计算机网络

实 验 指 南

计算机科学与工程学院

华南理工大学

2017年9月

# 目 录

[目 录 1](#_Toc493805799)

[实验一 网线制作 3](#_Toc493805800)

[1. 实验目的 3](#_Toc493805801)

[2. 实验器材及安排 3](#_Toc493805802)

[3. 实验步骤 3](#_Toc493805803)

[3.1任务与说明 3](#_Toc493805804)

[3.2直通线 4](#_Toc493805805)

[3.3交叉线 4](#_Toc493805806)

[3.3 RJ－45接头的制作步骤 5](#_Toc493805807)

[实验二 网络报文抓取与分析 7](#_Toc493805808)

[1．实验目的 7](#_Toc493805809)

[2．实验环境 7](#_Toc493805810)

[2.1 Wireshark介绍 7](#_Toc493805811)

[2.2 实验要求 7](#_Toc493805812)

[3．实验步骤 8](#_Toc493805813)

[3.1 wireshark的安装 8](#_Toc493805814)

[3.2 查看本机的网络适配器列表 8](#_Toc493805815)

[3.3 在指定网络适配器上进行监听 8](#_Toc493805816)

[3.4 记录一个TCP三次握手过程 9](#_Toc493805817)

[3.5 一个TCP握手不成功的例子 9](#_Toc493805818)

[3.6 侦听网络上的ARP包 10](#_Toc493805819)

[3.7 侦听网络上的ICMP包 10](#_Toc493805820)

[实验三 路由器及组网操作实验 12](#_Toc493805821)

[3.1 路由器的基本操作 12](#_Toc493805822)

[1． 实验目的 12](#_Toc493805823)

[2． 实验环境和要求 12](#_Toc493805824)

[3． 实验步骤 12](#_Toc493805825)

[4． 主要实验内容 13](#_Toc493805826)

[4.1 观察和验证类 13](#_Toc493805827)

[4.2 配置类 14](#_Toc493805828)

[3.2组网实验 16](#_Toc493805829)

[1. 实验目的 16](#_Toc493805830)

[2. 实验环境和要求 16](#_Toc493805831)

[2.1 实验拓扑 16](#_Toc493805832)

[2.2 实验要求 17](#_Toc493805833)

[3.实验步骤（参考） 17](#_Toc493805834)

[3.1 按实验图连接线路 17](#_Toc493805835)

[3.2 两个路由器的初始化配置 17](#_Toc493805836)

[3.3 路由配置 18](#_Toc493805837)

[实验四：网络Socket编程 21](#_Toc493805838)

[1. 实验目的 21](#_Toc493805839)

[2. 实验主要内容 21](#_Toc493805840)

[2.1 实验要求 21](#_Toc493805841)

[2.1 推荐参考书籍 21](#_Toc493805842)

[3. 实验环境要求 22](#_Toc493805843)

[4. 编程参考 22](#_Toc493805844)

[4.1套接字简介 22](#_Toc493805845)

[4.2 WinSock简介 29](#_Toc493805846)

[可选实验 交换机相关的实验 30](#_Toc493805847)

[1. 实验目的 30](#_Toc493805848)

[2. 实验设备 30](#_Toc493805849)

[3. 实验拓扑 30](#_Toc493805850)

[4. 主要实验内容 30](#_Toc493805851)

[4.1 交换机的基本配置 30](#_Toc493805852)

[4.2 VLAN间路由 33](#_Toc493805853)

[附录1：实验报告提交要求 35](#_Toc493805854)

[附录2：Packet Tracer简介 36](#_Toc493805855)

