计算机网络

实 验 指 南

（计算机类本科生试用）

广东省计算机网络重点实验室
计算机科学与工程学院
华南理工大学

2015 年 6 月

目 录

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。

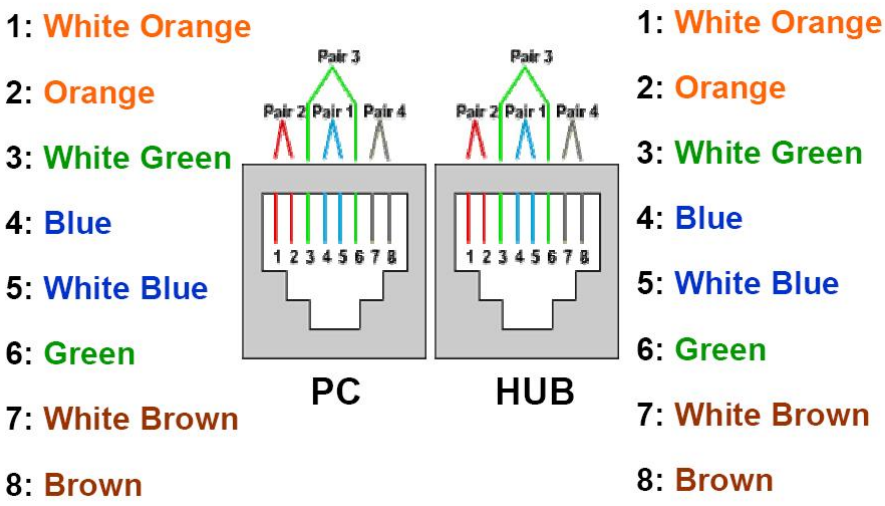
说明：为节约资源，本次实验每个同学只使用三个水晶头和一根网线。先做好一条直连线经检查合格后。剪去网线的一端，再做一根交叉线。即共用一次 T568B 线端。

线序标准：主要有 T568A 和 T568B 两个标准，如下表所示：

引针号	1	2	3	4	5	6	7	8
T568A	白绿	绿	白橙	蓝	白蓝	橙	白棕	棕
T568B	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

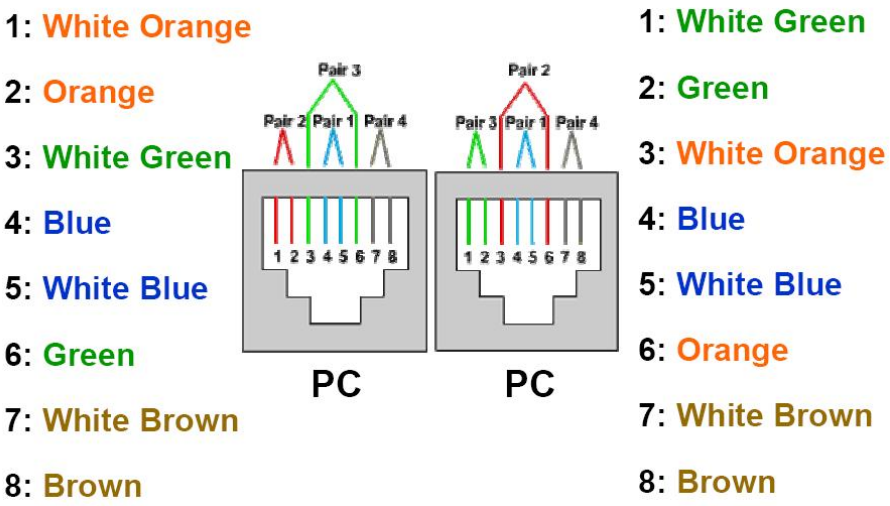
DCE：Data Communication Equipment 数据通信设备，数据电路终端设备，通常产生时钟。例：Modem、Hub 、Switch 等

