《计算机网络原理》

实验指导

北京交通大学计算机学院

《计算机网络原理》课程组

二零二二年九月

目录

目录 1

引言 2

实验一 WEB 服务器编程实验..... 4

实验二 SMTP 客户端编程实验..... 13

实验三 可靠数据传输原理（GBN 或 SR）编程实验 15

实验四 编程实现路由算法 17

实验五 交换机 VLAN 实验 18

实验六 RIP 配置实验..... 30

引言

《计算机网络原理》课程是计算机科学与技术专业的重要专业课程之一。计算机网络技术的迅速发展及其在当今信息社会中的广泛应用，给高校《计算机网络原理》课程的教学提出了新的更高的要求。

由于计算机网络是一门实践性较强的技术，课堂教学应该与实践环节紧密结合。近几年，在校、院、系和教研室的大力支持下，我们筹建了《计算机网络原理》的教学实验环境。这个实验环境为同学们提供了基本的网络实验平台，达到了高等院校和科研机构的计算机网络基本水平。在这样的硬件环境下，我们配合本科网络系列课程教学，编写了配套实验指示书，加大了本科网络系列课程教学的实践力度。希望同学们能够充分利用实验条件，认真完成实验，从实验中得到应有的锻炼和收获。

1，计算机网络实验的特点

计算机网络实验的对象和环境是一个计算机网络系统，它由若干台主机通过接口电路（网卡），Modem，网络传输介质和网络互联设备（Hub,交换机，路由器，…）等构成计算机网络的硬件环境，由运行在各主机上的网络操作系统，网络数据库系统，网络管理系统，应用系统以及网络互联设备上的网络软件构成的软件环境，硬件环境与软件环境的有机结合构成计算机网络系统，从而实现计算机网络的各种功能和服务。每个实验都是在计算机网络系统环境下才能顺利进行。

本实验指导书中的实验主要分为四大类：验证型实验、设计型实验、综合型实验和创新型实验，验证型实验主要训练学生的基本技能，设计型实验要求学生运用所学知识自行设计，并加以实现。综合型实验体现知识、能力、素质培养的综合性，创新型实验主要培养学生独立思考、综合运用知识进行创新等适应科研工作的能力。

2，本实验指导书的使用

1）实验预习

因为很多实验需要计算机网络基本知识比较多，预习工作非常重要，是整个实验不可少的一个环节。在这个环节当中，需要明确实验目的，通过阅读相关资料理解并掌握实验原理；熟悉实验的硬件和软件环境。仔细阅读实验指导书中的实验方法和操作步骤，并参阅相关理论知识和有关设备的说明书，写出预习报告。预习报告的内容应该包括：

- 实验目的
- 实验原理
- 实验环境的建立
- 实验步骤和预期的结果
- 对各种可能出现的运行结果进行理论分析

2） 实验操作

进入实验室进行实验操作前，应将实验预习报告交实验指导教师审查，获得实验指导教师的批准后，领取相应实验设备，并进行登记后，才可进行实验操作。

在实验过程中，要认真观察实验现象，详细记录实验结果，若有异常情况，要及时报告实验指导教师，并妥善处理，排除故障后才可继续进行实验。

实验结束前，应经实验指导教师验收并在预习报告上签字后才结束实验。

3） 实验总结

根据实验情况写出实验报告。在实验报告中，应对实验记录进行整理，对实验结果从理

论上加以分析归纳，对实验过程中出现的问题及解决办法进行分析和讨论，以加深对所学理论知识的理解。

希望老师和同学们在使用本实验指示书及进行实验的过程中，能够帮助我们不断地发现问题，并提出建议，以改善计算机网络系列课程的建设。

实验一 WEB 服务器编程实验

实验目的：

运用各种语言实现 WEB 服务器软件，要求：

（1） 处理一个 http 请求

（2） 接收并解析 http 请求

（3） 从服务器文件系统中获得被请求的文件

（4） 创建一个包括被请求的文件的 http 响应信息

（5） 直接发送该信息到客户端

实验意义：

通过本实验，使学生能够进一步理解 HTTP 协议的技术细节以及 WEB 服务器的实现原理。

实验背景：

HTTP 的英文全称是：**H**yper**T**ext **T**ransport **P**rotocol，即超文本传输协议，HTTP 是一个属于应用层的协议，由于其简捷、快速的方式，适用于分布式超媒体信息系统。它于 1990 年提出，经过几年的使用与发展，得到不断地完善和扩展。

