

---

# 华中科技大学计算机学院

## 《计算机通信与网络》实验报告

班级\_\_\_\_ 姓名\_\_\_\_\_ 学号\_\_\_\_\_

项目	Socket 编程 (40%)	数据可靠传输协议设计 (20%)	CPT 组网 (20%)	平时成绩 (20%)	总分
得分					

教师评语：

教师签名：

给分日期：

---

---

# 目 录

实验三 基于 CPT 的组网实验 .....	1
1.1 环境 .....	1
1.2 实验要求 .....	1
1.3 基本部分实验步骤说明及结果分析 .....	2
1.4 综合部分实验设计、实验步骤及结果分析 .....	16
心得体会与建议 .....	23
2.1 心得体会 .....	23
2.2 建议 .....	23

---

## 实验三 基于 CPT 的组网实验

### 1.1 环境

（实验机器的硬件配置、系统软件组件、第三方软件）

操作系统：Microsoft Windows 10

仿真软件：Cisco Packet Tracer 6.0

### 1.2 实验要求

1. 了解 IP 协议、网络层协议和数据链路层协议的工作原理及机制：在实验中，要求对 IP 协议、网络层协议（如 IPv4 和 IPv6）以及数据链路层协议（如 Ethernet）的工作原理和机制有一定的了解，包括数据包的封装和解封装过程、路由选择机制、地址解析和转发等方面的知识。
2. 掌握 IP 地址的规划方法：实验要求熟悉 IP 地址的规划方法，包括了解不同 IP 地址类型（如公网 IP 和私有 IP）、子网划分和子网掩码的计算、IP 地址的分配和路由表的配置等内容。
3. 掌握路由协议的配置方法：要求掌握常见的路由协议（如静态路由和动态路由协议如 RIP、OSPF 等）的配置方法，了解路由表的维护和更新过程，能够实现路由器之间的通信和数据包转发。
4. 掌握路由器及二/三层交换机的配置方法：实验要求熟悉路由器和二/三层交换机的配置方法，包括端口设置、VLAN 的创建和配置、链路聚合（如 EtherChannel）的配置等，能够正确地连接和配置这些网络设备。
5. 了解 VLAN 的划分原理：要求了解虚拟局域网（VLAN）的划分原理，包括 VLAN 的概念、VLAN 的配置和管理、VLAN 的隔离和互通等内容。
6. 掌握访问控制的配置方法：实验要求熟悉访问控制列表（ACL）的配置方法，包括了解 ACL 的作用、规则的设置和应用场景等，能够实现对网络流量的过滤和控制。
7. 熟悉 Cisco Packet Tracer 仿真软件：要求熟悉使用 Cisco Packet Tracer 仿真软件进行网络拓扑配置和模拟实验的操作，包括设备的添加和连接、配置命令的输入和验证等。
8. 利用 Cisco Packet Tracer 仿真软件完成实验内容：实验要求使用 Cisco Packet Tracer 仿真软件完成实验，包括创建网络拓扑、配置设备、测试网络连接和功能等，并记录实验过程中的步骤和结果。

## 1.3 基本部分实验步骤说明及结果分析

### 1.3.1 IP 地址规划与 Vlan 分配实验的步骤及结果分析

#### 1) 绘制网络拓扑图

根据实验要求给定的拓扑图，在 Cisco Packet Tracer 中绘制等效的拓扑图，如图 1-1。图中有 8 台 pc 机，四台交换机和一台路由器。

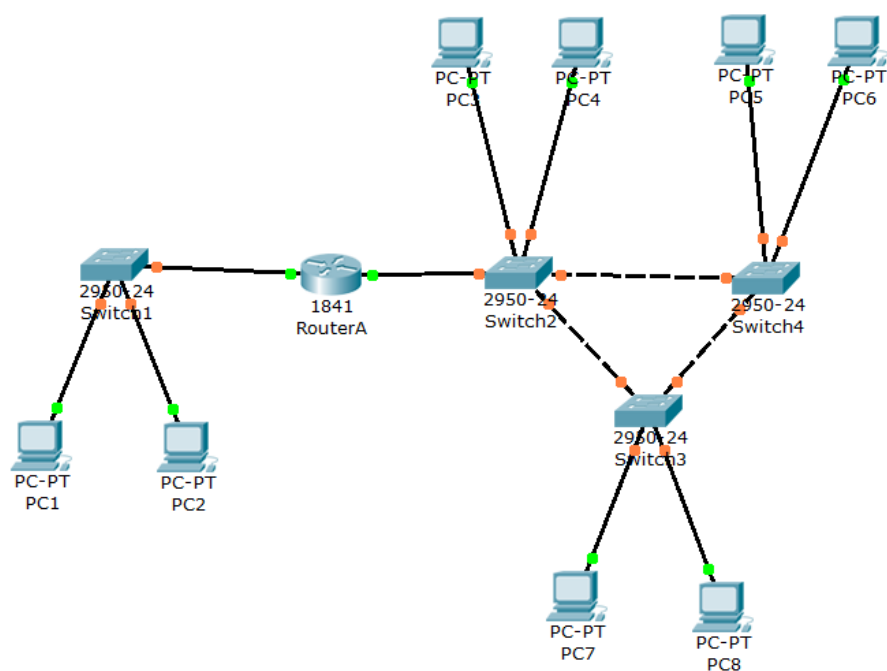


图 1-1 网络拓扑图

#### 2) 基本内容 1

a) 单击路由器，弹出其配置信息，选择接口配置中的以太网接口 FastEthernet0/0，这是路由器与交换机 1 相连的接口，掌管的是 pc1 和 pc2，该子网的网络地址为 192.168.0.0。由于 192.168.0.0 作为网络地址不可直接使用，所以将该端口地址设为 192.168.0.1，子网掩码自动生成成为 255.255.255.0。配置结果如图 1-2：

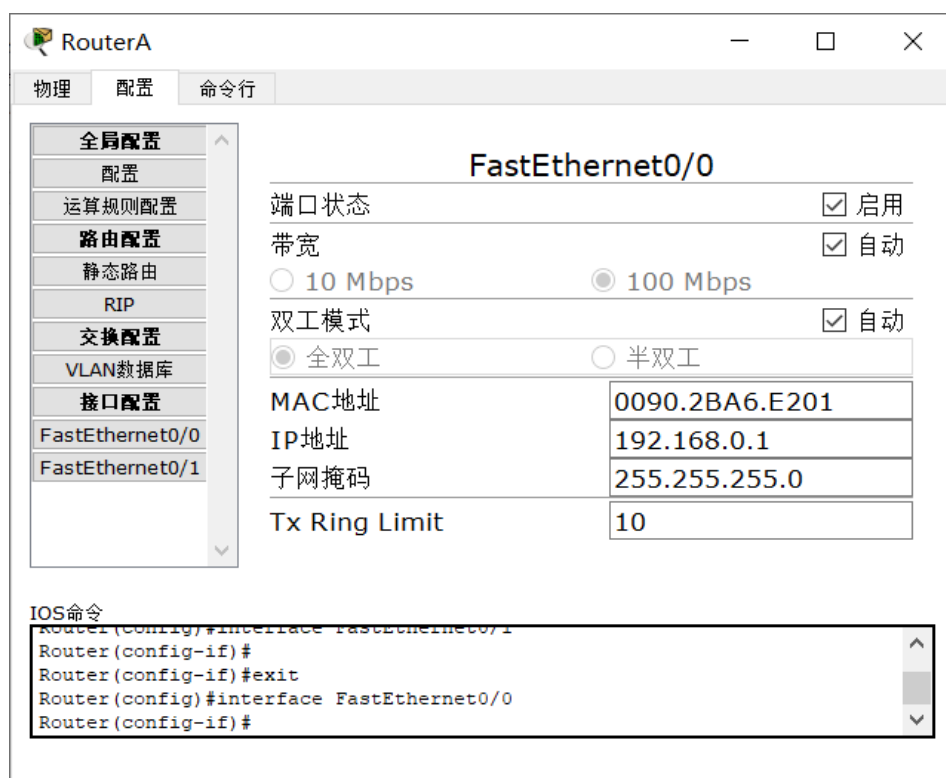


图 1-2 路由器配置

在图 1-2 的下方可以看到，每次配置以后，都会自动生成相应的命令行。因此我们可以想到，这些配置信息也可以用命令行实现，只是该软件提供了相当一部分功能的图形界面配置方法，所以我们要充分利用起来，尽量使用图形界面。

b) 配置完接口 0/0，还需要配置接口 0/1，选择快速以太网端口 0/1，该端口控制右侧的 6 台 pc 机，子网地址为 192.168.1.0，所以该端口地址为 192.168.1.1，配置方法和结果都与端口 0/0 类似，不再赘述。

c) 配置 PC 机 PC1 IP 地址，单击 PC1，弹出其配置窗口，选择快速以太网接口 0，配置 IP 地址为 192.168.0.2，当然也可以选择 192.168.0.0 网段的其他地址，只要不与路由器端口 1 的 IP 地址 192.168.0.1 重复即可；子网掩码可以直接生成，为 255.255.255.0，配置结果如图 1-3：