# 实验一 网线制作

## 1. 实验目的

（1）了解常用传输介质的性质。

（2）了解直通线和交叉线及其使用的情形。

（3）制作UTP直通线和交叉线。

（4）使用测试仪检查网线制作是否成功。

（5）通过网线制作熟悉相关工具和测试仪的使用。

## 2. 实验器材及安排

（1）每人网线一根，RJ-45连接器（水晶头）三个

（2）每组公用压线钳和测线仪

（3）考核方式：直连线、交叉线制作效果，实验报告（包括网线制作心得，实验后提交）

## 3. 实验步骤

### 3.1任务与说明

任务：根据下面表格的排线方法来做一条直通线和一条交叉线。

说明：为节约资源，本次实验每个同学只使用三个水晶头和一根网线。先做好一条直连线经检查合格后。剪去网线的一端，再做一根交叉线。即共用一次T568B线端。

线序标准：主要有T568A和T568B两个标准，如下表所示：

**引针号**

**T568A**

**T568B**

**1**

**2**

**3**

**4**

**5**

**6**

**7**

**8**

**白绿**

**绿**

**白橙**

**蓝**

**白蓝**

**橙**

**白棕**

**棕**

**白橙**

**橙**

**白绿**

**蓝**

**白蓝**

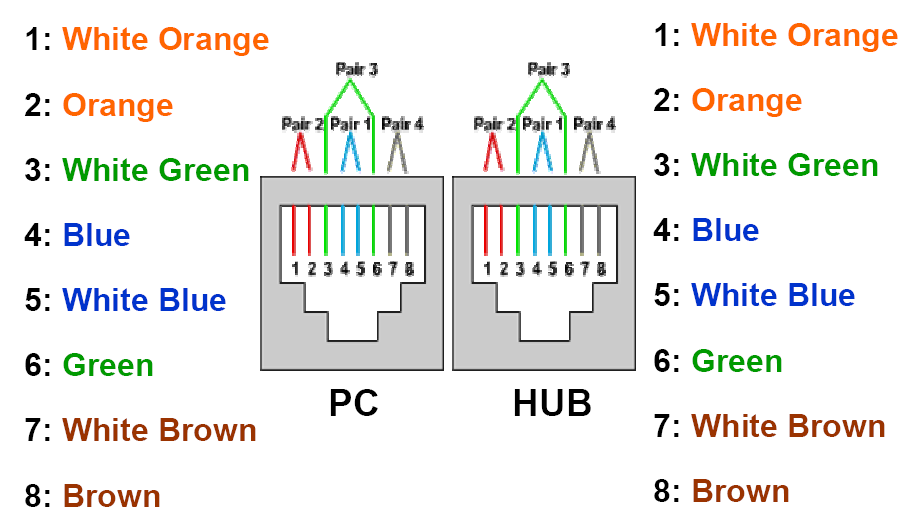
**绿**

**白棕**

**棕**

### 3.2直通线

制作一条T568－B的标准直通线，用于工作站和集线器(或交换机或路由器)之间的连接，即用于DTE和DCE之间的连接。如下图所示：



**直通线示意图**

说明：

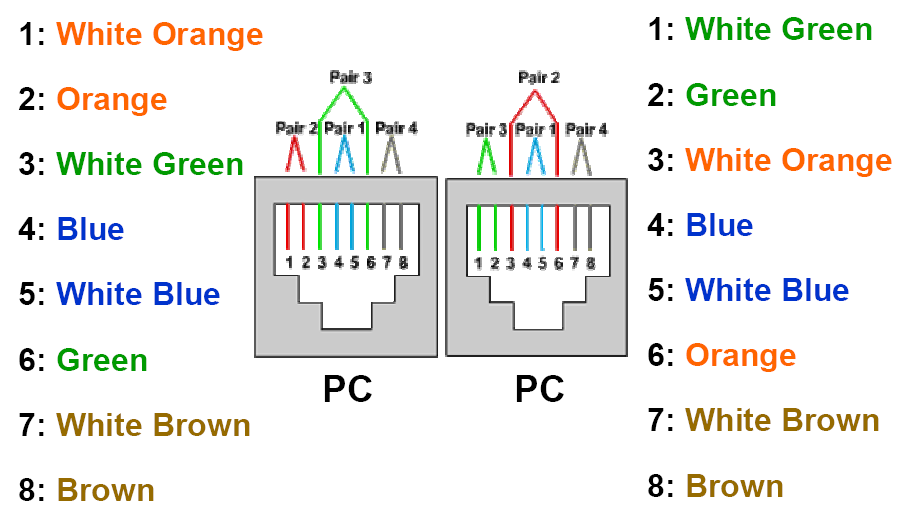
DTE：Data Terminal Equipment数据终端设备，产生或接收数据，通常是一些数据输入输出设备例：计算机、路由器、扫描仪、打印机等

DCE：Data Communication Equipment数据通信设备，数据电路终端设备，通常产生时钟。例：Modem、Hub 、Switch等

### 3.3交叉线

制作一条交叉线，用于两个集线器或交换机之间的连接，即用于DTE和DTE之间或DCE和DCE之间的连接。一头是T568A的接线标准，另一头是T568B的接线标准。

交叉线的制作应利用已经做好的直连线资源。制作的直连线通过检查并登记后，请剪去一端，另外一端保持不变。在剪去的一端制作一个T568A线序的接头。如下图所示：



**交叉线示意图**

### 3.3 RJ－45接头的制作步骤

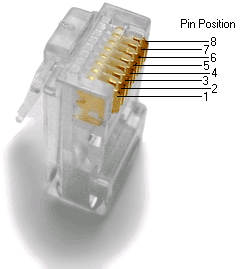
步骤1：清除末端线的外皮

将双绞线端头剪齐,再将双绞线端头伸入剥线钳刀口，使线头触及前挡板，然后适度握紧卡线钳同时慢慢旋转双绞线，让刀口划开双绞线的保护胶皮，取出端头从而剥下保护胶皮。双绞线的外皮除去3厘米左右，

步骤2：根据正确的颜色序列排好线的位置

按照T568B的线序标准对双绞线进行排序。（注意线要拉直，线序正确）。排好序后的线应该尽量笔直紧靠并在一个平面内。

注意，水晶头的编号方式如下：

****

**RJ-45 水晶头线序**

步骤3：用RJ-45压线工具将排完序的双绞线一次性剪断，长度控制在12mm左右。

目的是使得八根线的线端是齐平的，为下一步网线的插入作准备。

注意：在剪线之前就应该把用力捏紧八根线，以免线扭动而出现线端不齐平的现象，并且要保持紧捏直到到双绞线插入水晶头中。

步骤4：用将双绞线插入水晶头中

用劲往里推。线要插到底。同时应注意线与水晶头的PIN脚对应。完全插入后，外层绝缘套应伸入到水晶头内，这样做出来的网线才会结实、耐用。

步骤5：用压线钳用力压紧。（注意力度一定要足够）

要保证水晶头正确的放到了压线钳的槽中（压线钳的槽中突起的小铁片应该与水晶头外面的凹槽槽对应吻合，同时水晶头应顶到压线钳槽的底部）。放置好后可尽力往下压，（放置正确一般是很难把水晶头压坏的，但放置不正确则很容易压坏，应小心）

步骤6：测试

将网线的两端分别插入测试仪的两个接口，通过观察测试仪器上亮灯的顺序，测试网线是否连接正确。

步骤7：检查登记

制作好后的网线应该到指导老师处检查登记方能生效。

# 实验二 网络报文抓取与分析

## 1．实验目的

（1）、学习了解网络侦听

（2）、学习抓包工具wireshark的简单使用

（3）、对所侦听到的信息作初步分析

（4）、从侦听到的信息中分析TCP的握手过程，进行解释

（5）、分析了解TCP握手失败时的情况

## 2．实验环境

### 2.1 Wireshark介绍

Wireshark（前称Ethereal）是一个网络报文分析软件。网络报文分析软件的功能是抓取网络报文，并逐层显示报文中各字段取值。网络报文分析软件的功能可想像成 "电工技师使用电表来量测电流、电压、电阻" 的工作 - 只是将场景移植到网络上，并将电线替换成网络线。

网络报文分析软件曾经非常昂贵，Ethereal/wireshark 开源软件的出现改变了这种情况。在GNUGPL通用许可证的保障范围底下，使用者可以以免费的代价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/wireshark 是目前世界使用最广泛的网络报文分析软件之一。