HTTP 协议的运作方式:

HTTP 协议是基于请求／响应模式的。一个客户机与服务器建立连接后，发送一个请求给服务器，请求方式的格式为，统一资源标识符、协议版本号，后边是 MIME 信息，包括请求修饰符、客户机信息和可能的内容。服务器接到请求后，给予相应的响应信息，其格式为一个状态行，包括信息的协议版本号、一个成功或错误的代码，后边是 MIME 信息包括服务器信息、实体信息和可能的内容。最简单的情况可能是在用户代理(UA)和源服务器(O)之间通过一个单独的连接来完成(见图 1.1)。

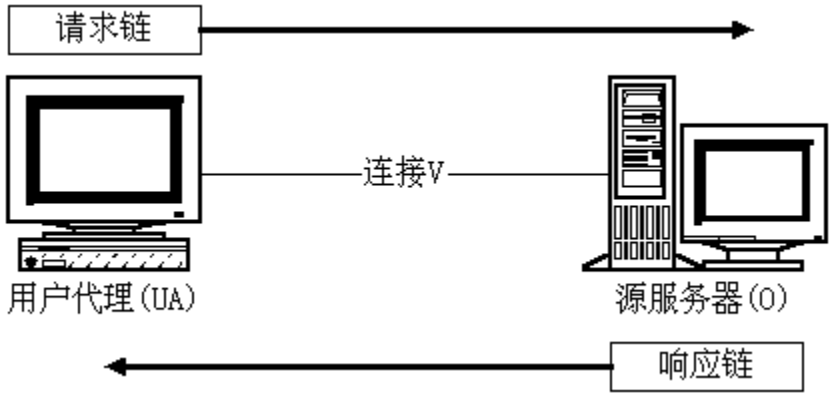


图 1.1 http 协议的通讯

在 Internet 上，HTTP 通讯通常发生在 TCP/IP 连接之上。缺省端口是 TCP 80，但其它的端口也是可用的。

HTTP 协议的内部操作过程:

基于 HTTP 协议的客户/服务器模式的信息交换过程如图 1.2 所示，它分四个过

程，建立连接、发送请求信息、发送响应信息、关闭连接。

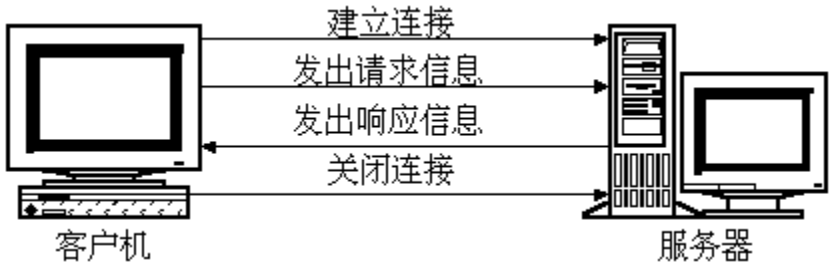


图 1.2 基于 HTTP 协议的客户/服务器模式的信息交换过程

在 WWW 中，“客户”与“服务器”是一个相对的概念，只存在于一个特定的连接期间，即在某个连接中的客户在另一个连接中可能作为服务器。WWW 服务器运行时，一直在 TCP80 端口(WWW 的缺省端口)监听，等待连接的出现。

HTTP 协议下客户/服务器模式中信息交换的实现:

1.建立连接

连接的建立是通过申请套接字(Socket)实现的。客户打开一个套接字并把它约束在一个端口上，如果成功，就相当于建立了一个虚拟文件。以后就可以在该虚拟文件上写数据并通过网络向外传送。

2.发送请求

打开一个连接后，客户机把请求消息送到服务器的停留端口上，完成提出请求动作。

HTTP/1.0　　请求消息的格式为：

request-line （请求行）

headers (0或有多个) (请求头)

<blank line>

body　(只对P O S T请求有效)

请求消息=请求行(通用信息|请求头|实体头) CRLF[实体内容]