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

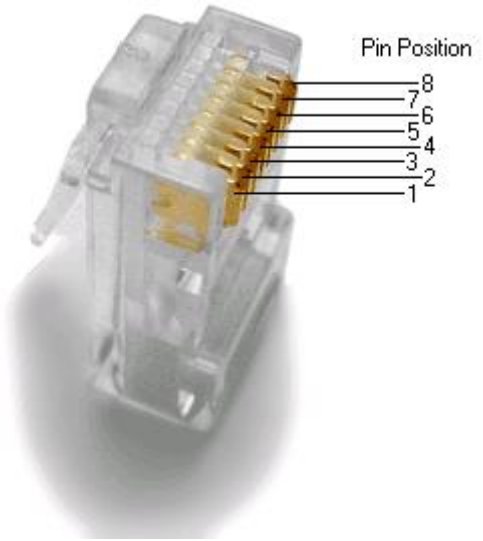
步骤 1：清除末端线的外皮

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，包括 ARP 报文，ICMP 报文。

（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）是一个免费的网络报文分析软件。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。网络报文分析软件有个形象的名字“嗅探工具”，像一只猎狗，忠实地守候在接口旁，抓获进出该进口的报文，分析其中携带的信息，判断是否有异常，是网络故障原因分析的一个有力工具。

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。

请需要的同学在教学在线上下载中文操作手册。

2.2 实验要求

软件： Wireshark （目前最新版本 1.4.1）

硬件：上网的计算机

3. 实验步骤

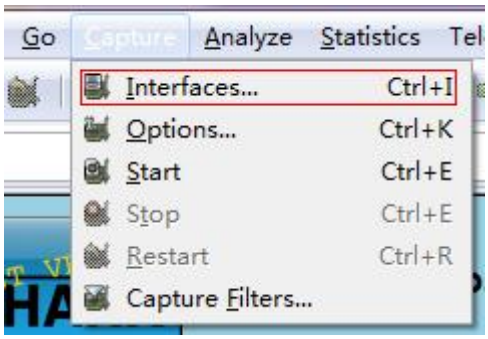
3.1 wireshark 的安装

wireshark 的二进制安装包可以在官网 http://www.wireshark.org/download.html#release 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

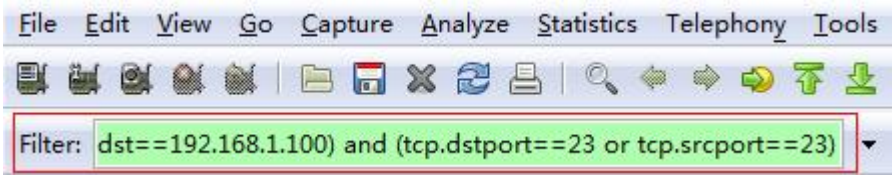
记录并解释 wireshark 监听的包内容（解释 1 条记录即可）

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

3.6.1 验证 ARP 工作原理

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，必须把目的IP 地址对应到以太网的MAC 地址。当一台主机自己的ARP表中查不到目的IP对应的MAC地址时，需要启动ARP协议的工作流程。

ARP 工作时，送出一个含有目的IP 地址的广播ARP请求数据包。如果被请求目的IP对应的主机与请求机位于同一个子网，目的主机将收到这个请求报文，并按照RFC826标准中的处理程序处理该报文，缓存请求报文中的源IP和源MAC地址对，同时发出ARP应答（单播），请求机收到ARP应答，将应答中的信息存入ARP表，备下次可能的使用。如果被请求目的IP对应的主机与请求机不在同一个子网，请求机所在的缺省网关（代理ARP）会发回一个ARP应答，将自己的MAC地址作为应答内容，请求机即将目的IP和网关的MAC地址存入ARP表中。

为了维护ARP表的信息是反应网络最新状态的映射对，所有的ARP条目都具有一个老化时间，当一个条目超过老化时间没有得到更新，将被删除。

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，首先将本机的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请求报文来查询被ping机器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。

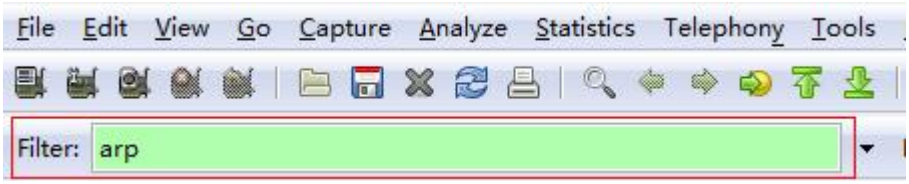
3.6.1 验证实验

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。

3.6.2 设计一个 ARP 缓存刷新机制的验证

为了避免子网中频繁发起ARP请求，让ARP工作得更加高效，每台主机（包括路由器）内部的内存中都开辟了一个ARP缓存空间，叫ARP表。按照教材上的讲解，ARP表的刷新因素主要有：（1）从应答中提取IP-MAC映射对；（2）从机器启动的时候发送的免费ARP请求（gratuitous ARP）中提取源IP-MAC映射对；（3）从子网中侦听到的普通ARP请求广播帧中读取源IP-MAC映射对。在PT模拟演示中，已经看到：侦听到ARP广播请求的主机，并没有刷新自己的ARP表。