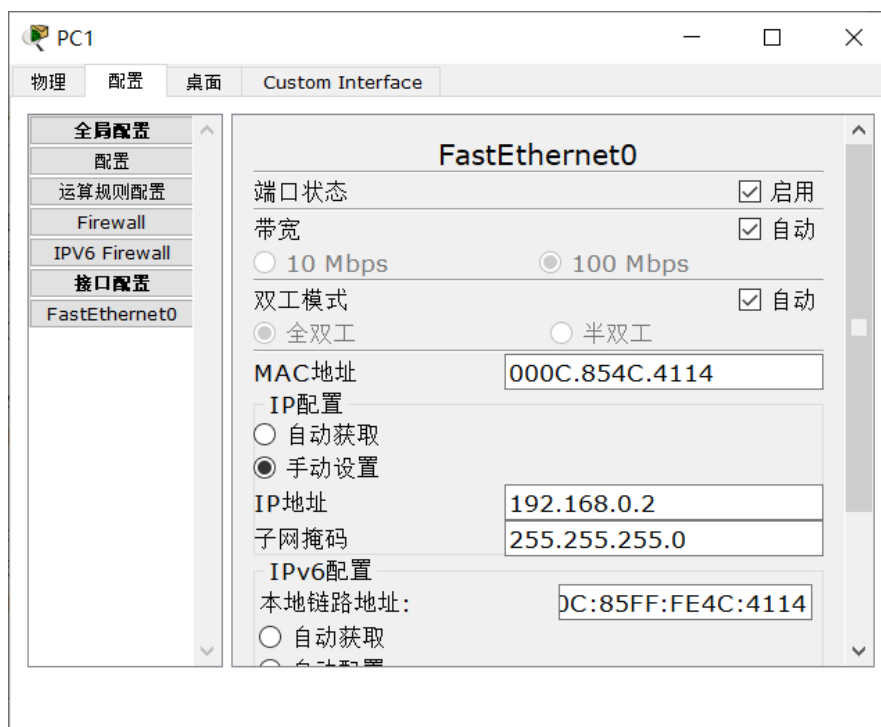


图 1-3 PC 配置 IP 地址和子网掩码

d) 配置 PC 机 PC2 子网掩码，配置完 PC1 的 IP 地址以后，还要配置子网掩码，也就是掌管该 PC 机的路由器端口的 IP 地址，即路由器端口 0/0 的地址。选择 PC1 的“配置”，在“网关”一栏填写路由器端口 0/0 的 IP 地址 192.168.0.1，如图 1-4：



图 1-4 PC 配置网关

e) PC2 和 PC1 处于同一网段，网关和子网掩码相同，因此只需给 PC2 分配同一网段内的不同 IP 地址 192.168.0.3 即可；

f) PC3-PC8 位于 192.168.1.0 网段，所以可以在 192.168.1.0 网段中选择 8 个 IP 地址分别对其进行配置，该网段由路由器的 fa0/1 端口进行管理，所以 6 台 PC 机的网关地址都应填写 fa0/1 的 IP 地址 192.168.1.1。

g) 网段 1 连通性测试：配置完成以后，应测试各个 PC 机之间的连通性是否符合实验要求，这里先测试网段 192.168.0.0。单击 pc1，选择：桌面->命令提示符，进入命令行界面，用“ping”指令与其他 pc 机进行通信，输入命令：ping 192.168.0.3，表示对 pc2（192.168.0.3）进行回话请求，向 pc2 发送四个报文段，均成功收到回复，如图 1-5：

