获的数据包进行详细分析，重点分析网络层数据包首部中的标识、标志和片偏移字段的含义和作用。

5．2．6 思考与讨论

1. IP 分组被分段后，其对应的标识字段、标志字段和片偏移字段的值是什么？说明其含义。
2．什么情况下 IPv4 分组需要分段？分段和重组分别在哪一端进行？
3．三个分段的总的数据长度为 1500+1500+68-3*20=3008，比 ping 命令后面的参数 3000 多了 8，为什么？

三、IPv4 首部选项

5．3．1 实验目的

掌握 IPv4 协议原理，理解 IPv4 分组首部选项字段的含义。

5．3．2 实验环境

1．软硬件环境：连接外网的 Windows XP 主机一台，并安装有科来网络分析系统。

2．实验分组：每名同学一组，根据实验指导书进行实验。

5．3．3 实验内容

1．用科来网络分析系统捕获数据包。

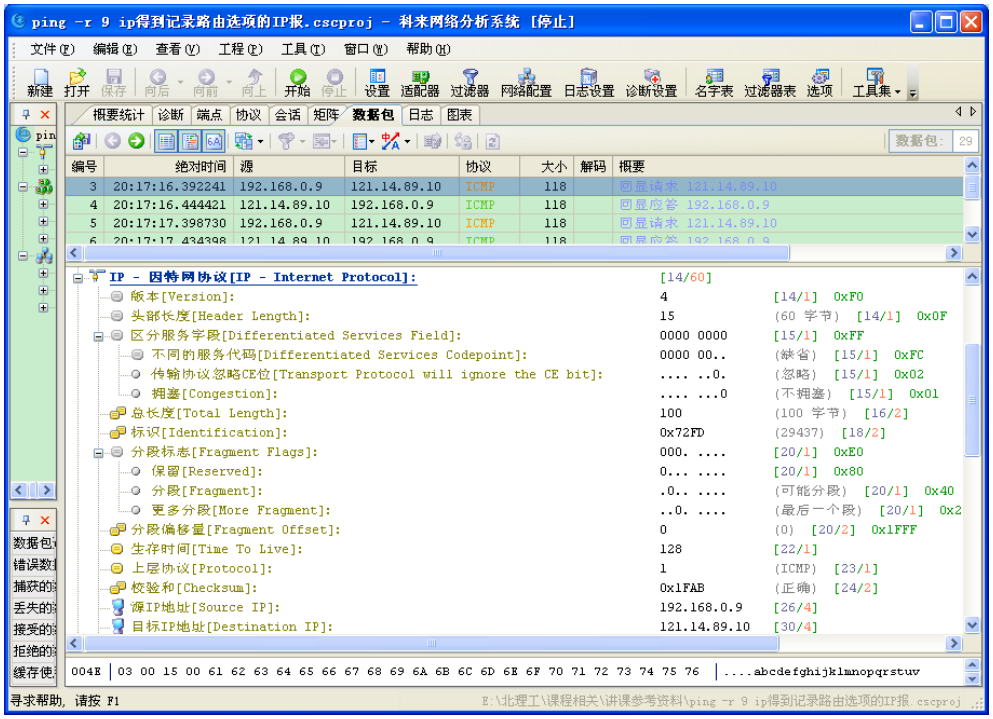
2．分析捕获到的 IP 数据包中首部选项字段的意义。

5．3．4 实验步骤

（一）、记录路由选项

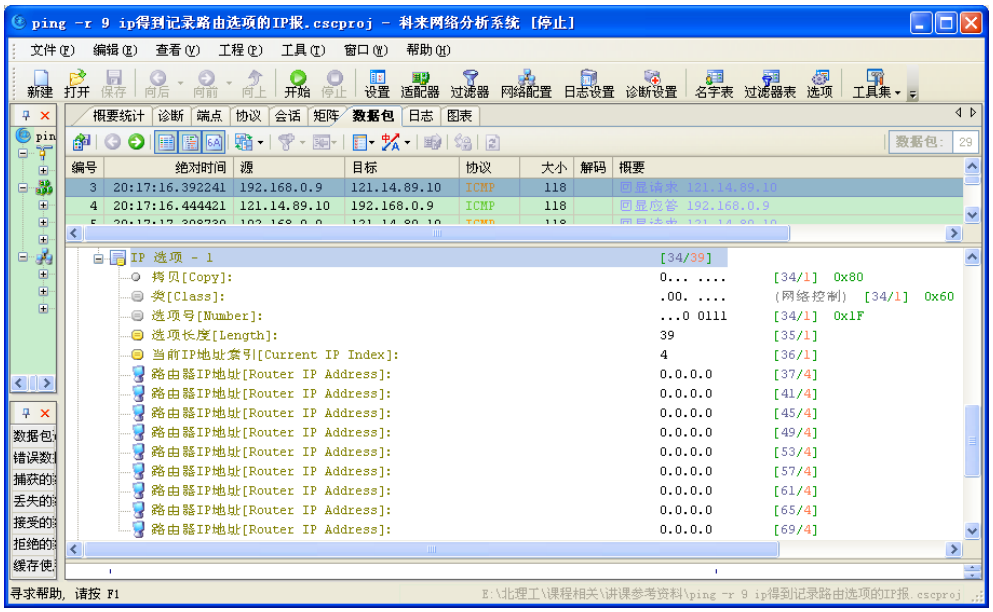
1．在本机运行科来网络分析系统并在 MS-DOS 窗口执行命令：“ping –r 9 远程 IP 地址”，向远方主机发送记录路径（9 跳）的 ping 分组。