请求行=方法　请求 URL　HTTP 版本号　CRLF

方法=GET|HEAD|POST|扩展方法

URL=协议名称+宿主名+目录与文件名

请求行中的方法描述指定资源中应该执行的动作，常用的方法有 GET、HEAD 和 POST。

HEAD——要求服务器查找某对象的元信息，而不是对象本身。

POST——从客户机向服务器传送数据，在要求服务器和 CGI 做进一步处理时会用到 POST 方法。POST 主要用于发送 HTML 文本中 FORM 的内容，让 CGI 程序处理。

一个请求的例子为：

GET http://www.njtu.edu.cn/xyjj.htm HTTP/1.0

头信息又称为元信息，即信息的信息，利用元信息可以实现有条件的请求或应答 。

请求头——告诉服务器怎样解释本次请求，主要包括用户可以接受的数据类型、压缩方法和语言等。

实体头——实体信息类型、长度、压缩方法、最后一次修改时间、数据有效期等。

实体——请求或应答对象本身。

3.发送响应

服务器在处理完客户的请求之后，要向客户机发送响应消息。

HTTP/1.0 的响应消息格式如下：

status-line （状态行）

headers (0个或有多个)（响应头）

<blank line>

b o d y

响应消息=状态行(通用信息头|响应头|实体头)　CRLF　〔实体内容〕

状　态　行=HTTP 版本号　状态码　原因叙述

状态码表示响应类型

1××　　保留

2××　　表示请求成功地接收

3××　　为完成请求客户需进一步细化请求

4××　　客户错误

5××　　服务器错误

响应头的信息包括：服务程序名，通知客户请求的 URL 需要认证，请求的资源何时能使用。

4.关闭连接

客户和服务器双方都可以通过关闭套接字来结束 TCP/IP 对话

附：HTTP 协议状态码含义如下表所示：

HTTP 协议状态码的含义

号码 含义

"100" : Continue

"101" : witching Protocols

"200" : OK

"201" : Created

"202" : Accepted

"203" : Non-Authoritative Information

"204" : No Content

"205" : Reset Content

"206" : Partial Content

"300" : Multiple Choices

"301" : Moved Permanently

"302" : Found

"303" : See Other

"304" : Not Modified

"305" : Use Proxy

"307" : Temporary Redirect

"400" : Bad Request

"401" : Unauthorized

"402" : Payment Required

"403" : Forbidden

"404" : Not Found

"405" : Method Not Allowed

"406" : Not Acceptable

"407" : Proxy Authentication Required

"408" : Request Time-out
"409" : Conflict
"410" : Gone
"411" : Length Required
"412" : Precondition Failed
"413" : Request Entity Too Large
"414" : Request-URI Too Large
"415" : Unsupported Media Type
"416" : Requested range not satisfiable
"417" : Expectation Failed
"500" : Internal Server Error
"501" : Not Implemented
"502" : Bad Gateway
"503" : Service Unavailable
"504" : Gateway Time-out
"505" : HTTP Version not supported