### 2.2 实验要求

软件： Wireshark

硬件：上网的计算机

## 3．实验步骤

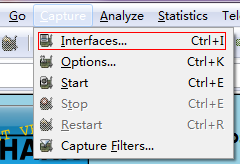
### 3.1 wireshark的安装

wireshark的二进制安装包可以在官网https://www.wireshark.org/download.html下载，或者可以在其他网站下载。

注意：下载后双击执行二进制安装包即可完成wireshark的安装。安装包里包含了WinPcap，并不需要单独安装WinPcap。

### 3.2 查看本机的网络适配器列表

**操作：**单击菜单Capture中的Interfaces选项



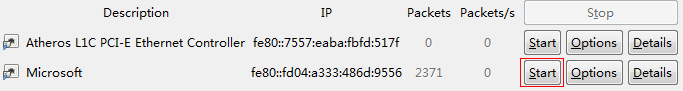
记录下你看到的信息，并回答问题：

（1）、你机器上的网络适配器有几个？

（2）、它们的编号分别是？

### 3.3 在指定网络适配器上进行监听

**操作：**在步骤3.2中弹出的Interfaces选项中，选择指定的网络适配器并单击start按钮



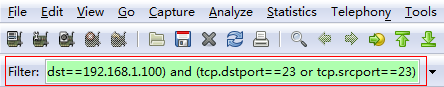
记录并解释wireshark监听的包内容（解释1条记录即可）

### 3.4 记录一个TCP三次握手过程

**操作：**在步骤3.3的基础上，单击start按钮后，打开命令行窗口并输入：telnet bbs.gznet.edu.cn，然后停止继续侦听网络信息。

在wireshark的Filter中输入表达式：

(ip.src==192.168.1.100 or ip.dst==192.168.1.100) and (tcp.dstport==23 or tcp.srcport==23)



其中192.168.1.100是你所在机器的IP，请自行根据自己机器的IP地址修改filter（可使用IPconfig查看）。telnet服务的传输层采用了tcp协议，并且其默认端口是23。

在wireshark窗口中，记下所显示的内容（可事先通过重定向的方式记录）并回答问题。

（1）根据得到的信息解释所键入的filter定制中的参数的含义？

（2）请从得到的信息中找出一个TCP 的握手过程。并用截图形式记录下来。

（3）结合得到的信息解释TCP 握手的过程。

### 3.5 一个TCP握手不成功的例子

**操作：**在步骤3.3的基础上，单击start按钮后，打开命令行窗口并输入：telnet 192.168.1.101，然后停止继续侦听网络信息。

在wireshark的Filter中输入表达式：

ip.src==192.168.1.100 or ip.dst==192.168.1.100 and (tcp.dstport==23 or tcp.srcport==23)

其中192.168.1.100是你所在机器的IP，telnet服务是tcp协议并且其默认端口是23。

上面的IP 192.168.1.101 可改为任何没有打开telnet 服务的IP。比如：可以用身边同学的IP。（注：此IP 的机器上要求没有打开telnet 服务，但要求机器是开的，否则将无法主动拒绝一个TCP 请求）

（1）试从得到的信息中找出一个TCP 的握手不成功的过程，并用截图记录下来

（2）并结合所得到的信息解释这个握手不成功的例子。

### 3.6 侦听网络上的ARP包

关于 ARP 的说明：IP 数据包常通过以太网发送。但以太网设备并不识别32 位IP 地址:它们是以48 位以太网地址传输以太网数据包的。因此，必须把IP 目的地址对应到以太网的MAC 地址。在这两种地址之间存在着某种静态的或算法的映射，常常需要查看一张表。地址解析协议(Address Resolution Protocol,ARP)就是用来确定这些映象的协议。

ARP 工作时,送出一个含有所希望的IP 地址的以太网广播数据包。目的地主机或另一个代表该主机的系统以一个含有IP 和以太网地址对的数据包作为应答。发送者将这个地址对高速缓存起来，以后再需要向这个IP 发送消息时，通过直接查表就可以得要这台主机对就的MAC 地址了。

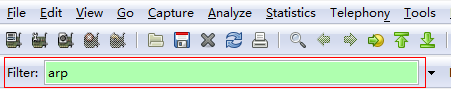
要看本机的 ARP 表（也即IP 与MAC 地址对应表）中的内容，只需在命令行方式下键入：arp –a命令即可。在下面的实验中，为了能够捕捉到ARP 消息，最好的做法是先将本机的ARP 表中的内容清空。这样当你使用Ping 命令时，它会首先使用arp 消息来查询IP 的MAC 地址。（当本地的ARP 表中有这个IP 对应的MAC 地址时，是不会再查询的）。要将本机的ARP 表中的内容清空，请使用命令：arp –d \*。关于ARP 更进一步的说明，请同学到网上查阅相关资料。

**操作：**在步骤3.3的基础上，单击start按钮后，打开命令行窗口并输入：

arp –d (清除ARP表)

ping 192.168.1.101 (Ping 任意一个和你的主机在同一个局域网的IP，说明:被Ping 的主机不能开防火墙）。

在wireshark的Filter中输入表达式：arp，然后就能会出现ARP 消息的记录。



请根据记录回答以下问题：

（1）记录下你所看到的信息，用截图形式。（找到ARP请求和ARP应答两个报文）

（2）请分析解释你的记录中的内容表示什么意思，从而说明ARP的工作原理。

### 3.7 侦听网络上的ICMP包

关于 ICMP 的说明：ICMP 是“Internet Control Message Protocol”（Internet 控制消息协议）的缩写。它是TCP/IP 协议族的一个子协议，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。

我们在网络中经常会使用到 ICMP 协议，只不过我们觉察不到而已。比如我们经常使用的用于检查网络通不通的Ping 命令，这个“Ping”的过程实际上就是ICMP 协议工作的过程。还有其他的网络命令如跟踪路由的Tracert 命令也是基于ICMP 协议的。另外，ICMP 消息也常常被用于作为网络攻击的手段。关于ICMP 更进一步的说明，请同学到网上查阅相关资料。

**操作：**在步骤3.3的基础上，单击start按钮后，打开命令行窗口并输入：

ping 192.168.1.101 (Ping 任意一个和你的主机在同一个局域网的IP,说明:被Ping 的主机不能开防火墙）。

在wireshark的Filter中输入表达式：icmp，然后就能会出现ICMP 消息的记录。

5

请根据记录回答以下问题：

（1）记录下你所看到的信息？（找到回声请求和回声应答两个报文）

（2）请分析解释一下你的记录中的内容，从而说明ping应用的原理。（提示：因为ICMP 报文是放在IP 报文中发送的，故wireshark侦听到的报文中有部分内容是属于ICMP 报文的，另有部分内容是属于IP 报文的，请注意加以区分）