2．停止捕获后，在科来网络分析系统中观察本机发出的第一个 ICMP 请求包中的 IP 首部各字段，如下图所示。



该图中，首部长度为 15，表示首部长度为 60 个字节，即包含了 40 个字节的选项字段。

3．停止捕获后，在科来网络分析系统中观察本机发出的第一个 ICMP 请求包中的 IP 首部的选项字段，如下图所示。



在上图中，可以看到路由器 IP 地址均为 0.0.0.0，说明该数据包还没有经过任何路由器，同样可以进一步说明这个一个请求包。

IPv4 首部选项的格式如下图

该图中，首部选项由 3 个部分组成：选项码、选项长度和选项数据。

选项码由 8 比特构成，分为复制位（COPY）、选项类和选项号 3 个子字段。

复制位占 1 比特，用于控制分片时是否将选项复制到各个分片个。复制位为“1”时，表示将原数据报所携带的选项复制到所有的分片中；复制位为“0”时，表示仅将选项复制到第一个分片中。

选项类占 2 个比特，用于定义选项的一般作用。

选项号占 5 个比特，用于定义选项的具体类型。

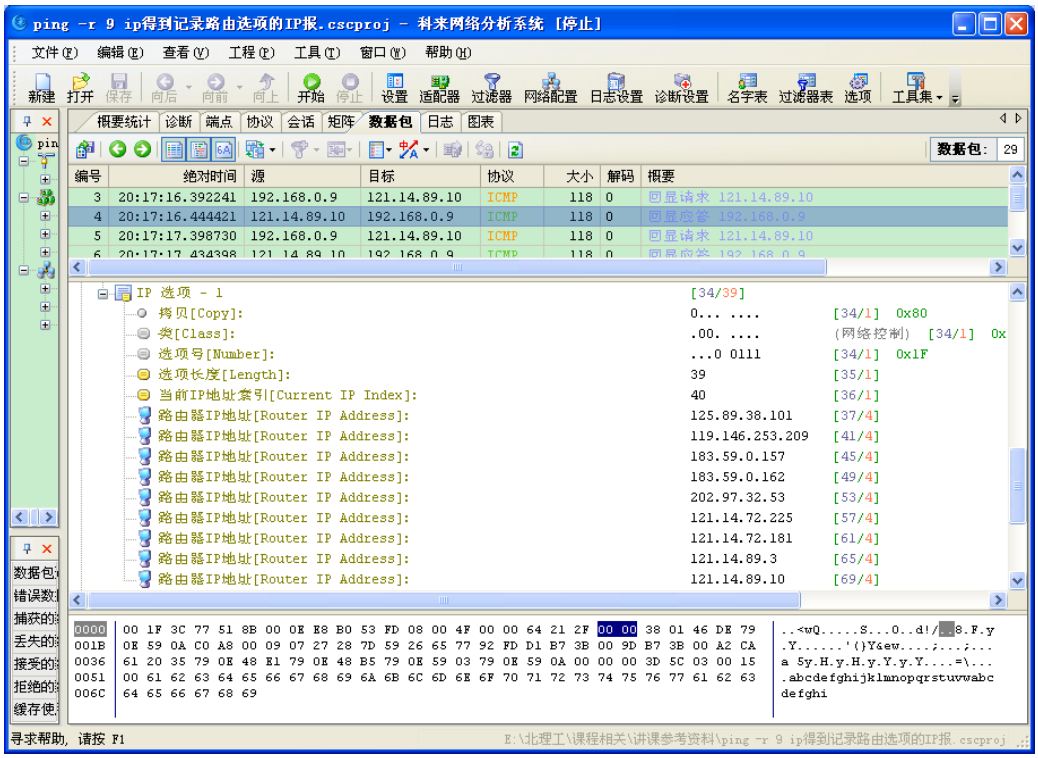
选项长度为一个字节，用于定义选项的长度。长度信息除了包含选项数据部分的长度外，还包括选项码和选项长度字段本身。