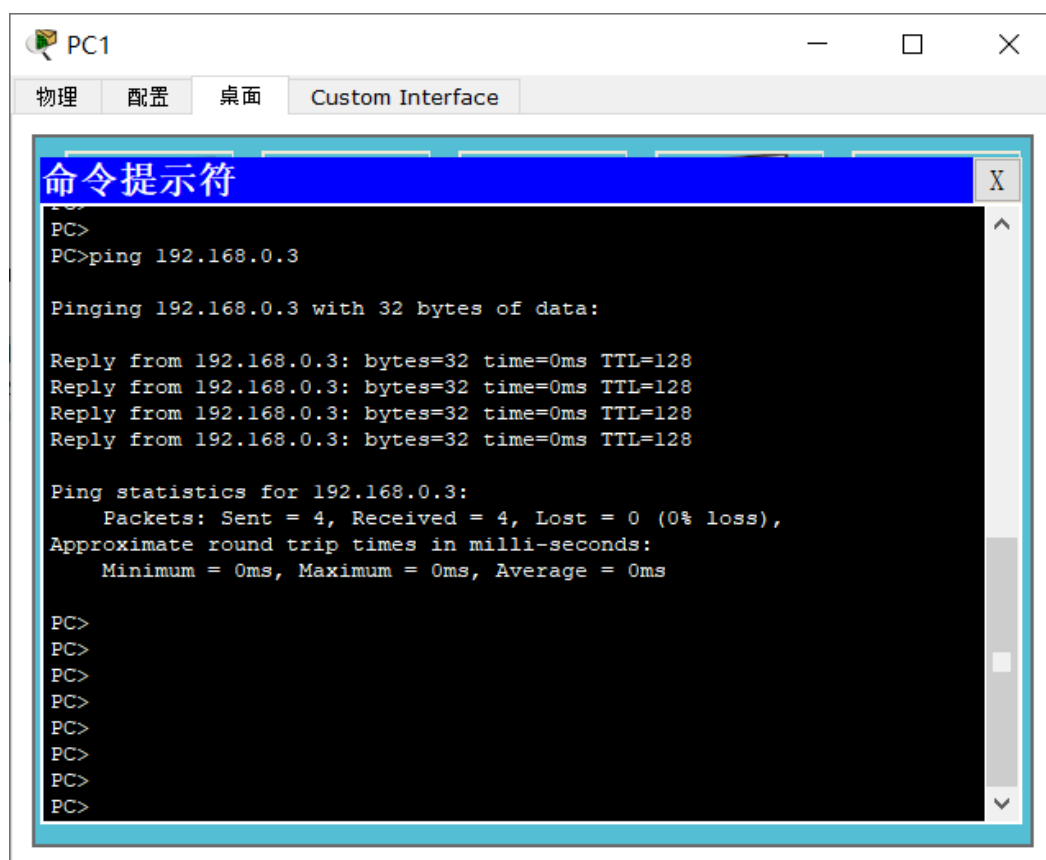


图 1-5 PC1 与 PC2 连通测试

单击 pc2，同样选择命令提示符，向 pc1 发起会话，也成功收到回复，如图 1-6：

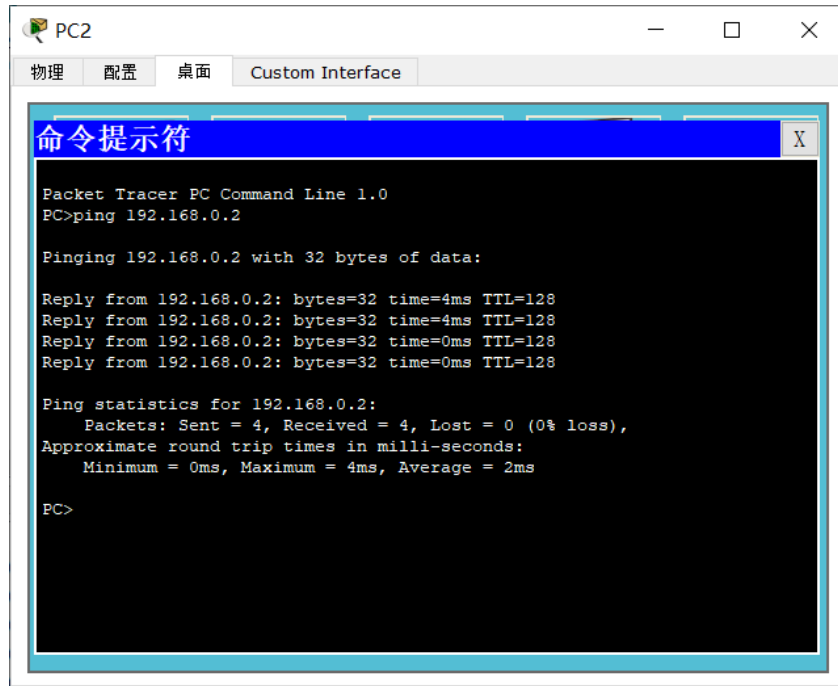


图 1-6 PC2 与 PC1 连通测试

#### h) 网段 2 连通性测试:

在 pc3-pc8 中,任意两台 pc 之间进行通信测试,都会通信成功,测试结果如图 1-7 的 pdu 窗口所示。

PDU列表窗口										
激活	最后状态	来源设备	目的设备	类型	颜色	时间(秒)	固定周期	顺序	编辑	删除
	成功	PC3	PC4	ICMP	蓝色	0.000	N	0	(编辑)	(删除)
	成功	PC3	PC7	ICMP	绿色	0.000	N	1	(编辑)	(删除)
	成功	PC6	PC8	ICMP	深蓝色	0.000	N	2	(编辑)	(删除)
	成功	PC7	PC5	ICMP	紫色	0.000	N	3	(编辑)	(删除)
	成功	PC8	PC4	ICMP	蓝色	0.000	N	4	(编辑)	(删除)

图 1-6 网段 2 连通测试

#### i) 结果分析:

配置 IP 后,两个网段内部都可以进行通信,第二次配置 IP 以后,三个网段内部的内部也可以分别进行通信,符合实验要求。网段每个网段内部的 pc 机之间都是通过交换机连接起来的,内部通信不需要经过路由器就可以直接发送至对方,所以不管有没有给路由器端口分配 IP 地址、有没有给 PC 机配置网关,都可以进行内部通信。

#### 3) 基本内容 2:

完成基本内容 1 以后,要求将 pc4、pc6、pc8 从子网 192.168.1.0 网段中分离出去,编入子网 192.168.2.0,所以需要在这三台 pc 重新配置 IP。

#### a) 配置 IP:



配置 IP 的过程已经在基本内容 1 中做过解释，因此此处不在过多赘述，此处的结果是将 pc4 的 IP 配置为 192.168.2.2, pc6 的 IP 配置为 192.168.2.3, pc8 的 IP 配置为 192.168.2.4，同时将三台 pc 的网关配置为 192.168.2.1。

b) 配置 VLAN:

交换机的 VLAN 可用图形界面配置。题目要求将右侧的 6 台 pc 机划分到两个 VLAN 中，所以需要在所有的路由器上都添加两个 VLAN，VLAN 号可以任意选择，只要不与路由器本身的 VLAN 号重复就可以。这里选择 3 和 4 作为 VLAN 号，两个 VLAN 名分别为 VLAN3 和 VLAN4。以交换机 switch0 为例，选择在：配置->交换配置->VLAN 数据库，添加两个 VLAN，如图 1-8。

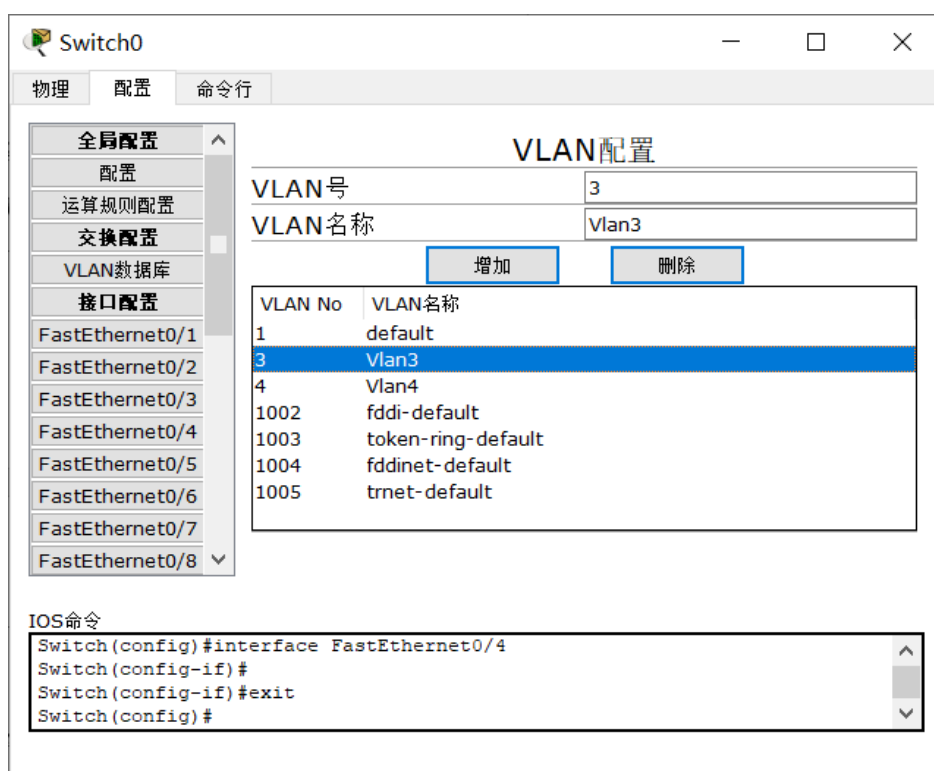


图 1-7 添加 VLAN

交换机的 VLAN 添加完成后，还需要对它的端口进行 VLAN 划分。对于交换机与交换机相连，或者交换机与路由器相连的链路，都称为主干链路，选中该链路对应的端口，选择链路类型为“trunk”，trunk 链路的 VLAN 默认包含了所有的 VLAN，不需要修改，如图 1-8。

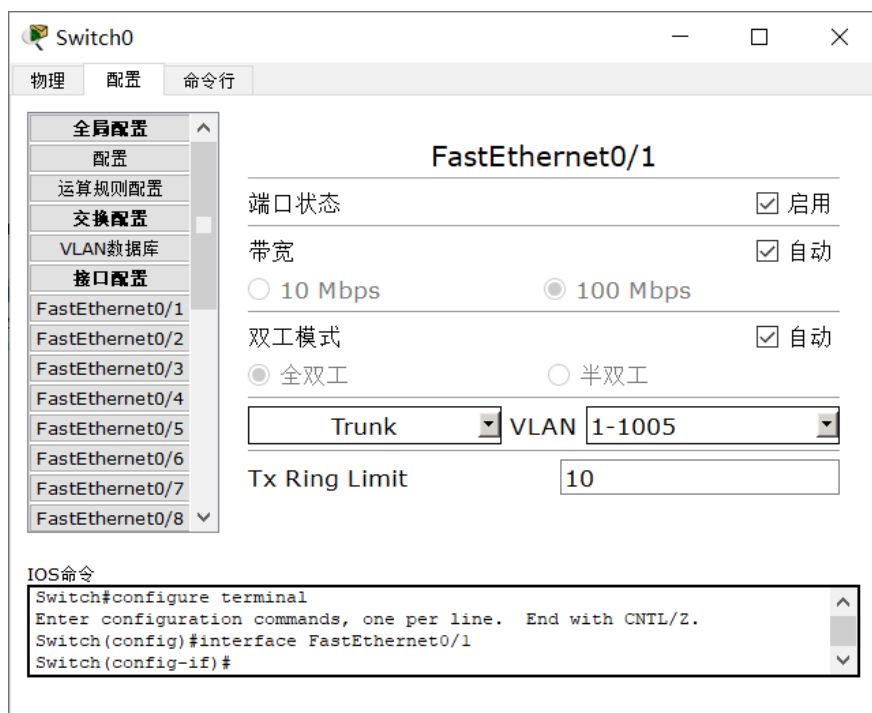


图 1-8 配置交换机主干线路

对于交换机与 pc 相连的链路，链路类型应该选择为 access 类型，access 链路的默认 vlan 为 vlan1，我们应该把它改成我们添加的 vlan，如果该端口连接了 pc3、pc5 或 pc7，就选择 vlan 3，如图 1-9；如果端口连接了 pc4、pc6 或 pc8，则选择 vlan 4。



图 1-9 配置交换机 PC 线路

c) 连通性测试:

先分别对两个 vlan 内部的主机进行访问测试, 如图 1-10, 对 pc3、pc5 和 pc7 进行互访, 都能成功; 对 pc4、pc6 和 pc8 进行互访, 也可以成功。