# 实验三 路由器及组网操作实验

# 3.1 路由器的基本操作

## 1． 实验目的

（1）熟悉路由器的各种操作模式，包括用户模式、特权模式、全局配置模式、其它各种配置模式；

（2）掌握模式之前的转换方法，掌握帮助命令的使用；

（3）掌握show命令；

（4）掌握路由器的基本配置，包括名字、口令和接口等的配置；

（5）掌握单子网通达的方法。

## 2． 实验环境和要求

请大家在模拟器packet tracer上完成。

## 3． 实验步骤

步骤1. 观察路由器的面板和背板；

步骤2. 连接路由器和主机，注意使用的线缆和两端的插口；

步骤3. 启动路由器，观察路由器的指示灯变化；

步骤4. 启动主机的超级终端，逻辑连接路由器，进入CLI用户模式；

步骤5. 从该模式出发，开始各项试验。

## 4． 主要实验内容

### 4.1 观察和验证类

1. 你所用的路由器的型号是什么?
2. 路由器上Console口的作用是什么?(请查资料回答)
3. 控制终端(Console terminal,即你的个人电脑)连在哪一个口上?
4. 观察你所用的路由器（从玻璃窗观察机柜内路由器的接口），使用show interface命令，了解路由器上所有端口作用，完成以下表格。

（请填写路由器几个网络端口的作用）

|  |  |  |  |
| --- | --- | --- | --- |
| 路由器端口名称 | MTU | 状态 | 备注 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. 比较路由器在不同模式下的提示符。把正确的选项填入下表中：

|  |  |
| --- | --- |
| 模式种类 | 提示符 |
| 1. 用户模式（User EXEC Mode） |  |
| 2. 特权模式（Privileged EXEC Mode） |  |
| 3. 全局配置模式（Global configuration mode） |  |
| 4. 路由配置模式（Router configuration mode） |  |
| 5. 接口配置模式（Interface configuration mode） |  |

1. Router#
2. Router>
3. Router(config-if)#
4. Router(config-router)#
5. Router(config)#
6. 比较路由器在不同模式下的功能。把正确的选项填入下表中：

|  |  |
| --- | --- |
| 模式描述 | 主要功能 |
| 1. User EXEC Mode |  |
| 2. Privileged EXEC Mode |  |
| 3. Global configuration mode |  |
| 4. Router configuration mode |  |
| 5. Interface configuration mode |  |

1. 详细查看路由器的运行情况，对路由器进行调试、测试，
2. 设置IP地址和子网掩码
3. 运行简单的配置命令
4. 有限度地查看路由器的运行情况，可远程登录
5. 设置路由选择协议
6. 写出进入下列模式的命令：

|  |  |  |
| --- | --- | --- |
| 欲进入的模式 | 当前模式 | 命令 |
| Privileged EXEC Mode | Router > |  |
| Global Config Mode | Router # |  |
| Interface Config Mode | Router (config)# |  |
| Router Config Mode | Router (config)# |  |

1. 使用帮助命令：在路由器提示符下打入“？”获得帮助，并回答以下问题：

1.路由器回应了什么信息?            \_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. 运行其他show命令，回答以下问题：

**A. show clock**命令的作用是什么?

**B. show history**命令的作用是什么?

1. **show arp**命令的作用是什么?
2. **show running-config**命令的作用是什么?                 ，它的信息保存在哪里？                 。
3. **show startup-config**命令的作用是什么?                 ，它的信息保存在哪里？                 。
4. 键入show interface命令获得端口配置的统计信息。回答以下问题：

A. **找到**接口 fastEthernet 0/0 的如下信息:MTU的数值是多少？

B. **找到**接口 fastEthernet 0/0 的如下信息:带宽的数值是多少？

C. 除了fastethnet接口外，还有什么接口？

### 4.2 配置类

1）为路由器配置一个名字，并截屏。

**注意**：掌握hostname命令

2）为路由器的以太接口配置IPv4地址，是否生效？并将操作过程和生效验证截屏。（参考4.2.1的拓扑和配置步骤）

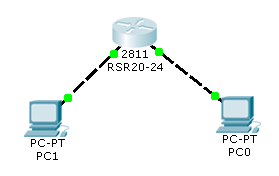
**注意**：掌握ip address 命令和show ip route命令。

**回答**：（1）PC1和PC2是否通达？为什么？

（2）为路由器的以太接口配置IPv4地址，是否生效？并将操作过程和生效验证截屏。

#### 4.2.1 IPv4单子网通达实验参考步骤

1. 绘制拓扑



1. 首先配置路由器，如下图所示：

Router(config)#interface fa0/0

Router(config-if)#ip address 192.168.6.254 255.255.255.0

Router(config-if)#no shutdown

Router(config)#interface fa0/1

Router(config-if)#ip address 192.168.7.254 255.255.255.0

Router(config-if)#no shutdown

注意：

(1)一定不要忘记使用“no shutdown”开启接口。

(2)完成了上述的配置和设置，PC和网关就能够互相ping通了。问：PC0和PC1是否能够 ping通？为什么？

# 3.2组网实验

## 1. 实验目的

路由器的基本使用和基本配置是本实验要达到的主要目标，本课程陆续开设的实验课，会对教材讲授到的基本原理进行验证，加深基本知识和基本技能的掌握。

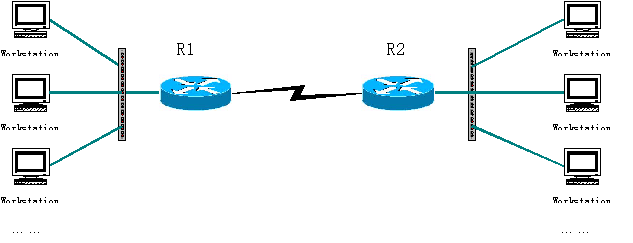
主要掌握以下路由器的基本操作：

1. 通过路由建立起网络之间的连接。
2. 熟悉路由器的基本操作命令，并掌握组网的基本技术。
3. 掌握静态路由的方法。
4. 掌握距离矢量路由协议中RIP的基本配置方法。
5. 掌握距离链路状态路由选择协议中OSPF的基本配置方法。