请设计一个实验来分析说明现实网络中，上述第二条和第三条刷新机制是否存在或者被实现。

注意：

（1）实验室B3-230、231的所有PC的 consel 网卡都处于同一个大子网中（255.255.252.0）。

（2）建议：这个设计实验，以4~8人的组来完成，并请组长在实验报告中写明实验方法，得到的结论，分析过程等，尽量详细。（组长一人写，并写明协助一起完成的组成员；组成员在自己的实验报告中，只需说明参加哪位组长的实验即可。）

（3）如果时间来不及，请在宿舍继续完成该项。

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。

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

实验可以在真实网络环境中和 Packet tracer 模拟器（或别的模拟器中）中完成。

请大家在网络实验室完成实验，在安排时间内无法完成的同学，请继续在模拟器 packet tracer 上完成。

路由器、交换机、上网主机，线缆若干条。

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。

注意：锐捷实验系统不采用超级终端，采用 sceCRT，无须手动启动，由锐捷实验系统自动调用。

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

5) 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）	

A. Router#
B. Router>
C. Router(config-if)#
D. Router(config-router)#
E. 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	

A. 详细查看路由器的运行情况，对路由器进行调试、测试，
B. 设置 IP 地址和子网掩码
C. 运行简单的配置命令
D. 有限度地查看路由器的运行情况，可远程登录
E. 设置路由选择协议

7) 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)#	

8) 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?_____

9) 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?_____

C. show arp 命令的作用是什么?_____

D. show running-config 命令的作用是什么?_____ ，它的信息保存在哪里？_____。

E. show startup-config 命令的作用是什么?_____ ，它的信息保存在哪里？_____。

10) 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

4.2.1 IPv4 直连路由

1）绘制拓扑

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。

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

3）请使用 show ip route 检查路由表，观察是否产生了直连路由。

回答：（1）PC1 和 PC2 是否通达？为什么？

4.2.2 IPv6 直连路由通达实验参考步骤（选做）

1) 绘制拓扑

2) 首先配置路由器，如下图所示：

```
Router(config)#interface fa0/1
Router(config-if)#ipv6 address 3::1/64
Router(config-if)#ipv6 enable
Router(config-if)#no shutdown
```

```
RSR20-24(config)#interface fa0/0
RSR20-24(config-if)#ipv6 address 2::1/64
RSR20-24(config-if)#ipv6 enable
RSR20-24(config-if)#no shutdown
RSR20-24(config-if)#
```

注意：（1）一定不要忘记使用“no shutdown”开启接口。（2）配置完一个接口，使用 show ipv6 route 查看 IPv6 路由表，注意观察随着接口地址的配置，路由表发生了什么变化？

3) 设置路由器接口下的 PC 的 IPv6 地址，让它和它的网关位于同一个子网，如上图中 PC0 的静态配置方法如下：（由于实验室未开启 DHCPv6 服务器，无法有状态获取 IPv6 地址）

第一步：安装 ipv6，在 dos 控制台，键入命令：

ipv6 install （如果在 GUI 界面安装了，该步骤省略）

第二步：为验证网卡配置一个 IPv6 地址：

Ipv6 adu 4/2::5

注意：上述命令的语法是 ipv6 adu *ifindex/address [life validlifetime]*，其中的参数 ifindex 表示验证网卡的索引号，如果不知道这号码，可使用命令 ipv6 if 查看。

第三步：在 IPv6 地址的配置中，并没有标识它所示的子网，所以，需要为它指明：

Ipv6 rtu 2::/64 4 (其中的 4 是索引号)