PDU列表窗口										
激活	最后状态	来源设备	目的设备	类型	颜色	时间(秒)	固定周期	顺序	编辑	删除
	成功	PC3	PC5	ICMP		0.000	N	0	(编辑)	(删除)
	成功	PC3	PC7	ICMP		0.000	N	1	(编辑)	(删除)
	成功	PC5	PC7	ICMP		0.000	N	2	(编辑)	(删除)
	成功	PC4	PC6	ICMP		0.000	N	3	(编辑)	(删除)
	成功	PC4	PC8	ICMP		0.000	N	4	(编辑)	(删除)
	成功	PC6	PC8	ICMP		0.000	N	5	(编辑)	(删除)

图 1-10 同 VLAN 连通性测试

尝试让 vlan 3 的主机访问 vlan 4, 不能成功, 反之亦然, 结果如图 1-10。

PDU列表窗口										
激活	最后状态	来源设备	目的设备	类型	颜色	时间(秒)	固定周期	顺序	编辑	删除
	失败	PC3	PC4	ICMP		0.000	N	0	(编辑)	(删除)
	失败	PC5	PC6	ICMP		0.000	N	1	(编辑)	(删除)
	失败	PC7	PC8	ICMP		0.000	N	2	(编辑)	(删除)
	失败	PC3	PC8	ICMP		0.000	N	3	(编辑)	(删除)
	失败	PC3	PC6	ICMP		0.000	N	4	(编辑)	(删除)
	失败	PC5	PC8	ICMP		0.000	N	5	(编辑)	(删除)

图 1-10 不同 VLAN 连通性测试

d) 路由器 vlan 配置:

由于路由器只有两个端口, fa0/1 端口所管理的网络中有两个网段的 pc 机, 所以要为该端口分配子端口, 并为子端口分配 vlan, 才能使两个 vlan 的主机可以通信。

对路由器 A 的快速以太网接口 0/1, 创建子接口 fa0/1.1, 并将其划分到 vlan 3 中, ip 地址设置为 192.168.1.1。这些都只能用命令行配置, 如图 1-11:

```

Router(config)#int fa0/1.1
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/1.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1.1, change
to up

Router(config-subif)#encap dot1q 10
Router(config-subif)#ip addr 192.168.1.1 255.255.255.0
Router(config-subif)#exit

```

图 1-11 路由器增加子接口

再用同样的方法建立子接口 fa0/1.2, 将其划入 vlan 4, ip 地址设置为 192.168.2.1。

e) PC1 和 PC2 的子网划分:

首先需要在 pc1 和 pc2 相连的交换机 1 上添加 vlan 2, 与其他三台交换机的添加方法相同, 将交换机与路由器相连的链路设置为 trunk 链路, vlan 使用默认参数, 即全选; 交换

机与 pc 相连的链路设置为 access 链路，vlan 都选择 2 号，这样就 将两台 pc 都划分到了 vlan 2 中。为路由器的 fa0/0 接口创建一个子接口 fa0/0.1，划分到 vlan 2，ip 设置为 192.168.0.1，至此，pc1 和 pc2 的 vlan 划分完成。

f) 连通性测试：

如图 1-12，vlan2 中的 pc1 和 pc2 可以任意访问其他网段。

PDU列表窗口										
激活	最后状态	来源设备	目的设备	类型	颜色	时间(秒)	固定周期	顺序	编辑	删除
	成功	PC1	PC3	ICMP		0.000	N	0	(编辑)	(删除)
	成功	PC1	PC4	ICMP		0.000	N	1	(编辑)	(删除)
	成功	PC2	PC5	ICMP		0.000	N	2	(编辑)	(删除)
	成功	PC2	PC6	ICMP		0.000	N	3	(编辑)	(删除)
	成功	PC1	PC7	ICMP		0.000	N	4	(编辑)	(删除)
	成功	PC2	PC8	ICMP		0.000	N	5	(编辑)	(删除)

图 1-12 vlan2 访问其他网段

如图 1-13，vlan3 和 vlan4 中的 pc 可以任意访问其他 pc。

PDU列表窗口										
激活	最后状态	来源设备	目的设备	类型	颜色	时间(秒)	固定周期	顺序	编辑	删除
	成功	PC3	PC7	ICMP		0.000	N	0	(编辑)	(删除)
	成功	PC3	PC8	ICMP		0.000	N	1	(编辑)	(删除)
	成功	PC4	PC5	ICMP		0.000	N	2	(编辑)	(删除)
	成功	PC4	PC6	ICMP		0.000	N	3	(编辑)	(删除)
	成功	PC6	PC7	ICMP		0.000	N	4	(编辑)	(删除)
	成功	PC8	PC6	ICMP		0.000	N	5	(编辑)	(删除)
	成功	PC3	PC1	ICMP		0.000	N	6	(编辑)	(删除)
	成功	PC6	PC2	ICMP		0.000	N	7	(编辑)	(删除)

图 1-13 vlan3 和 vlan4 互相访问

g) 结果分析：

网段 192.168.0.0 与 192.168.1.0 之间可以进行通信，这是因为路由器的端口都分配了 IP，而且在两个网段的 pc 机上将路由器端口 ip 设为了网关，所以 由第一个网段发往第二个网段的消息在经过路由器时，路由器可以进行转发， 故两个网段可以跨过路由器进行通信。

网段 192.168.2.0 与其他两个网段都不能进行通信，这是因为该网段没有配置 网关，路由器只有两个端口，都被其他两个网段占用了，该网段将没有网 关可用，所以它无法与其他子网进行通信，发送出的消息将被路由器忽略。

在交换机上划分 vlan 以后，各个主机被分入不同的 vlan，一个 vlan 是一个逻辑上的整体，他们不受空间和子网的限制，所以 pc1、pc2 可以跟 pc3 处于同一个 vlan 中。若不在路由器上进行 vlan 配置，一个 vlan 内部的主机可以进行通信，但是他们不能和其他 vlan 的主机通信，相当于这个 vlan 是与世隔 绝的。只有在路由器上进行 vlan 配置，一个 vlan 的主机向其他 vlan 主机发 送的消息才能被路由器识别并转发，否则，路由器不清楚消息该发向何处，因为路由器本地没有相关 vlan 可以选择。

### 1.3.2 路由配置实验的步骤及结果分析

#### 1) 绘制网络拓扑图

根据给定的拓扑图，绘制等效拓扑图，如图 1-14。图中有 4 台 pc 机，3 台交换机和 4 台路由器。

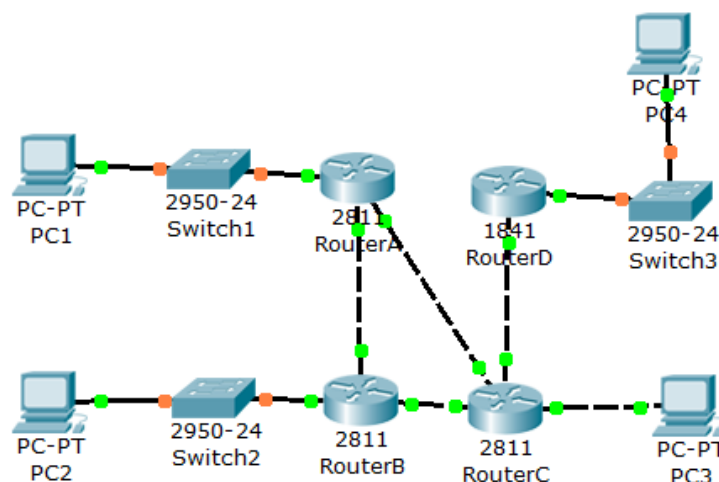


图 1-14 网络拓扑图

#### 2) 基本内容 1

##### a) 增加路由器端口

路由器与交换机连接可以使用快速以太网端口 FastEthernet，但是该端口不能用于路由器之间的互联，所以需要为路由器添加串口。以路由器 A 为例，如图 1-15，选择“物理”选项，在右端的开关处关闭路由器电源，在左侧的模块列表中，选中第一个模块“HWIC-2T”，拖到左侧的黑框中，再打开路由器电源，重新启动，并重新启用所有端口。