## 实验环境和要求

请大家在模拟器packet tracer上完成。

### 2.1 实验拓扑



### 2.2 实验要求

给定3个C类网络地址：192.168.6.0，192.168.7.0，192.168.8.0。

1. 请按实验网络拓扑作出网络规划。并写出路由器的端口地址和各节点网络地址。
2. 配置静态路由，使R1和R2两边的机器能够互相连通。
3. 配置动态路由，使R1和R2两边的机器能够互相连通。

## 3.实验步骤（参考）

### 3.1 按实验图连接线路



### 3.2 两个路由器的初始化配置

#### 3.2.1 R1配置

1. 登录路由器R1，进入普通用户模式 R1>
2. 键入enable 进入超级用户模式 R1#
3. 使用 configure terminal进入全局配置模式 R1(config)#

**配置FastEthernet 0/0 端口**

1. R1(config)#interface FastEthernet 0/0
2. R1(config-if)#ip address 192.168.6.254 255.255.255.0
3. R1(config-if)#no shutdown

**配置FastEthernet 0/1 端口**

1. R1(config)#interface FastEthernet 0/1
2. R1(config-if)#ip address 192.168.7.5 255.255.255.252
3. R1(config-if)#no shutdown

#### 3.2.2 R2配置

参看R1配置方法进入全局配置模式 R2(config)#

**配置FastEthernet 0/0 端口**

1. R2(config)#interface FastEthernet 0/0
2. R2(config-if)#ip address 192.168.8.254 255.255.255.0
3. R2(config-if)#no shutdown

**配置FastEthernet 0/1端口**

1. R2(config)#interface FastEthernet 0/1
2. R2(config-if)#ip address 192.168.7.6 255.255.255.252
3. R2(config-if)#no shutdown

**效果：**此时两路由器的端口都应是UP，并两路由器的FastEthernet 0/1端口能ping 通，FastEthernet 0/0端口和下接的本网段主机能ping通，但两网段的主机还不通，无法互访。

### 3.3 路由配置

#### 3.3.1 静态路由配置

**R1 配置：**

1. 进入全局配置模式 R1(config)#
2. R1(config)#ip route 192.168.8.0 255.255.255.0 192.168.7.6

**R2 配置：**

1. 进入全局配置模式 R1(config)#
2. R2(config)#ip route 192.168.6.0 255.255.255.0 192.168.7.5

**效果：**此时，两边主机都能ping通，并可以正常互访。

**在路由器R1上删除静态路由：**

R1(config)#no ip route 192.168.3.0 255.255.255.0 192.168. 7.6

**在路由器R2上删除静态路由：**

R2(config)#no ip route 192.168.1.0 255.255.255.0 192.168. 7.5

#### 3.3.2 动态路由配置

#### RIP

参看前面的配置方法进入全局配置模式

**R1配置**

1. R1(config)#router rip （启动RIP路由协议）
2. R1(config-router)#network 192.168.6.0 （指定192.168.6.0 可接受RIP信息）
3. R1(config-router)#network 192.168.7.0 （指定192.168.7.0 可接受RIP信息）

**R2配置**

1. R2(config)#router rip （启动RIP路由协议）
2. R2(config-router)#network 192.168.7.0 （指定192.168.7.0 可接受RIP信息）
3. R2(config-router)#network 192.168.8.0 （指定192.168.8.0 可接受RIP信息）

**效果：**此时两网段任意主机都能互访，在全局配置模式下用show ip route 命令，可看到路由标识是以R开头。在R1添加网段192.168.4.0，在R2则可看到此网段的路由。

**删除在R1中的RIP：**

R1(config)#no router rip

**删除在R2中的RIP：**

R2(config)#no router rip

#### OSPF

参看前面的配置方法进入全局配置模式

**R1配置**

1. R1(config)# router ospf 10 （启动 ospf 路由协议）
2. R1(config-roueter)# network 192.168.6.0 0.0.0.255 area 0 （指定连接的网络）
3. R1(config-roueter)# network 192.168.7.0 0.0.0.255 area 0 （指定连接的网络）

**R2配置**

1. R1(config)#router ospf 100 （启动 ospf 路由协议）
2. R1(config-roueter)# network 192.168.7.0 0.0.0.255 area 0 （指定连接的网络）
3. R1(config-roueter)# network 192.168.8.0 0.0.0.255 area 0 （指定连接的网络）

**效果：**此时两网段任意主机都能互访。

**删除在R1中的OSPF：**

R1(config)#no router ospf 10

**删除在R2中的OSPF：**

R2(config)#no router ospf ,100

**问题：**配置后的路由选择协议是否正常工作，请使用一种方法检查，并给出检查的结果，截图在这里。

实验四：网络Socket编程

## 1. 实验目的

（1）掌握Socket网络编程的基本原理和方法。

（2）深刻理解Socket的底层运作原理。

（3）通过实践加深对计算机网络体系结构和运行机制的理解。

（4）提高编程和分析问题，解决问题的能力。

## 2. 实验主要内容

### 2.1 实验要求

1. 基本要求：实现一个FTP协议的客户端和服务端，完成基本的文件传输功能。
2. 提交的内容：文档报告（包括设计文档，使用说明）， 源代码，可执行程序，以上内容分成三个文件夹存放（分别是Doc、Src、bin），再统一打包提交到教学在线。
3. 建议附加功能（可酌情获得加分，有附加功能的FTP可以分组进行，最多不超过3人）
   * 多客户端访问。
   * 在获取文件之前能够先得到文件列表。
   * 有兴趣的同学可以提交其它的作品，但作品必须基于底层的Socket(具体见实验要求)，不能使用高层封装的Socket（如Java类库，MFC等）。

### 2.1 推荐参考书籍

《UNIX网络编程》

《UNIX环境高级编程》

《TCP/IP网络互联技术 卷III （winsock版 ）》

《WINDOWS网络编程》

## 3. 实验环境要求

（1）实验平台：Linux或Windows均可

（2）开发语言：C或C++

（3）开发环境：不限，如Visual C++, .NET, Vi等

重要要求：为了让同学们更好的理解Socket的底层运作原理，Linux平台下只能使用底层库socket(socket.h)，Windows平台下只能使用Winsock(winsock.h)，请勿使用其它高层封装的Socket库（如Java库，MFC等）。