4) 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？

实验四 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。

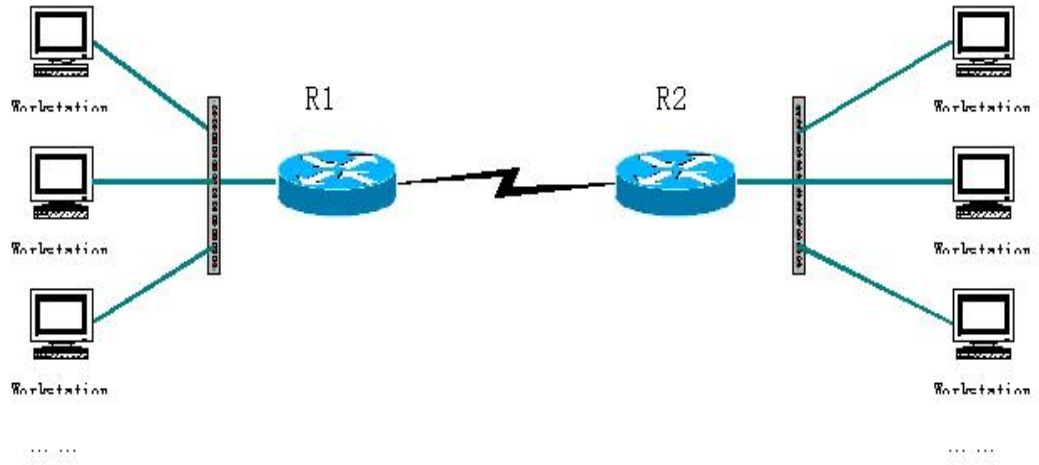
3） 掌握静态路由的方法。

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。

2. 实验环境和要求

2.1 实验拓扑



2.2 实验器材

1） 路由器两台

2) 交换机两台

3) 学生实验主机

4) 网线若干。请注意主机与交换机，交换机与路由器之间使用直通线。路由器与路由器之间使用交叉线。

2.3 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。

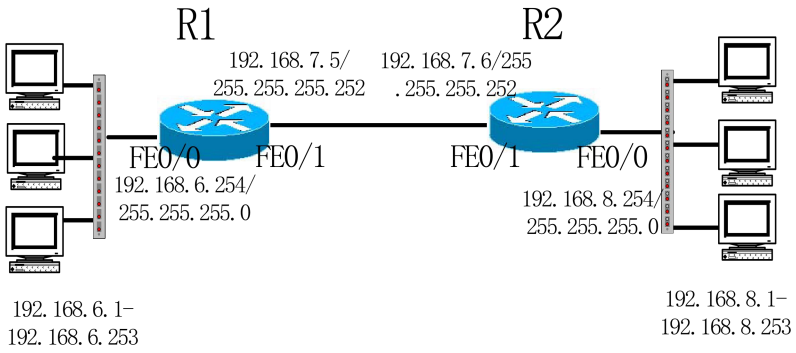
1) 请按实验网络拓扑作出网络规划。并写出路由器的端口地址和各节点网络地址。

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。

实验五：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）。

4. 编程参考

4.1 套接字简介

（1）网络应用程序编程接口(API)