两比特的 IP 选项类定义了 4 种选项类型：00 用于 IP 数据报路径的控制和测试；10 用于时间戳的测试；01 类和 11 类未用。

每个选项类又由选项号进行细分，其中 00 类中常用的有 5 个选项号，10 类中只使用 1 个选项号。具体内容如下表。

选项类	选项号	选项长度（字节）	意义
00	00000	无	选项结束
00	00001	无	无操作（作为填充数据）
00	00011	变长	宽松源路由
00	00111	变长	记录路径
00	01001	变长	严格源路由
10	00100	变长	时间戳

4．在科来网络分析系统中观察本机收到的第一个 ICMP 应答包中的 IP 首部的选项字段，如下图所示。



在上图中，可以看到各个字段的参数值，其中记录了 9 条路由信息。

（二）、时间戳选项

时间戳选项用于记录 IP 数据报经过各路由器时的当地时间（采用世界时间），根据时间戳可以估算 IP 数据报从一个路由器到另一个路由器所花费的时间。

1．启动科来网络分析系统，开始捕获数据包。

2．在 MS-DOS 窗口执行命令 ping –s 4 121.14.89.10。

3．命令执行完成后，停止捕获，观察命令执行的结果和捕获的数据包。

5．3．5 实验要求

完成本次实验后，通过查找资料，整理并总结 IPv4 分组的首部选项字段所包含的内容，了解并熟悉选项字段的作用，特别是记录路由选项和时间戳选项的各个字段的意义和作用。

5．3．6 思考与讨论

1．记录并分析记录路由和时间戳操作中的 ping 请求和应答分组中，IPv4 选项的各个字段的值并说明其含义。

2．记录路由选项中的 len 值，该值表示可以记录多少条 IPv4 地址？

3．记录路由选项中，ping 应答分组与请求分组的不同之处在于分组经过路径上的路由器出口地址被记录下来了，应答分组的指针的值是多少？表示下一条记录是第几条记录？

实验 6 TCP 和 UDP 协议分析

一、TCP 的连接建立与释放

6．1．1 实验目的

掌握 TCP 协议建立连接与释放连接中首部的变化，深入理解 TCP 协议中的连接管理。

6．1．2 实验环境

1．一台安装 Windows XP 操作系统的连网计算机，并安装科来网络分析系统。

2．实验分组：一名同学一组，独自进行实验。

6．1．3 实验内容

用科来网络分析系统捕获数据包，观察 TCP 首部的变化，重点观察 SYN、ACK、FIN 位，同时观察源端口、目的端口、序号、确认号、数据偏移、窗口字段的变化。

6．1．4 实验步骤

1．观察连接建立

在计算机上启动科来网络分析系统开始捕获，用 Web 浏览器访问百度网站，页面出现后，稍等片刻，停止捕获，将数据记录在下表中，观察捕获到的数据，找出连接建立的数据包中关于 TCP 首部各字段的内容，分析连接建立过程中，某些字段的变化。