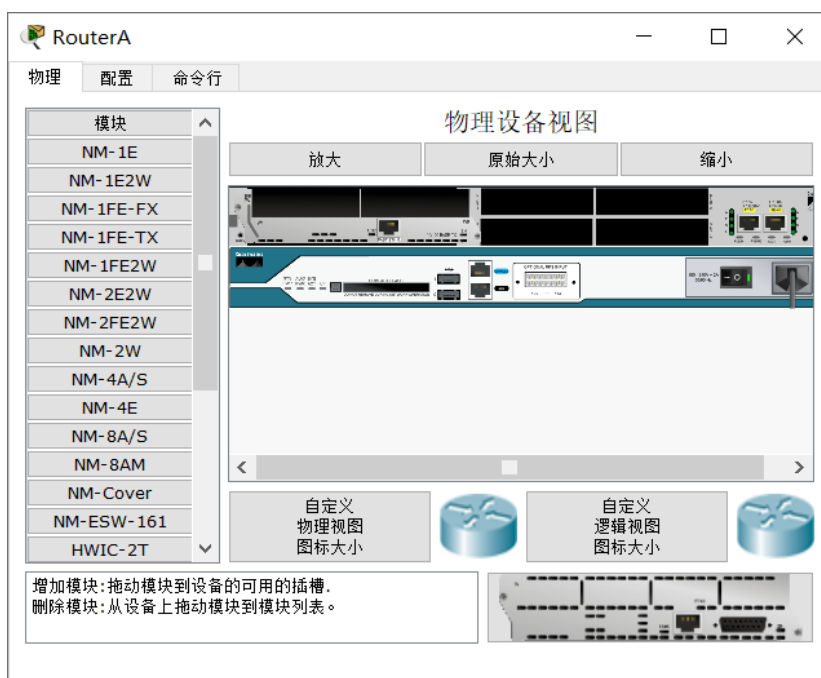


图 1-15 路由器 A

进入“配置”选项,可以看到路由器在原来的两个 fa 端口基础上,增加了一个 fa 端口,如图 1-16,可以用于路由器之间的连接。



图 1-16 路由器 A 接口

b) 配置路由器端口 IP ① 图 1-14 中有四个路由器,每个路由器管理一个子网,四个子网分别处于 192.168.1.0、192.168.2.0、192.168.3.0、192.168.4.0 网段,所以路由器与 pc 机或者交换机连接的端口 IP 应该配置为对应网段的 IP。路由器 A 的左端口 IP 为 192.168.1.1,路由器 B 的左端口 IP 为 192.168.2.1,路由器 C 的右方端口 IP 为 192.168.3.1,路由器 D 的右方端口 IP 为 192.168.4.1,图 1-17 所示为路由器 A 的 fa 端口 IP 配置,其他三个路由器与之类似。



图 1-17 路由器 A fa0/0 接口

第一步只配置了路由器连接 pc 的端口的 IP,在路由器之间的端口 IP 也需要配置,这些端口的 IP 选择比较自由,只要不与 PC 机所处网段的 IP 重叠即可,我们不妨选择 192.168.5.0、192.168.6.0、192.168.7.0、192.168.8.0 四个子网为路由器之间的四条链路进行 IP 分配,链路两端的 IP 分别设为 xxx.xxx.xxx.1 和 xxx.xxx.xxx.2,比如路由器 A 的 fa0/1 端口 IP 为 192.168.5.1,与之相连的路由器 B 的 fa0/1 端口 IP 为 192.168.5.2,其他端口 IP 可以类推得到。

d) 路由器 RIP 协议配置 RIP 协议是用于自治系统内的动态路由协议,它只和与自己相连的路由器交换信息,所以每个路由器配置该协议时,只需要把自己每个端口的 IP 地址所在网段填上即可。以路由器 A 为例,它的 fa0/0 端口 IP 为 192.168.1.1,另外两个端口 IP

分别为 192.168.5.1 和 192.168.6.1，所以应该配置这三个网段。选择：配置->路由配置->RIP，在方框中填入三个 IP 地址对应的网段，点击添加，如图 1-18，成功添加了三个网段，该路由器 RIP 协议配置成功。



图 1-18 RIP 协议配置 IP 网段

其他三个路由器的配置与之相似，只需要改变网段的 IP 即可。

e) 配置 PC 机 IP 地址和网关 pc1-pc4 分别处于 192.168.1.0、192.168.2.0、192.168.3.0、192.168.4.0 网段，可将其 IP 地址分别设置为 192.168.1.2、192.168.2.2、192.168.3.2、192.168.4.2。每台 pc 的网关都应该是与它距离最近的路由器的 IP 端口的地址，设为 192.168.1.1、192.168.2.1、192.168.3.1、192.168.4.1，这分别是路由器 A、B、C、D 的 fa0/0 端口地址。

f) 连通性测试

任选两台 PC 机相互通信，如图 1-19，pc1 与 pc2，pc2 与 pc3，pc3 与 pc4，pc4 与 pc1，均可进行访问（第一次访问请求可能失败，只要第二次访问成功，就说明两台 pc 可以进行访问），符合实验预期。

PDU列表窗口										
激活	最后状态	来源设备	目的设备	类型	颜色	时间(秒)	固定周期	顺序	编辑	删除
	失败	PC1	PC2	ICMP		0.000	N	0	(编辑)	(删除)
	成功	PC1	PC2	ICMP		0.000	N	1	(编辑)	(删除)
	失败	PC2	PC3	ICMP		0.000	N	2	(编辑)	(删除)
	成功	PC2	PC3	ICMP		0.000	N	3	(编辑)	(删除)
	失败	PC3	PC4	ICMP		0.000	N	4	(编辑)	(删除)
	成功	PC3	PC4	ICMP		0.000	N	5	(编辑)	(删除)
	成功	PC4	PC1	ICMP		0.000	N	6	(编辑)	(删除)

图 1-19 RIP 协议连通性测试



### 3) 基本内容 2

a) 除配置路由 OSPF 协议与 RIP 协议不同外, 其他配置均与 RIP 协议相同, 因此这里只给出配置 OSPF 协议的过程。

b) OSPF 协议是区别于 RIP 协议的另一种选路协议, 同样可以用于以太网的通信, 我们采用命令行来为路由器配置 OSPF 协议。以路由器 A 为例, 如图 1-20, 任选一个数字作为进程号, 为路由器配置 OSPF, network 开头的命令将路由器端口的 IP 地址和子网掩码绑定到路由器上。该路由器有三个端口, 所以使用了三条这样的语句。配置完成后, 用 copy run startup 语句建立配置。

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#network 192.168.5.0 0.0.0.255 area 0
Router(config-router)#network 192.168.6.0 0.0.0.255 area 0
Router(config-router)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#copy run startup
Destination filename [startup-config]?
Building configuration...
[OK]
```

图 1-20 OSPF 协议配置

其他三个路由器的配置与之相似, 只需要改变进程号和端口 ip。

### d) 连通性测试

为了验证前面配置的 OSPF 协议是否有效, 需要测试各个 PC 间的连通性。如果配置成功, 那么 PC 之间应该和 RIP 协议配置完成以后一样可以任意通信。如图 1-21, pc1 对 pc2, pc2 对 pc3, pc3 对 pc4, pc4 对 pc1 都可以进行访问, 所以我们可以认为, 网络中的任意两台 pc 都可以互相访问, OSPF 协议配置成功。

PDU列表窗口										
激活	最后状态	来源设备	目的设备	类型	颜色	时间(秒)	固定周期	顺序	编辑	删除
	成功	PC1	PC2	ICMP		0.000	N	0	(编辑)	(删除)
	失败	PC2	PC3	ICMP		0.000	N	1	(编辑)	(删除)
	成功	PC2	PC3	ICMP		0.000	N	2	(编辑)	(删除)
	失败	PC3	PC4	ICMP		0.000	N	3	(编辑)	(删除)
	成功	PC3	PC4	ICMP		0.000	N	4	(编辑)	(删除)
	成功	PC4	PC1	ICMP		0.000	N	5	(编辑)	(删除)

图 1-21 OSPF 协议连通性测试

### 4) 基本内容 3

#### a) 路由器访问控制列表配置

用命令行对路由器 A 进行配置。要使得 pc1 无法访问其他网段, 而且不能被其他网段访问, 应该在路由器 A 与交换机 switch1 相连的端口进行配置。先用 access-list 命令创建访问控制列表, deny 表示屏蔽某网段的消息, permit 表示接受某网段的消息, 这里使用了 deny, 因为我们要屏蔽 pc1 的通信。命令中的 ip 地址是要屏蔽或接受的网段, 最后一个参数是子网掩码的反码。创建 acl 完成, 打开端口 fa0/0, 用 access-group 命令把 acl 绑定到路由器上, acl 就配置完成了, 如图 1-22。