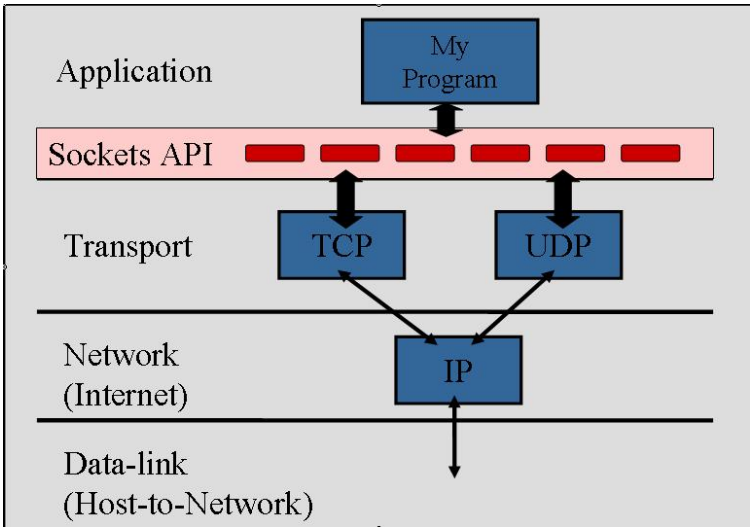
计算机用它来对网络发送或接收信息。

（2）套接字接口（socket interface）

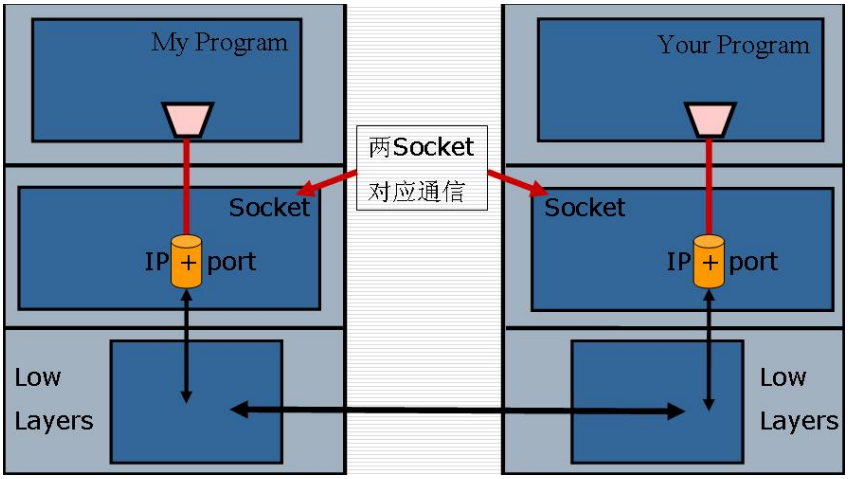
由加州大学伯克利分校 UNIX 小组开发，目前最为流行。定义了网络上的各种操作（如生成套接字，发送/接收消息等。