2．观察连接释放

在上述步骤所捕获的数据包中，查找连接释放的数据包，观察 TCP 首部中源端口号、目标端口号、序号、确认号、SYN、ACK、FIN 字段值的变化，分析连接释放过程中，相应字段的变化过程。需记录的项目如下表：

	编号	源端口号	目标端口号	序号	确认号	SYN	ACK	FIN	数据发送方向
连接建立									
连接释放									

6．1．5 实验要求

完成本次实验后，仔细分析所捕获的数据包，找出 TCP 连接建立和释放所涉及到的数据包，在观察和分析相关字段后，加深理解 TCP 的工作原理。

6．1．6 思考与讨论

1．TCP 连接建立和连接释放的标志是什么？

2．连接释放的过程有哪几种状态？每种状态代表什么情况？

二、TCP 可靠传输的实现

6．2．1 实验目的

理解并掌握利用 TCP 协议的窗口机制进行流量控制和拥塞控制的实现过程。

6．2．2 实验环境

1．一台安装 Windows XP 操作系统的连网计算机，并安装科来网络分析系统。

2．实验分组：一名同学一组，独自进行实验。

6．2．3 实验内容

用科来网络分析系统捕获数据包，观察 TCP 首部中窗口的变化，即双向进行的流量控制过程。

6．2．4 实验步骤

1．观察连接建立

在计算机上启动科来网络分析系统开始捕获，用 Web 浏览器访问百度网站，页面出现后，稍等片刻，停止捕获，观察捕获到的数据，找出连接建立的数据包中关于 TCP 首部各字段的内容，分析连接建立过程中，某些字段的变化。

2．观察源端口号、目的端口号、序号、确认号、数据偏移和窗口字段的变化过程

上述捕获的数据包中，逐一观察并记录每个数据包中的端口号、序号、确认号、数据偏移和窗口字段的值，将这些值记录在下表中，并验证 TCP 协议中序号和确认号的数值以及 TCP 的确认机制。需记录的项目如下表：

编号	源端口号	目标端口号	序号	确认号	偏移量	窗口	数据发送方向

根据上表，验证端口号的定义，验证序号和确认号的关系，说明偏移量的含义，说明窗口值的含义。

6．2．5 实验要求

完成本次实验后，通过仔细分析捕获的数据包，理解并掌握 TCP 首部各字段的含义和作用，可靠传输的实现机理，理解了端口号的含义和窗口的作用。

6．2．6 思考与讨论

1．TCP 首部中窗口的作用是什么？

2．TCP 保证可靠传输的机理是什么？

三、TCP 的选项

6．3．1 实验目的

理解并掌握 TCP 首部选项字段的种类、每种选项的作用，重点掌握最大报文段选项。

6．3．2 实验环境

1．安装科来网络分析系统的连网的 Windows XP 主机一台。
2．实验分组：一名同学一组。

6．3．3 实验内容

用科来网络分析系统捕获 TCP 报文段，查找包含选项字段的 TCP 报文段，观察选项字段的内容。

6．3．4 实验步骤

1．启动浏览器，清空缓存。
2．启动科来网络分析系统，开始捕获数据包。
3．在浏览器地址栏中输入 http://mail.163.com/，回车后可以看到邮箱页面。
4．停止捕获，在数据包窗口仔细观察所有捕获到的数据包，找出包含 TCP 选项字段的报文段，查看选项字段的内容。
5．用同样的方式访问百度，在捕获的数据包中观察 TCP 选项字段的内容。

6．3．5 实验要求

完成本次实验后，通过查找资料，整理并总结 TCP 选项字段的内容和含义，理解并掌握 TCP 选项字段的类型和作用，了解选项字段“最大报文段长度”的应用时机。

6．3．6 思考与讨论

1．指出在捕获到的数据包中哪些是具有选项字段的 TCP 报文段？
2．指出选项“最大报文段长度”的各个字段的含义以及在什么样的连接中使用该选项？
3．通过查找资料，整理出选项所有字段的内容。