实验设备： 台式机两台，一台操作系统为 Windows professional，一台操作系统为 Windows server。

实验学时： 1 学时

实验步骤：

一、本实验学生可以根据情况选择何时语言，需要安装相应的语言环境。JAVA 环境安装过程如下：

1.双击 j2sdk-1_3_0_01-win.exe，开始 Java 2 SDK1.3.0.01 的安装，如图 1.3 所示：

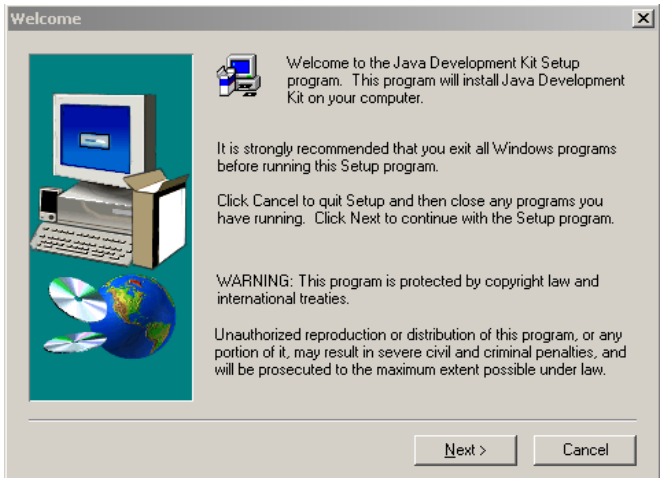


图 1.3

2.单击“next”,进入图 1.4 所示界面：

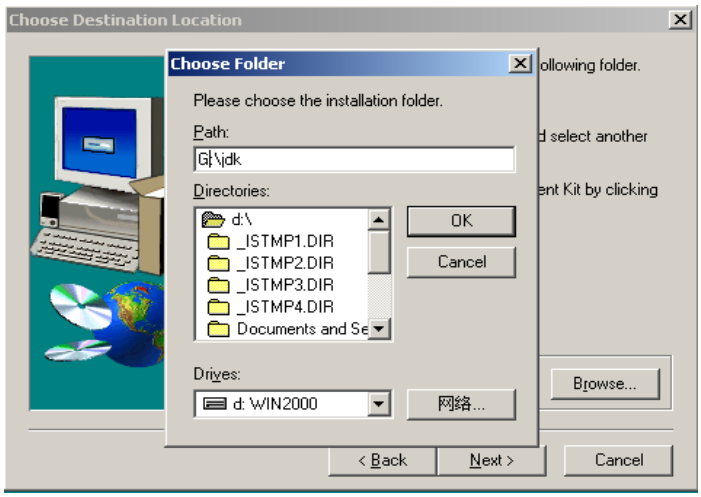


图 1.4

5.单击“OK”,完成安装路径的修改，进入如图 1.5 所示窗口：

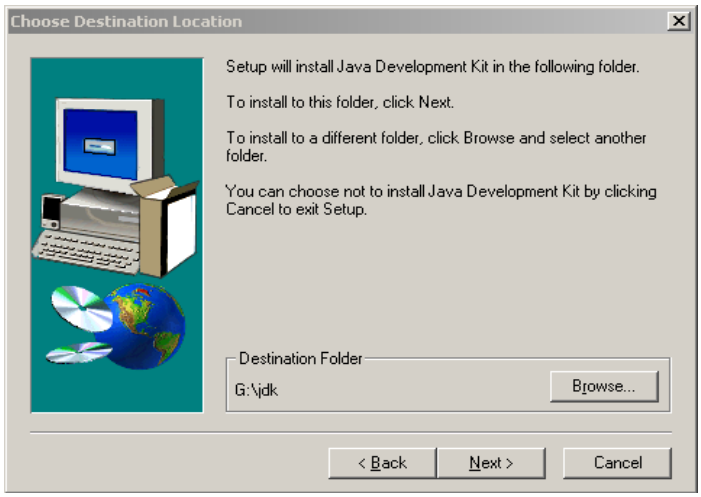


图 1.5

6. 单击“next”,进入图 1.6 所示界面：

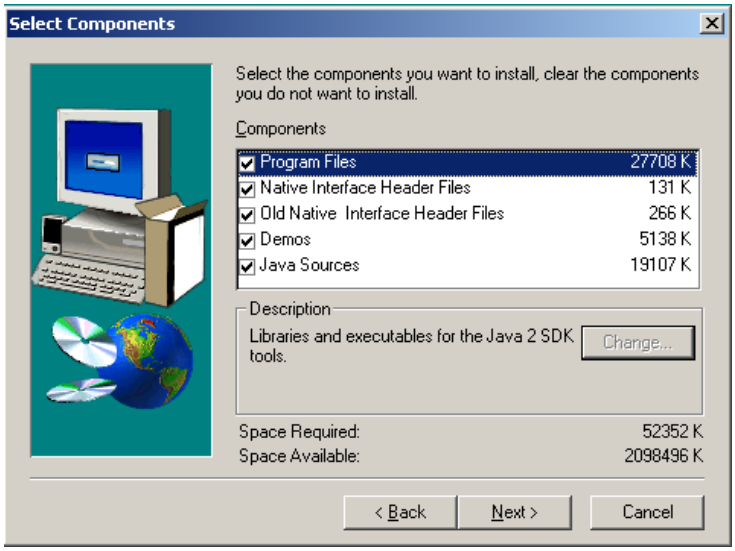