```

!
access-list 101 deny ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.255.255
access-list 101 deny ip 192.168.0.0 0.0.255.255 192.168.1.0 0.0.0.255
access-list 101 deny ip 192.168.0.0 0.0.255.255 host 192.168.1.1
access-list 101 permit ip any any
!

```

图 1-22 路由器 A 访问控制表 1

#### b) 连通性测试

如图 1-23 所示，pc1 向其他三个 pc 的访问请求都发送失败，其他三个 pc 对 pc1 的访问也发送失败。

PDU列表窗口										
激活	最后状态	来源设备	目的设备	类型	颜色	时间(秒)	固定周期	顺序	编辑	删除
	失败	PC1	PC2	ICMP		0.000	N	0	(编辑)	(删除)
	失败	PC1	PC3	ICMP		0.000	N	1	(编辑)	(删除)
	失败	PC1	PC4	ICMP		0.000	N	2	(编辑)	(删除)
	失败	PC4	PC1	ICMP		0.000	N	3	(编辑)	(删除)
	失败	PC3	PC1	ICMP		0.000	N	4	(编辑)	(删除)
	失败	PC2	PC1	ICMP		0.000	N	5	(编辑)	(删除)

图 1-23 连通性测试 1

#### c) 重新配置 ACL

pc1 不能访问 pc2，但能访问其他 pc。第一次配置 acl 使只使用了 deny 指令，所以只能屏蔽作用，这里既需要屏蔽一部分消息，又需要允许一部分消息通过，所以还要使用 permit 指令。

仍然对路由器 A 进行配置，如图 1-24。首先 deny 来自 pc2，也就是 192.168.2.0 网段的信息，然后 permit 其他任何信息，acl 列表就创建好了，然后绑定到端口 fa0/0 上。