四、UDP 协议分析

6．4．1 实验目的

掌握 UDP 协议原理，理解 UDP 报文格式。

6．4．2 实验环境

1．安装科来网络分析系统的连网的 Windows XP 主机一台。

2．实验分组：一名同学一组。

6．4．3 实验内容

用科来网络分析系统捕获 UDP 报文段，观察 UDP 报文段首部各字段的内容。

6．4．4 实验步骤

1．实验准备

打开浏览器，清空缓存，打开科来网络分析系统，开始捕获数据包，在命令窗口执行命令：ping www.baidu.com，命令执行完成后，停止捕获。

2．观察 UDP 分组

观察捕获到的 DNS 分组中的 UDP 协议的端口信息、总长度、检验码以及数据长度。

3．在捕获到的分组中，找出包含 UDP 协议的分组，比较不同分组中 UDP 的总长度字段，每个分组中的 UDP 总长度字段的值与 UDP 的数据部分的长度是否一致。

6．4．5 实验总结

完成本次实验后，整理捕获到的数据包中 UDP 首部的内容，理解并掌握 UDP 协议首部各字段的含义。

6．4．6 思考与讨论

1．DNS 通常情况下使用 UDP，在什么情况下会使用 TCP？

2．UDP 与 TCP 的区别是什么？

实验 7 HTTP 协议分析

一、HTTP 报文段首部

7．1．1 实验目的

掌握 HTTP 协议首部种类、格式、主要字段的含义。

7．1．2 实验环境

1．安装科来网络分析系统的连网的 Windows XP 主机一台。

2．实验分组：一名同学一组。

7．1．3 实验内容

用科来网络分析系统捕获 HTTP 报文段，观察几种常用 HTTP 报文段的格式和主要字段的含义。

7．1．4 实验步骤

1．实验准备

打开浏览器，清空缓存，打开科来网络分析系统，开始捕获数据包，在浏览器地址栏输入 www.baidu.com，页面显示完成后，停止捕获。

2．观察 HTTP 报文

观察捕获到的 HTTP 报文中的 HTTP 请求报文和 HTTP 应答报文。

3. 记录在 HTTP 请求报文和响应报文中各字段的名称和各字段的值，说明每个字段的含义。

7．1．5 实验要求

完成本次实验后，整理捕获到的数据包中关于 HTTP 首部各字段的内容，理解并掌握 HTTP 协议的请求报文段和响应报文段中各字段的含义和作用。

7．1．6 思考与讨论

1．通过实验和查资料，写出 HTTP 协议的请求报文和响应报文都包括哪些字段？各个字段的含义和作用是什么？

2．在捕获的 HTTP 请求报文和响应报文中，显示的 HTTP 版本号是多少？

二、HTTP 的高速缓存

7．2．1 实验目的

掌握 HTTP 高速缓存的作用，理解 HTTP 协议中与时间有关的字段的含义和作用。

7．2．2 实验环境

1．安装科来网络分析系统的连网的 Windows XP 主机一台，即 PC1。

2．主机 PC2 上配置 IIS【如果不安装 DNS，则在 PC1 上用 IP 地址访问 PC2 的 index.htm 文件】，在 PC2 的 WWW 主目录下建立一个 index.htm 文件并重新启动 IIS。在 PC1 上启动浏览器，将浏览器的缓存清空。