图 1.6

7. 单击“next”,进入图 1.7 所示界面：

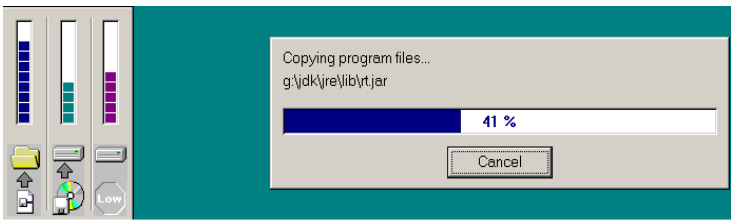


图 1.7

8.安装完成时则出现如图 1.8 所示窗口：

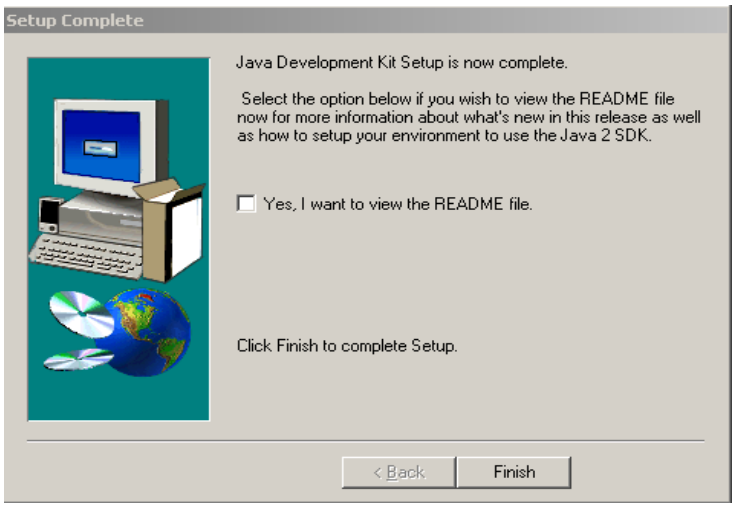


图 1.8

9.单击“Finish”,则完成了 Java 2 SDK1.3.0.01 的安装。

二、Java 2 SDK1.3.0.01 安装完成后，我们将编写 java 程序来实现 web 服务器功能。

我们将代码保存到 I 盘根目录下，文件名为 MultiWebServer.java（注：Java 2 SDK1.3.0.01 为命令行运行方式，要求文件路径中不能出现中文，且路径越短越好），同时为了用 Java 2 SDK1.3.0.01 进行编译及运行，也将其复制到 Java 2 SDK1.3.0.01 的安装文件中，本例的路径为：G:\jdk\bin。