```

access-list 101 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
access-list 101 permit ip any any
!

```

图 1-24 路由器 A 访问控制表 2

#### d) 连通性测试

尝试让 pc1 与 pc2 互相通信，如图 1-25，通信全都失败。

PDU列表窗口										
激活	最后状态	来源设备	目的设备	类型	颜色	时间(秒)	固定周期	顺序	编辑	删除
	失败	PC1	PC2	ICMP		0.000	N	0	(编辑)	(删除)
	失败	PC1	PC2	ICMP		0.000	N	1	(编辑)	(删除)
	失败	PC2	PC1	ICMP		0.000	N	2	(编辑)	(删除)
	失败	PC2	PC1	ICMP		0.000	N	3	(编辑)	(删除)

图 1-25 连通性测试 2

pc1 访问 pc2 以外的主机，pc2 访问 pc1 以外的主机，都能访问成功，如图 1-26。

PDU列表窗口										
激活	最后状态	来源设备	目的设备	类型	颜色	时间(秒)	固定周期	顺序	编辑	删除
	成功	PC1	PC3	ICMP		0.000	N	0	(编辑)	(删除)
	成功	PC1	PC4	ICMP		0.000	N	1	(编辑)	(删除)
	成功	PC2	PC3	ICMP		0.000	N	2	(编辑)	(删除)
	成功	PC2	PC4	ICMP		0.000	N	3	(编辑)	(删除)

图 1-26 连通性测试 3

### 5) 结果分析

a) 从上述实验结果可以看出，我们用两种路由选择协议实现了网络通信，虽然配置的方法不同，但是达到了相同的目的。由于我们实验中只能模拟小型网络，所以看不出两者的区别，其实 RIP 和 OSPF 是有很大差异的。

b) RIP 协议是一种传统的路由协议，适合比较小型的网络，但是网络的迅速发展和急剧膨胀使 RIP 协议无法适应今天的网络。OSPF 协议则是在网络急剧膨胀的时候制定出来的，它克服了 RIP 协议的许多缺陷。RIP 是距离矢量路由协议；OSPF 是链路状态路由协议。RIP 会定时广播路由表，而 OSPF 只有在路由状态发生变化时才广播路由表……两者的差异远不止这些，在实验中只做初步了解，还需要以后继续深入学习才能理解透彻。

c) Acl 是访问控制列表 Access Control List 的英文缩写，用于控制路由器和交换机进出端口的数据包。在路由器 A 的端口上 deny 掉 pc1 所在网段的消息，路由器就会过滤掉与 pc1 有关的所有消息，使之无法与外界进行通信；若既要过滤部分消息，又要选通部分消息，则需要 deny 和 permit 指令的结合，就像进阶部分所做的一样。

## 1.4 综合部分实验设计、实验步骤及结果分析

### 1.4.1 实验设计

#### 1) 分配子网

当学校申请了前缀为 211.69.4.0/22 的地址块后，可以依据优先分配子网主机多的网段的规则，按照以下步骤进行分配：

学生宿舍 1：我们选择 211.69.4.0/24 作为学生宿舍 1 的子网。这个子网包含了从 211.69.4.0 到 211.69.4.255 共 256 个 IP 地址，其中 211.69.4.0 是网络地址，211.69.4.255 是广播地址。

学生宿舍 2：下一个可用的子网是 211.69.5.0/24，包含了从 211.69.5.0 到 211.69.5.255 共 256 个 IP 地址，其中 211.69.5.0 是网络地址，211.69.5.255 是广播地址。

学生宿舍 3：下一个可用的子网是 211.69.6.0/24，包含了从 211.69.6.0 到 211.69.6.255 共 256 个 IP 地址，其中 211.69.6.0 是网络地址，211.69.6.255 是广播地址。

图书馆：下一个可用的子网是 211.69.7.0/25，包含了从 211.69.7.0 到 211.69.7.127 共 128 个 IP 地址，其中 211.69.7.0 是网络地址，211.69.7.127 是广播地址。

学院 1：下一个可用的子网是 211.69.7.128/27，包含了从 211.69.7.128 到 211.69.7.159 共 32 个 IP 地址，其中 211.69.7.128 是网络地址，211.69.7.159 是广播地

址。

学院 2：下一个可用的子网是 211.69.7.160/27，包含了从 211.69.7.160 到 211.69.7.191 共 32 个 IP 地址，其中 211.69.7.160 是网络地址，211.69.7.191 是广播地址。

学院 3：下一个可用的子网是 211.69.7.192/27，包含了从 211.69.7.192 到 211.69.7.223 共 32 个 IP 地址，其中 211.69.7.192 是网络地址，211.69.7.223 是广播地址。

学院 4：下一个可用的子网是 211.69.7.224/27，包含了从 211.69.7.224 到 211.69.7.255 共 32 个 IP 地址，其中 211.69.7.224 是网络地址，211.69.7.255 是广播地址。

通过这个地址分配方案，每个 IP 地址范围的最后一个地址是广播地址，第一个地址是网络地址，不能用于分配给主机使用。剩余的地址可供设备使用。这个分配方案可以满足学校的需求，并提供了足够的 IP 地址给学生宿舍、图书馆和学院使用。

## 2) 网络拓扑设计

a) 从理论上来说，只需要一个路由器就可以解决全校的通信问题，所有的交换机之间也不需要相连，直接往路由器上连接即可。但是我们要充分结合实际，以我校的通信系统为例，所有宿舍楼、学院都应有自己的路由器，即便没有，也会与临近的宿舍或学院共享一台路由器，绝不会全校使用一台，因为这样更便于管理，更方便维修。

b) 网络拓扑图的大致结构是：图书馆和四个学院共用一台路由器、三个宿舍共用一台路由器。每 23 台主机共用一台交换机（因为一台交换机最多只有 24 个接口），宿舍的交换机直接连接在路由器上，而学院间的交换机互相连接，保证每台交换机都是可达的，最终通过一台交换机与路由器相连。图书馆要求无线上网，所以既有无线上网的笔记本，也有有线上网的 pc 机，此外还有一台无线路由器。全校的两台路由器直接相连接。

c) 每个网段只连接第一台和最后一台主机，中间的其余主机省略，这不影响系统功能的实现。最终绘制的网络拓扑图如图 1-27 所示。

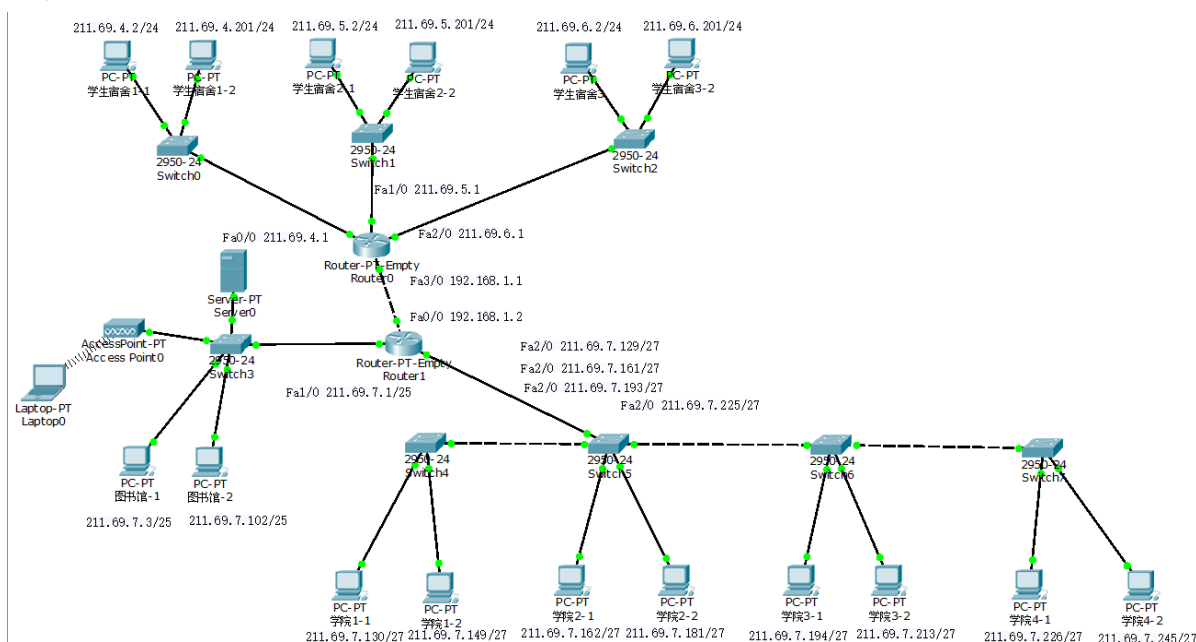


图 1-27 学校组网拓扑图

## 3) 功能设计

a) 四个学院是相对独立的子网，三个宿舍也是相对独立的子网，然而他们连接在路由器的同一个端口上，所以需要对路由器分配子端口。各学院之间要能够通信，所以还需要划分成功四个 vlan，同理三个宿舍也要划分 vlan。

b) 学院和宿舍要跨过路由器访问图书馆，需要在路由器上配置 RIP 协议或者 OSPF 协议进行选路。

c) 要禁止学院和宿舍互相访问，需要进行 ACL 配置。

#### 1.4.2 实验步骤

##### 1) 交换机配置

宿舍的每台交换机彼此并不相互连接，而是直接连接在路由器上，因此不需要手动划分 vlan。

学院的每台交换机都增加三个 vlan，分别编号为 2、3、4，加上默认的 vlan1 对应四个学院。将交换机之间、交换机与路由器之间的链路设为 trunk 链路，交换机与 pc 机之间的链路设为 access 链路，vlan 设为该 pc 机对应的学院的 vlan，这样，就把四个学院分成了 4 个 vlan。

图书馆不需要划分 vlan。

##### 2) 路由器接口配置

a) 路由器之间相连的接口 IP 使用 192.168.xxx.xxx 系列，不能使用 211.69.xx.xx 系列，否则会与学校的 pc 机 IP 相冲突。

b) 宿舍路由器 Router0 添加两个接口，一共有四个接口，三个接口分别与三个宿舍的网段相连接，并配置对应的网关地址，第四个接口用于连接路由器。学院和图书馆的路由器 Router1，添加一个接口，一共有三个接口，分别用于连接宿舍路由器，图书馆网段和学院网段，图书馆网段和学院网段共用一个网关地址。

d) 路由器使用 RIP 路由协议，需要在其中添加连接的网段的网络，以及两个路由器的端口地址的网络地址 192.168.1.0，如图 1-28 和 1-29。

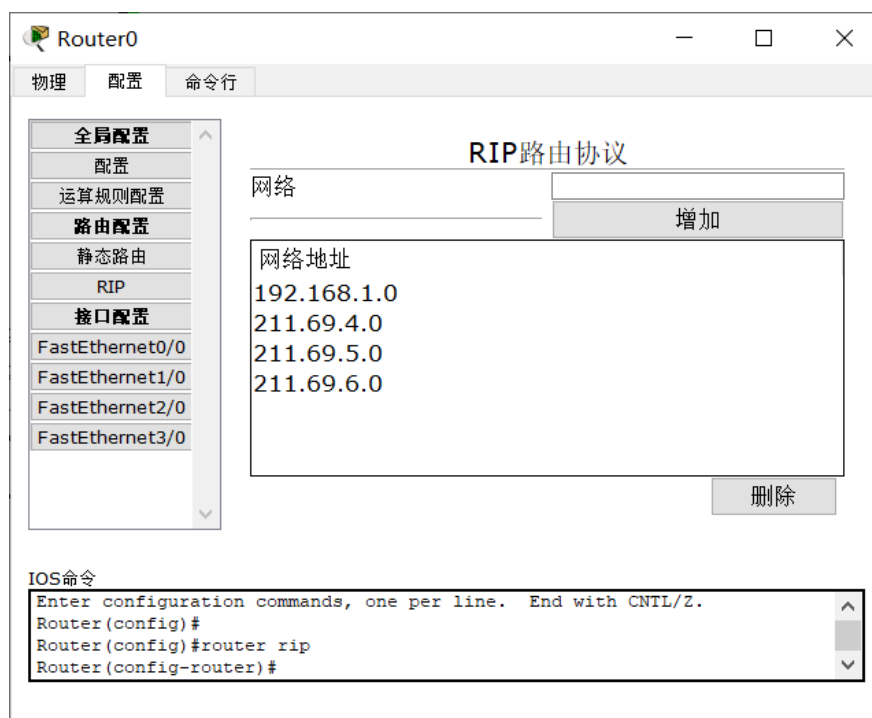


图 1-28 Router0 RIP 配置

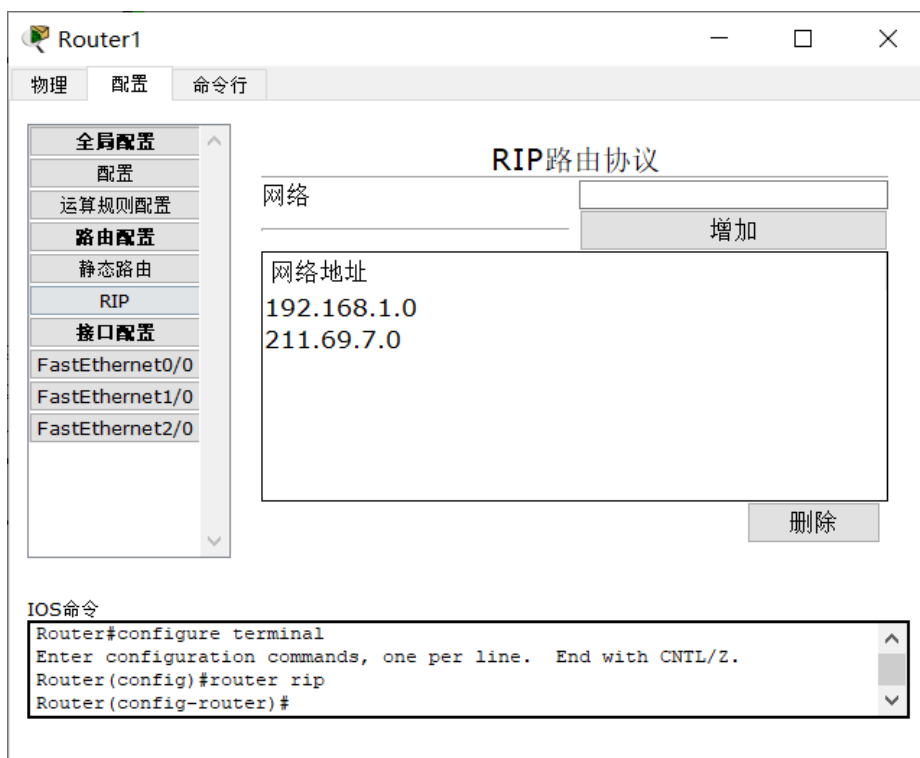


图 1-29 Router1 RIP 配置

### 3) 无线路由器

选择无线设备中的第一个 AccessPoint-PT，使用默认配置即可，如图 1-30。



图 1-30 无线路由器

### 4) 笔记本

图书馆的无线上网功能可以用 pc 机或者笔记本实现，无论哪种电脑，都是默认安装有线网卡，所以我们要对其改装。如图 1-31，将笔记本断电，把有线网卡拖下，从左侧的模块列表中选择第一个“Linksys-WPC300N”，拖到笔记本上，然后再开电，无线网卡就装上了，它会自动连接到无线路由器，并且路由器会给它分配 IP。



图 1-31 笔记本

#### 5) PC 机 IP 地址配置

对于除了笔记本以外的其他电脑，可以将 IP 地址设置为其所在网段的任意值，只要不重复即可。此处将每个网段中示例的两台 pc 机设置为网段的第一台 pc 和最后一台 pc 的 ip 地址，网关设置为网段的第一个 ip 地址。

#### 6) 路由器 ACL 配置

实验要求学院和宿舍不能互访，但是他们都可以访问图书馆，所以需要在学院和宿舍的路由器之间屏蔽掉对方的信号，如图 1-32 和 1-33。