## 编程参考

### 4.1套接字简介

（1）网络应用程序编程接口(API)

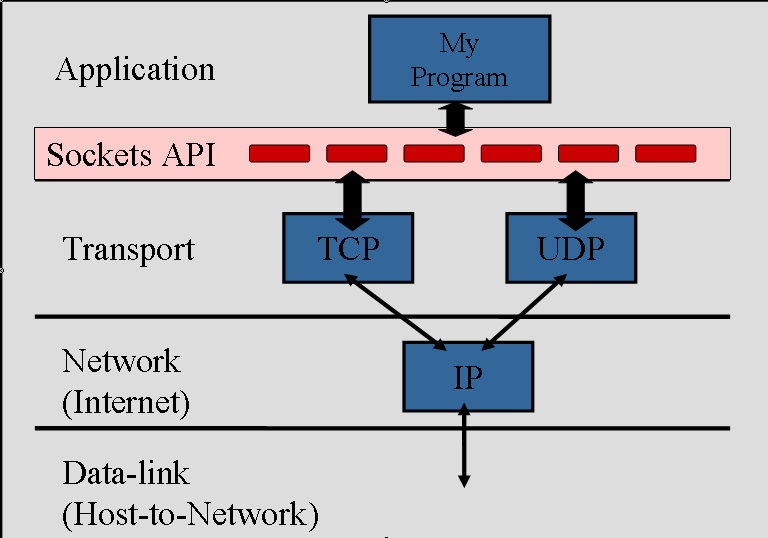
计算机用它来对网络发送或接收信息。

（2）套接字接口（socket interface）

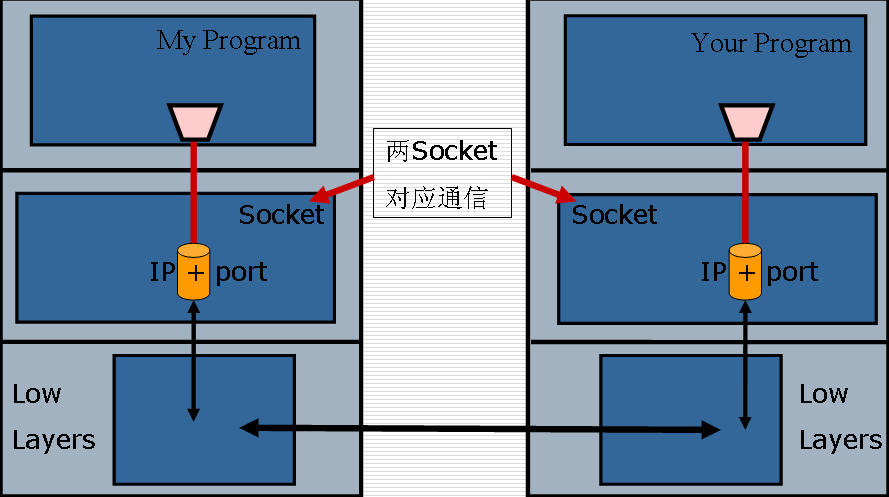
由加州大学伯克利分校UNIX小组开发，目前最为流行。定义了网络上的各种操作（如生成套接字，发送/接收消息等。

（3）常用的套接字接口

* Linux/Unix下： Berkeley Socket是最突出的一套接口。
* Windows下： Win Socket ，也称winsock，与Berkeley Socket很类似的接口

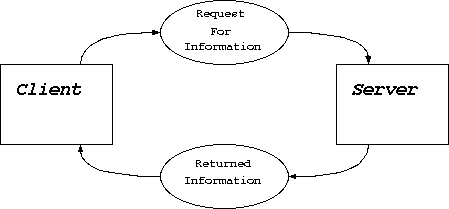


可认为一个IP与一端口（port）联合在一起形成一个套接字，它是网络上的一个传输接口。在网络的另外一端可有一个对应的套接字与通信。



#### 4.1.1 客户/服务器模式

TCP/IP网络应用中，最常用的通信模式是客户/服务器模式(Client/Server model)，即客户向服务器发出服务请求，服务器接收到请求后，提供相应的服务。

****

客户端与服务器的连接方式主要有两种：

* 流式套接口连接

流式套接口是可靠的双向通讯的数据流。传送的包会按发送时的顺序到达。

* 数据报套接口连接

使用这种方式，传送的包不一定会按发送时的顺序到达。当然每个包的内部是无错误的。

（1）服务器端

* + 服务器先要端打开一个通信通道，并告知本地主机它需要在某个端口上（如FTP为21）接收客户请求；
  + 等待客户请求到达该端口；
  + 接收到服务请求，处理该请求并应答。直至交互完成；
  + 返回第二步，等待另一客户请求；
  + 关闭服务器。

（2）客户端

* + 打开一个通信通道，连接到服务器所在主机的特定端口，此时，服务器端已经在这个Socket等待请求；
  + 向服务器发服务请求报文，等待并接收应答；
  + 继续提出请求并等待应答；
  + 请求结束后关闭通信通道并终止。

从上面所描述过程可知：

* 客户与服务器进程的作用是非对称的，它们各自完成的功能不同，因此编码也不同。
* 服务进程一般是先于客户请求而启动的，启动后即在相应的Socket监听来自客户端的请求。只要系统运行，该服务进程一直存在，直到正常或强迫终止。

服务器方面初始时需要执行的操作：

int socket () 建立一个Socket

int bind() 与某个端口绑定

int listen() 开始监听端口

int accept() 等待/接受客户端的连接请

客户端需要执行的操作：

int socket () 建立一个Socket

int connect() 连接到服务器



#### 4.1.2 使用伯克利套接字

（1）int socket (int domain, int type, int protocol)