三、运行 Java 2 SDK1.3.0.01 对编写的代码进行编译，过程如下：

1.“开始”—>“附件”—>“命令提示符”，出现如图 1.9 所示窗口：

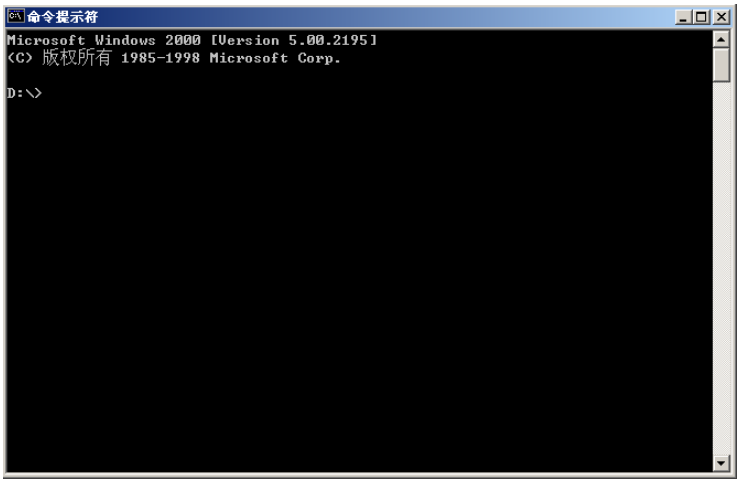


图 1.9

2.在该窗口中敲入如下字符：“G:”，然后回车，则窗口显示为图 1.10：

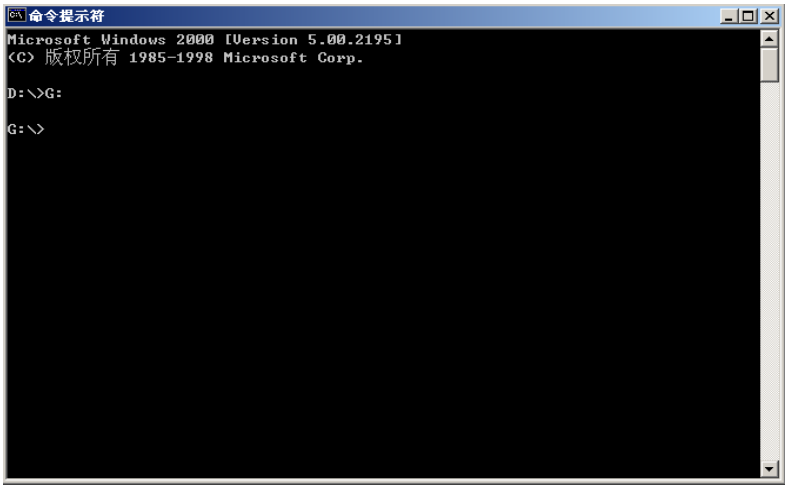


图 1.10

3. 在该窗口中敲入如下字符：“cd jdk”，然后回车，则窗口显示为图 1.11：

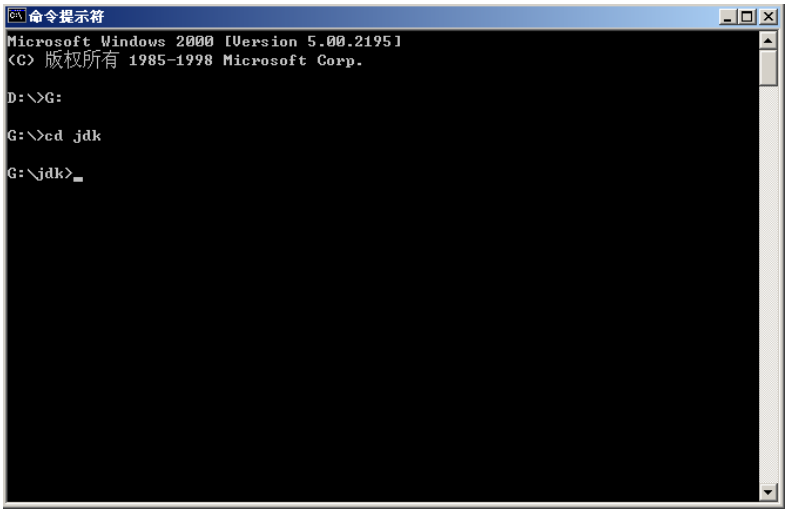


图 1.11

4. 在该窗口中敲入如下字符：“cd bin”，然后回车，则窗口显示为图 1.12：

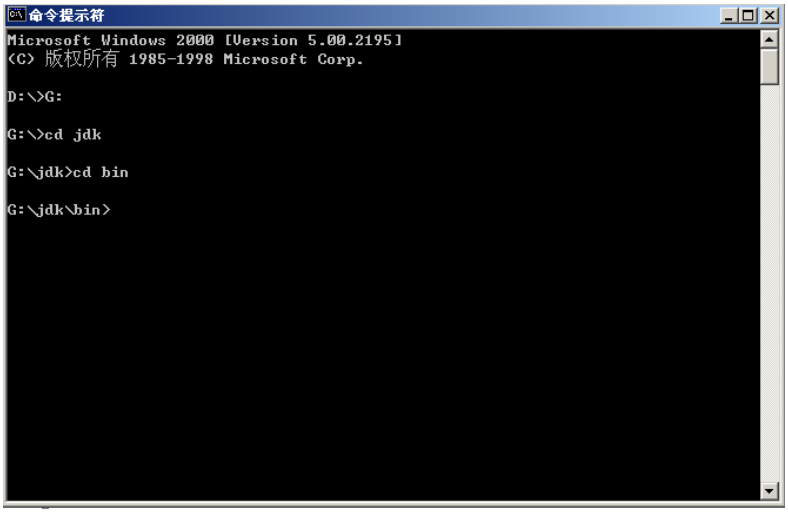


图 1.12

5. 在该窗口中敲入如下字符：“javac MultiWebServer.java”，然后回车，则窗口显示

为图 1.13：

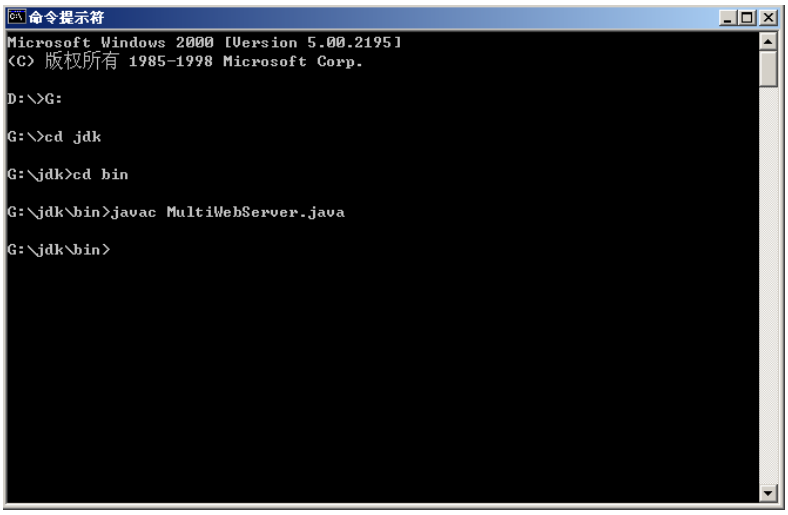


图 1.13