```
!
access-list 101 deny ip 211.69.7.128 0.0.0.127 211.69.4.0 0.0.0.255
access-list 101 deny ip 211.69.7.128 0.0.0.127 211.69.5.0 0.0.0.255
access-list 101 deny ip 211.69.7.128 0.0.0.127 211.69.6.0 0.0.0.255
access-list 101 permit ip any any
.
```

图 1-32 Router0 访问控制表

```
:
access-list 102 deny ip 211.69.4.0 0.0.0.255 211.69.7.128 0.0.0.127
access-list 102 deny ip 211.69.5.0 0.0.0.255 211.69.7.128 0.0.0.127
access-list 102 deny ip 211.69.6.0 0.0.0.255 211.69.7.128 0.0.0.127
access-list 102 permit ip any any
access-list 1 deny 211.69.6.0 0.0.0.255
access-list 1 deny 211.69.5.0 0.0.0.255
access-list 1 deny 211.69.4.0 0.0.0.255
access-list 1 permit any
|
```

图 1-32 Router1 访问控制表



### 1.4.3 结果分析

1) 如图 1-33 和图 1-34 所示, 测试学校各个部门内部的访问权限。四个学院内部、三个宿舍内部和图书馆内部的主机都能互相访问。

	成功	学院1-1	学院1-2	ICMP		0.000	N	0	(编辑)	(删除)
	成功	学院1-1	学院2-1	ICMP		0.000	N	1	(编辑)	(删除)
	成功	学院1-1	学院3-1	ICMP		0.000	N	2	(编辑)	(删除)
	成功	学院1-2	学院3-2	ICMP		0.000	N	3	(编辑)	(删除)
	成功	学院2-1	学院4-1	ICMP		0.000	N	4	(编辑)	(删除)
	成功	学院3-1	学院2-2	ICMP		0.000	N	5	(编辑)	(删除)
	成功	学院4-2	学院3-1	ICMP		0.000	N	6	(编辑)	(删除)
	成功	学院4-2	学院1-2	ICMP		0.000	N	7	(编辑)	(删除)

图 1-33 连通性测试 1

	成功	学生宿舍1-1	学生宿舍2-1	ICMP		0.000	N	0	(编辑)	(删除)
	成功	学生宿舍1-2	学生宿舍2-2	ICMP		0.000	N	1	(编辑)	(删除)
	成功	学生宿舍2-1	学生宿舍3	ICMP		0.000	N	2	(编辑)	(删除)
	成功	学生宿舍2-2	学生宿舍3-2	ICMP		0.000	N	3	(编辑)	(删除)
	成功	学生宿舍3	学生宿舍2-2	ICMP		0.000	N	4	(编辑)	(删除)
	成功	学生宿舍2-2	学生宿舍1-1	ICMP		0.000	N	5	(编辑)	(删除)
	成功	学生宿舍3-2	学生宿舍1-1	ICMP		0.000	N	6	(编辑)	(删除)
	成功	图书馆-1	图书馆-2	ICMP		0.000	N	7	(编辑)	(删除)

图 1-34 连通性测试 2

2) 如图 1-35, 学院和宿舍的主机都可访问图书馆, 而且图书馆的有限设备和无线设备都能被访问。

	成功	学生宿舍1-1	Laptop0	ICMP		0.000	N	0	(编辑)	(删除)
	成功	学生宿舍1-1	图书馆-1	ICMP		0.000	N	1	(编辑)	(删除)
	成功	学生宿舍3-2	Laptop0	ICMP		0.000	N	2	(编辑)	(删除)
	成功	学生宿舍3-2	图书馆-2	ICMP		0.000	N	3	(编辑)	(删除)
	成功	学院1-1	图书馆-1	ICMP		0.000	N	4	(编辑)	(删除)
	成功	学院1-1	Laptop0	ICMP		0.000	N	5	(编辑)	(删除)
	成功	学院3-2	图书馆-2	ICMP		0.000	N	6	(编辑)	(删除)
	成功	学院3-2	Laptop0	ICMP		0.000	N	7	(编辑)	(删除)

图 1-35 连通性测试 3

3) 如图 1-36, 学院和宿舍之间互访失败。

















	失败	学生宿舍1-1	学院1-2	ICMP		0.000	N	0	(编辑)	(删除)
	失败	学生宿舍2-1	学院2-2	ICMP		0.000	N	1	(编辑)	(删除)
	失败	学生宿舍3-2	学院3-1	ICMP		0.000	N	2	(编辑)	(删除)
	失败	学生宿舍2-2	学院2-1	ICMP		0.000	N	3	(编辑)	(删除)
	失败	学院2-1	学生宿舍2-1	ICMP		0.000	N	4	(编辑)	(删除)
	失败	学院1-2	学生宿舍2-2	ICMP		0.000	N	5	(编辑)	(删除)
	失败	学院4-1	学生宿舍3	ICMP		0.000	N	6	(编辑)	(删除)
	失败	学院4-2	学生宿舍3-2	ICMP		0.000	N	7	(编辑)	(删除)

图 1-36 连通性测试 4



---

## 心得体会与建议

### 2.1 心得体会

在完成计算机网络与通信实验课程的过程中，我学到了许多关于网络通信和数据传输的知识，并且通过实际动手操作，加深了对这些概念和技术的理解。以下是我在实验中的一些心得体会：

**Socket 编程：**通过 Socket 编程，我学会了如何使用套接字进行网络通信。这对于实现客户端和服务端之间的数据传输非常重要。我了解了套接字的基本概念、创建和绑定套接字以及使用套接字进行数据发送和接收的方法。

**可靠数据传输协议设计：**在实验中，我实现了基于 GBN (Go-Back-N) 和 SR (Selective Repeat) 的可靠传输协议。通过这些实现，我深入了解了可靠数据传输的原理和机制，如序号管理、确认和重传等。我通过编写代码实现了这些协议，并进行了测试和验证，进一步加深了对它们的理解。

**简化版 TCP 的实现：**基于 GBN 协议和 TCP 的可靠数据传输机制，我实现了一个简化版的 TCP。这个实验对我来说是一个挑战，因为 TCP 协议的可靠性和拥塞控制等方面涉及到许多复杂的概念和算法。通过这个实验，我更深入地理解了 TCP 的工作原理，并学会了如何应用这些原理来设计和实现一个可靠的数据传输协议。

**基于 CPT 的组网实验：**在这个实验中，我通过使用 CPT (Cisco Packet Tracer) 软件进行网络拓扑的设计和配置，学习了如何搭建和管理一个计算机网络。我了解了网络设备的配置和连接方法，学会了设置 IP 地址、子网掩码和路由表等网络参数。通过模拟不同网络场景和故障，我深入理解了网络的工作原理和网络故障排除的方法。

总的来说，这门计算机网络与通信实验课程让我对网络通信和数据传输有了更深入的了解。通过实际动手操作和实验实践，我不仅学到了理论知识，还提升了了自己的实践能力和问题解决能力。这些实验心得将对我今后在网络领域的学习和工作中产生积极的影响。

### 2.2 建议

对于计算机网络与通信的实验课程，我有以下几点建议：

1. **强调团队合作：**计算机网络与通信是一个团队合作的领域。建议将一部分实验设计为小组项目，让学生在团队中合作完成。通过团队合作，学生可以学会有效地分工合作、协商解决问题，并培养团队协作和沟通能力。
2. **提供实际案例和应用场景：**为了将课程内容与实际应用联系起来，建议引入实际案例和应用场景。可以通过讲解互联网、移动通信、物联网等领域的实际应用，让学生更好地理解网络技术在现实生活中的应用和意义。
3. **提供额外学习资源：**除了课堂教学和实验指导，建议提供额外的学习资源。可以提供相关的参考书籍、在线教程、学术论文等，供学生进一步深入学习和研究。同时，提供网络模拟器等工具，帮助学生进行实验和调试。

---

通过以上建议,希望这门计算机网络与通信实验课程能够更加有效地培养学生的实践能力和问题解决能力,使他们能够在网络通信领域有所建树。