（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

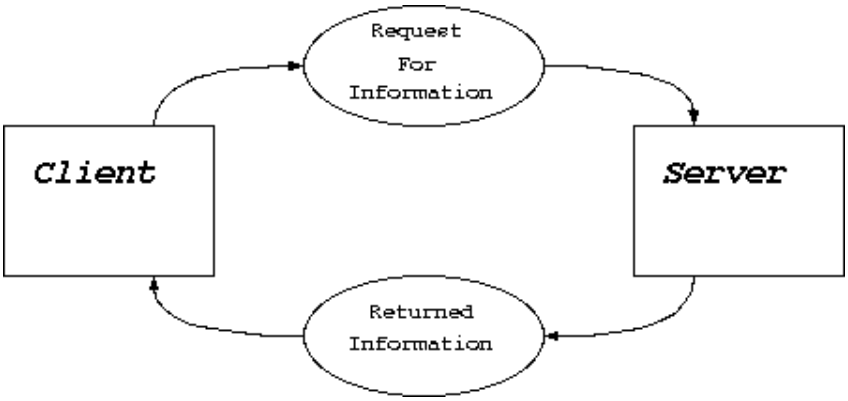


可认为一个 IP 与一端口（port）联合在一起形成一个套接字，它是网络上的一个传输接口。在网络的另外一端可有一个对应的套接字与通信。



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

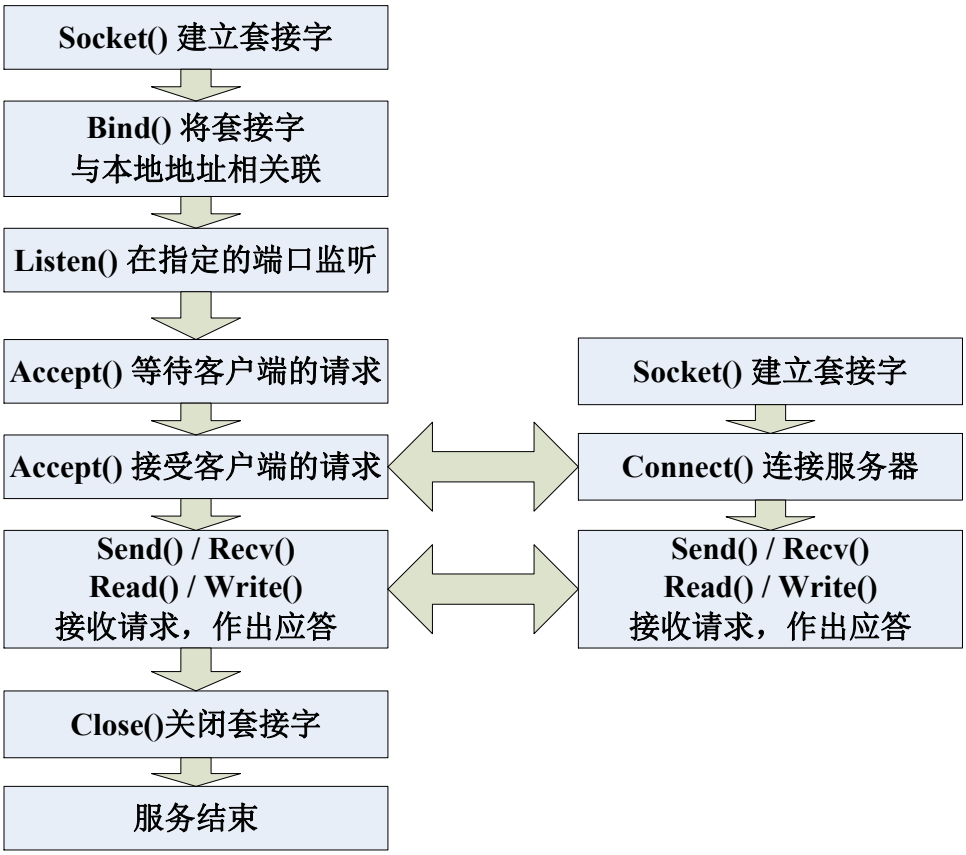
int listen() 开始监听端口

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

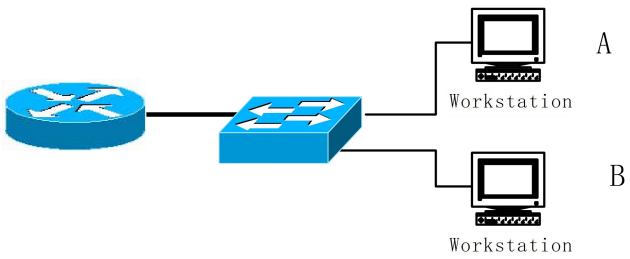
1） CISCO 路由器一台。

2） 交换机一台。

3） 学生实验主机每人一台。

4） 网线若干。请注意主机与交换机，交换机与路由器之间使用直通线。路由器与路由器之间使用交叉线。

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

2) 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

3) 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? _____

2) 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? _____

3) 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
```

3) 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
```

4) 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
```

2) 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：_____

致谢

1. 实验二初稿由研究生李振宁起草；

2. 其它实验参考 CCNA 的实验指南编制。

本指南仅供教学之用，不用作任何商业目的，在此对李振宁和 Cisco 公司表示感谢。

附录 1：实验室网络设备的使用

1. B3-230、B3-231 于 2013 年 5 月正式启用新的网络设备，本门课程用到的主要是锐捷的路由器和交换机。锐捷路由器和交换机安放在每台左面旁边的透明机架内，不能搬动，但可以观看，操作它只能通过锐捷的系统。
2. 每位同学一个座位，桌面显示器上贴有系统网址，本机 consel 网卡的 IP 地址和网关等信息。请同学们先打开 secCRT 应用程序，点击“选项”——“全局选项”—— “网页浏览器”，在右下角勾选 telnet、SSH1、SSH2 设置 CRT 为您的默认 Telnet 工具。然后打开浏览器，输入系统网址：http://192.168.1.251:8088/limp，出现如下的登陆页面：

3. 每位同学请使用自己的学号登陆，初始密码是 123456，登入系统之后，自行修改密码。登入后，进入如下页面，请选择“开始实验”，在出现的页面右上方选择“开放实验”下的“”进入实验按钮，打开实验选择界面，在左边选择“自定义”之“初级”，在展开的列表中，选择某个实验开始实验（实验 3 路由器的基本操作（袁华） 或 实验 4 组网实验（袁华））：

4. 实验 3 中，每位同学须独立进行操作。一张实验台 8 个桌位，一个机架，包括 4 台二层交换机（S2628G-I）、2 台 3 层交换机（S5750-28GT-L），3 台路由器（RSR20-24）。同时操作路由器的同学不能多过 3 位，其它同学可以在系统中围观。
5. 实验 4，建议 4 位同学一组，分别选用 2 台路由器（或 3 层交换机）和 2 台交换机和 4 台 PC 进行组网。第一位进入实验操作的同学为组长，由组长负责实验拓扑的绘制和协调各位同学的操作。每 4 位同学一组提交实验报告（教学在线）。
6. 当需要验证网络是否通达的时候，请使用 PC 和其上的验证网卡，地址和网关配置根据实验需要进行。注意：当启用验证网卡验证的时候，请先取消 consel 网卡的网关配置等信息。
7. 更多的操作细节，请参考锐捷提供的“用户手册-学生篇”。

附录 2：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；
3. 实验 4 的报告按组提交，4 人一组，只有组长提交，在报告封面中注名组成员，其它同学不提交。
4. 在实验时间未完成实验或实验报告的同学，可继续在宿舍中完成；
5. 请计算机操作不太熟练的同学提前在宿舍熟悉实验中用到的工具和命令。

附录 3：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。

请需要的同学，在教学在线中下载 packet tracer 的中文操作手册。