6. 对文件 MultiWebServer.java 编译完毕，生成文件 MultiWebServer.class 及 WebServeOne.class，同时，我们将这两个文件复制到 I 盘根目录下，以备将来运行并验证该服务器用。

四、为了验证 web 服务器能否成功运行，可以用 HTML 语言编写两个 HTML 文件，并制作两个网页。

五、运行并验证：

1.将作好的 HTML 文件 index.html、next.html 以及存放网页中图片的文件夹 images 分别复制到目录 G:\jdk\bin 和 I:。

2. “开始”—>“附件”—>“命令提示符”，重复（3）中 1—4 步，在步骤 4 所示窗口中输入字符“java MultiWebServer”,然后回车，窗口如图 1.14 所示：

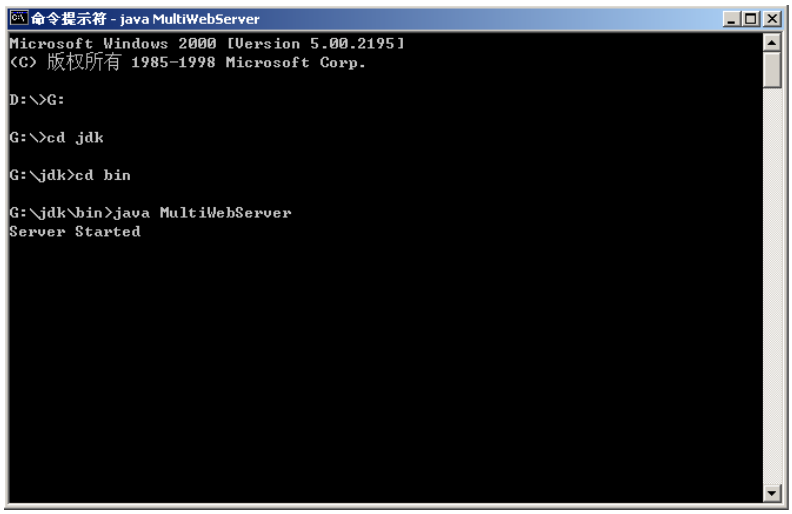


图 1.14

从该窗口中可以看到，web 服务器已经开始运行啦。

3. 如何验证呢？运行 IE 浏览器，在地址栏中输入字符 http://196.168.0.2:8080/I:index.html（设本实验服务器 IP 为 196.168.0.2，在程序中设置的访问端口为 8080），然后回车，可看到所制作的网页，如图 1.15 所示：