功能：创建套接字。

返回值：返回值是新创建套接字的句柄，即以后引用该套接字时使用的标识符。错误时返回-1。

参数 domain 描述将使用的协议族。

AF\_INET ： 用于表示因特网协议族。

AF\_UNIX ： 用于表示U n i x 管道功能

参数 type表明通信的语义。

SOCK\_STREAM： 字节流服务，可理解为TCP连接

SOCK\_DGRAM： 面向消息的服务，可理解为TCP连接

参数 protocol 则指明将要用到的特定协议

IPPROTO\_TCP： 指的是使用TCP协议

（2）int bind(int socket, struct socketaddr \*address, int addr\_len)

功能：将创建的 socket 与 adress （包含 IP和port信息）绑定。

返回值：在错误的时候会返回-1

参数 socket 描述将使用的套接字。

参数 addr\_len 描述的是参数 adress的长度。

参数 adress 描述将绑定的地址。

参数中用到的数据结构：

struct socketaddr：在因特网协议中地址描述使用的数据结构

struct sockaddr {

unsigned short sa\_family;

char sa\_data[14];

};

sa\_family 描述将使用的协议族，一般为AF\_INET

sa\_data 为套接口储存目标地址和端口信息。

**注意：** 有两种字节排列顺序：重要的字节在前面，或者不重要的字节在前面。前一种叫“网络字节顺序 (Network Byte Order)”。不同机器，不同语言之间的字节存放顺序是不一样的，所以在网络上传输数据时，一定要转成网络字节顺序 。

数据必须按照 NBO 顺序，那么你要调用函数(例如 htons() )来将他从“本机字节顺序 (Host Byte Order) ”转换过来。

有以下四个主要的转换函数：

htons() 将Short型数据转换为网络字节类型

htonl() 将Long型数据转换为网络字节类型

ntohs() 将Short型数据转换为本地字节类型

ntohl() 将Long型数据转换为本地字节类型

事实上，上面的struct sockaddr并不好用，因它没有明确细化内部结构。于是程序员创造了一个并列的结构sockaddr\_in ，它可以与结构sockaddr互相转换。

struct sockaddr\_in {

short int sin\_family;

unsigned short int sin\_port;

struct in\_addr sin\_addr;

unsigned char sin\_zero[8];

}

首先，你需要将 IP 地址储存到 struct sockaddr\_in ina中。

当IP地址的形式是“numbers-and-dots”时(如“32.41.5.10”)，你要用的函数是 inet\_addr()：

ina.sin\_addr.s\_addr = inet\_addr(“132.241.5.10”);

注意：inet\_addr() 返回的地址已经是按照网络字节顺序的，你没有必要再去调用 htonl()。

当IP地址的形式已经是long时，则你需要使用htonl()函数来进行转换。

（3）int listen(int socket, int backlog)

功能：定义在指定的 Socket 上可有多少个待处理的连接。

返回值：在发生错误时返回-1。

参数socket 是调用 socket() 返回的套接口文件描述符。

参数backlog 是 在进入队列中允许的连接数目。

（4）int accept(int socket, struct socketaddr \*address

, int addr\_len)

功能：接收客户端连接请求。

返回值：如果连接成功， 函数将返回一个新的套接口文件描述符。接下来，就可以对这个描述符进行发送 (send()) 和接收 (recv()) 操作了。错误时返回-1

参数socket 套接口文件描述符。

参数address struct sockaddr\_in 的指针。

参数addrlen 长度，常为 sizeof(struct sockaddr\_in)

（5）int connect(int socket, struct sockaddr \*serv\_addr, int addrlen)

功能：在客户端被用于连接到服务器。

返回值：发生错误的时候返回-1

参数socket 套接口文件描述符。

参数serv\_addr 包含是服务器的地址和端口信息

参数addrlen 长度，常为 sizeof(struct sockaddr\_in)

（6）int setsockopt(int socket,int level,int optname

　,const void \*optval,socklen\_t \*optlen)

功能：设置套接字行为

参数level 指定控制套接字的层次。

SOL\_SOCKET表示通用套接字选项.

参数optname 指定控制的方式(选项的名称)　  
 SO\_REUSERADDR表示重用本地地址和端口

参数optval 指示相应的行为，如功能的开启或关闭

（7） 其它函数：

int read(int filedes, char \*buff, unsigned nbytes);

int write(int filedes, char \*buff, unsigned nbytes);

功能：分别表示对指定的文件描述符进行读定操作

返回值：读定成功时，返回一个表示读出/写入字节数的正数。

返回0表示文件尾，-1表示读/写失败。

int close(int socket);

功能：关闭对应的套接口。

struct  hostent gethostbyname(const char \*hostname);

功能：据主机名查找主机的IP 。 Hostname是域名。

返回值：成功时返回一个指向结构体 hostent 的指针

或者是空 (NULL) 指针

void \*memset(void \*s, char ch, unsigned n);

功能：将已开辟内存空间 s 的首 n 个字节的值设为值 ch

void \*memcpy(void \*destin, void \*source, unsigned n);

从源source中拷贝n个字节到目标destin中

int open(char \*pathname, int access[, int permiss]);   
 打开一个文件用于读或写  
 void exit(int status);  
 退出程序

### 4.2 WinSock简介

（1）概述

Windows Socket 是从 Berkeley Socket扩展而来的，其在继承 Berkeley Socket的基础上，又进行了新的扩充。这些扩充主要是提供了一些异步函数，并增加了符合Windows消息驱动特性的网络事件异步选择机制。

Windows socket的版本：

* Winsock1.1
* Winsock2.0

（2）Windows Socket 与 Berkeley Socket的异同

Win socket保持了与Berkeley Socket的最大程度的兼容。

Berkeley Socket下的大部分的函数在Win socket均有同名的函数，而且调用也基本上是一样的，但Win socket对某些函数进行了扩展，但命名时会加前缀来区别。

windows中需要先使用WSAStartup()函数来初始化Socket才能使用，并且需要使用SACleanup( )函数来关闭。而Linux中则不需要。

（3）Window下其它的Socket

CSocket (MFC)

CSocket封装了使用socket时的所有细节，包括网络字节顺序，主机名解析和地址族等。所以，使用它相对直接使用Winsock要简单一些。当然，涉及底层的操作时，则灵活性不一定有Winsock好。