3．实验分组：两名同学一组，轮流实验。

7．2．3 实验内容

用科来网络分析系统捕获 HTTP 报文段，观察 HTTP 响应报文段中与时间有关的字段的内容、种类和作用。

7．2．4 实验步骤

1．在 PC1 上启动抓包软件，用浏览器访问 PC2 上的 index.htm 文件，停止抓包，将抓到的数据包保存成“第 1 次抓包”。

2．在 PC1 上启动抓包软件，用浏览器再访问一次 PC2 上的 index.htm 文件，停止抓包，将抓到的数据包保存成“第 2 次抓包”。

3．将 PC2 上的 index.htm 文件的内容进行修改并保存。

4．在 PC1 上启动抓包软件，用浏览器访问 PC2 上的 index.htm 文件，停止抓包，将抓到的数据报保存成“第 3 次抓包”。

5．根据第 1 次抓包、第 2 次抓包和第 3 次抓包的结果观察第一个 HTTP GET 请求报文段中的与时间有关系的字段。

7．2．5 实验要求

完成本次实验后，通过分析捕获的数据包，理解并掌握 HTTP 请求报文和响应报文中与时间有关系的字段的作用，加深理解本机高速缓存的工作过程及其作用。

7．2．6 思考与讨论

1．分析浏览器向服务器发出的请求报文中，是否有一行是 IF-MODIFIED-SINCE？

2．分析浏览器向服务器发出的第二个“HTTP GET”请求，在该请求报文中，是否有一行是 IF-MODIFIED-SINCE？如果有，在该行后面的信息是什么？

3．服务器对第二个 HTTP GET 请求的应答中的 HTTP 状态码是什么？服务器是否返回了文件的内容？

4. 第 3 次抓包的文件中，客户发出的 HTTP GET 请求报文段中是否有 IF-MODIFIED-SINCE 字段，如果有，该字段的内容是什么？

5．第 3 次抓包的文件中，服务器返回的报文段中是否有 LAST-MODIFIED 字段，如果有，该字段的内容是什么？

6. 根据上面的分析，问：三次访问过程中哪一次客户端没有从服务器上获取数据，为什么？除了第 1 次抓包以外，还有哪一次客户端从服务器获取数据了，为什么？

实验 8 综合实验

8．1 实验目的

掌握客户端刚刚启动，用浏览器访问 www 服务器，直到页面显示完成的整个过程种，计算机网络各个设备的各层协议所做的工作，进而掌握计算机网络的工作原理。

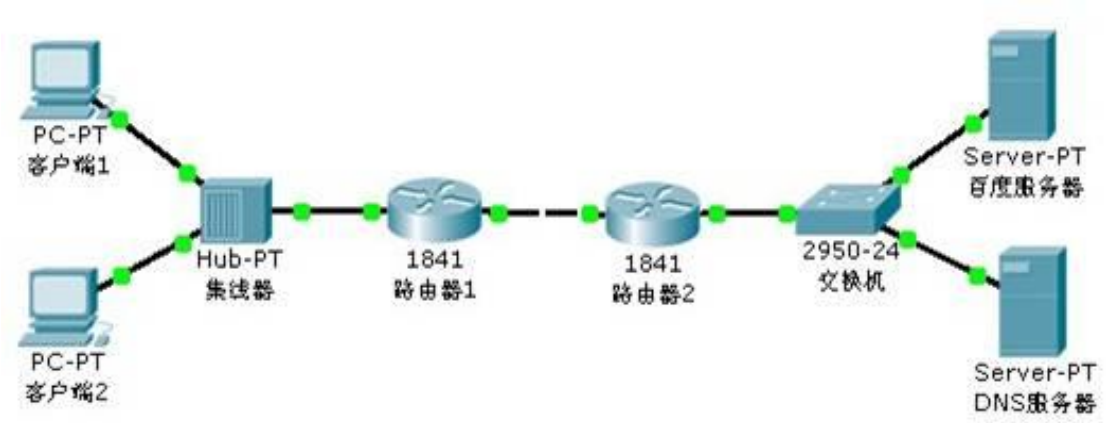
8．2 实验环境

1．安装科来网络分析系统的连网的 Windows XP 主机一台。

2．实验分组：一名同学一组。

8．3 实验内容及拓扑

完成从客户端访问服务器的整个过程的网络工作原理。



8．4 实验步骤

1．实验准备

打开浏览器，清空 DNS 缓存、浏览器缓存、ARP 缓存，打开科来网络分析系统，开始捕获数据包，在浏览器地址栏输入 www.baidu.com（上图中的百度服务器），页面显示完成后，停止捕获。

2．观察报文

观察捕获到的左右报文的内容。

3．详细描述整个访问过程，完成论文。

8．5 实验要求

完成本次实验后，按照毕业论文的格式要求，完成一个完整访问过程的论文。

8．6 思考与讨论

1．此处写出实验过程中遇到的问题和解决方案。

2．完成实验总结

（1）学到了 xx。

（2）实验中需要特别注意什么，有哪些细节和技巧。

（3）体会