# 可选实验 交换机相关的实验

## 1. 实验目的

本实验利用交换机创建虚拟局域网VLAN，并为VLAN分配成员，还利用路由器完成VLAN间的通信，通过本实验加深对VLAN基=基本原理和配置的理解。

主要掌握以下基本操作：

1. 创建两个VLAN，并验证配置结果。
2. 为每个VLAN命名，并分配交换机成员端口给他们。
3. 进行删除VLAN的操作，理解VLAN 1为什么不能被删除。

## 2. 实验设备

请大家在模拟器packet tracer上完成。

## 3. 实验拓扑



请按照上述图连接好路由器、交换机和主机。

## 4. 主要实验内容

### 4.1 交换机的基本配置

**步骤1：查看交换机配置状态**

1. 查看IOS的版本

在交换机的特权模式下键入show version，如下：

Switch#show version

1. 显示当前交换机vlan 接口信息

在交换机的特权模式下键入show vlan，如下：

Switch#show vlan

1. 显示当前交换机的配置信息

在交换机的特权模式下键入show running-config，如下：

Switch#show running-config

**步骤2：创建新的VLAN**

产生并命名两个新的VLAN，键入如下命令产生两个VLAN：

Switch#vlan database

Switch(vlan)#vlan 2 name VLAN2

Switch(vlan)#vlan 3 name VLAN3

Switch(vlan)#exit

**步骤3：为新创建的VLAN分配端口（成员）**

分配端口给VLAN时必须在接口配置模式（interface mode）下进行。输入如下命令，它们完成的主要功能是 。

Switch#config terminal

Switch(config)#interface Ethernet 0/2

Switch(config-if)#switchport access vlan 2

Switch(config-if)#interface Ethernet 0/3

Switch(config-if)#switchport access vlan 2

Switch(config-if)#interface Ethernet 0/6

Switch(config-if)#switchport access vlan 3

Switch(config-if)#interface Ethernet 0/7

Switch(config-if)#switchport access vlan 3

**步骤4：测试VLAN**

1. 在连接0/2的主机上ping 连接端口0/1的主机；

ping 成功了吗? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

为什么? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. 在连接0/2的主机上ping 连接端口0/3的主机；

ping 成功了吗? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

为什么? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. 在连接0/2的主机上ping 连接端口0/6的主机；

ping 成功了吗? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

为什么? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**步骤5：从VLAN中除去一个主机**

使用 no switchport 格式的命令在端口配置模式下进行配置，如下：

Switch#config terminal

Switch(config)#interface fastethernet 0/2

Switch(config-if)#no switchport access vlan 2

验证配置结果：（特权模式下 show vlan 命令）

问：端口0/2 还是VLAN 2的成员吗? \_\_\_\_\_\_\_\_\_\_\_

**步骤6：删除VLAN**

进入VLAN database mode ，使用no格式命令，如下：

Switch#vlan database

Switch(vlan)#no vlan 3

Switch(vlan)#exit

验证配置结果：（特权模式下 show vlan 命令）

问：VLAN 3 已经被删除了吗? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

问：当删除了VLAN后，对端口来说发生了些什么? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**步骤7：删除VLAN1**

尝试删除 VLAN 1，结果如下：

Switch#vlan database

Switch(vlan)#no vlan 1

A default VLAN may not be deleted.

Switch(vlan)#exit

**请查阅资料后回答：**为什么VLAN1不能被删除？

### 4.2 VLAN间路由

#### 4.2.1 交换机的配置

**步骤1：配置两台工作站**

在计算机A（下称“A机”）上配置192.168.2.1的地址，子网掩码255.255.255.0，网关192.168.2.254. 在计算机B（下称“B机”）上配置192.168.3.1的地址，子网掩码255.255.255.0，网关192.168.3.254。然后把A机和B机插入vlan2和vlan3的端口中。

**步骤2：将相应的接口加入VLAN中**

1. vlan1为默认vlan，故不用配置
2. 将2－4口划分为vlan2

switch(config)#interface FastEthernet 0/2

switch(config)#switchport access vlan 2

switch(config)#interface FastEthernet 0/3

switch(config)#switchport access vlan 2

switch(config)#interface FastEthernet 0/4

switch(config)#switchport access vlan 2

1. 将6－8口划分为vlan3

switch(config)#interface FastEthernet 0/6

switch(config)#switchport access vlan 3

switch(config)#interface FastEthernet 0/7

switch(config)#switchport access vlan 3

switch(config)#interface FastEthernet 0/8

switch(config)#switchport access vlan 3

1. 开启FastEthernet 0/24的Trunk

switch(config)#interface fastethernet 0/24

switch(config-if)# switchport trunk encapsulation dot1q

switch(config-if)# switchport mode trunk

#### 4.2.2 路由器的配置

**步骤1：配置子端口，封装和接口地址**

1. 激活快速以太网0/0口

Router(config)#interface FastEthernet 0/0

Router(config-if)#no shutdown

1. 配置子接口并且封装

Router(config)#int f0/0.1

Router(config-if)#encapsulation dot1q 2

Router(config-if)#ip address 192.168.2.254 255.255.255.0

Router(config)#int f0/0.2

Router(config-if)#encapsulation dot1q 3

Router(config-if)#ip address 192.168.3.254 255.255.255.0

Router(config-if)#exit

Router(config)#exit

**步骤2：检测并思考**

完成以上配置，检查无误后，A机和B机互相Ping对方的IP地址。回答以下问题：

A机和B机是否可以互相Ping通？\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

记下A机到B机的tracert结果：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# 附录1：实验报告提交要求

1. 根据实验指南，提前撰写实验报告，适当留空，可在实验过程中填入截图和进行分析解释；
2. 实验报告封面至少需提供 姓名（如果要求分组的实验，应包括组成员姓名学号）、学号、班级等信息；

# 附录2：Packet Tracer简介

Packet Tracer 是由Cisco公司发布的一个辅助学习工具，为学习思科网络课程的初学者去设计、配置、排除网络故障提供了网络模拟环境。用户可以在软件的图形用户界面上直接使用拖曳方法建立网络拓扑，并可提供数据包在网络中行进的详细处理过程，观察网络实时运行情况。可以学习IOS的配置、锻炼故障排查能力。软件还附带4个学期的多个已经建立好的演示环境、任务挑战，目前最新的版本是 Packet Tracer 6.\*。它还支持VPN,AAA、IPv6等高级配置。