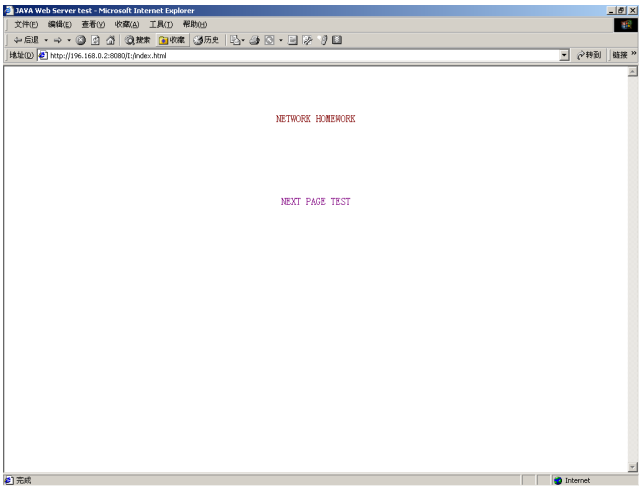


图 1.15

4.单击“NEXT PAGE TEST ”，则可看到我们制作的另一张网页，如图 1.16 所示：

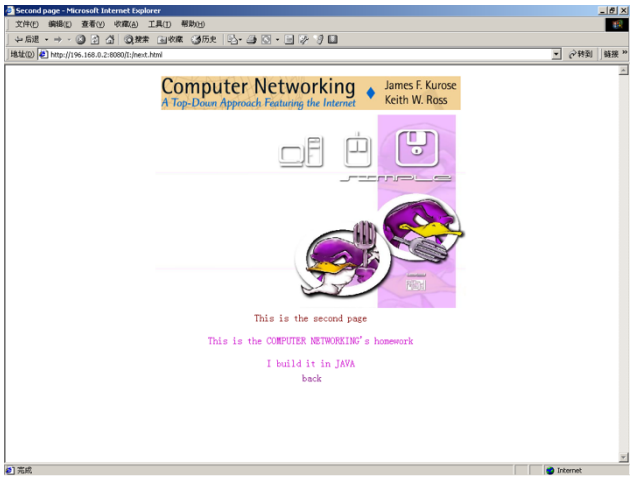


图 1.16

5.单击“back”,则又可以看到步骤 3 中的网页。

6.如果我们输入了错误的地址又该如何呢？如我们在编代码时所考虑到的，此时服务器将产生错误信息，发送给客户端，为了验证这一点，我们在地址栏中输入下列字符 http://196.168.0.2:8080/I:/毕业设计/index.html，看看结果如何？结果如图 1.17 所示：

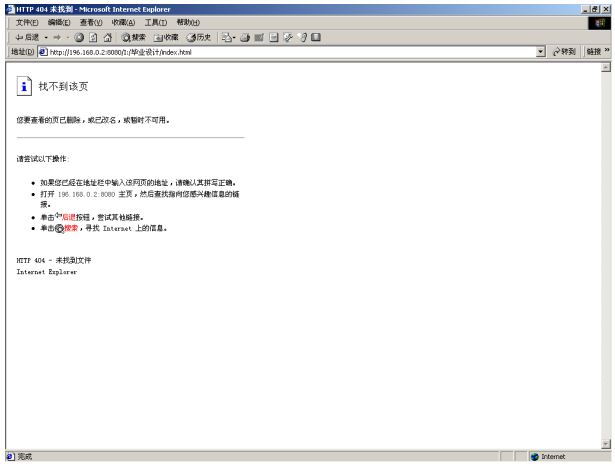


图 1.17

经过运行及验证，该 web 服务器的功能正常。

实验二 SMTP 客户端编程实验

实验目的：

运用各种编程语言实现基于 smtp 协议的 Email 客户端软件。

实验意义：

通过本实验，使学生能够对网络编程有进一步的理解和掌握，并能够理解 smtp 协议的细节。

实验背景：

RFC 821 [Postel 1982] 规范了SMTP协议，指定了在一个简单TCP连接上，两个MTA（报文传送代理 Message Transfer Agent）如何进行通信。RFC 822 [Crocker 1982] 指定了在两个MTA之间用RFC 821 发送的电子邮件报文的格式。图2.1是用T C P / I P交换电子邮件的示意图

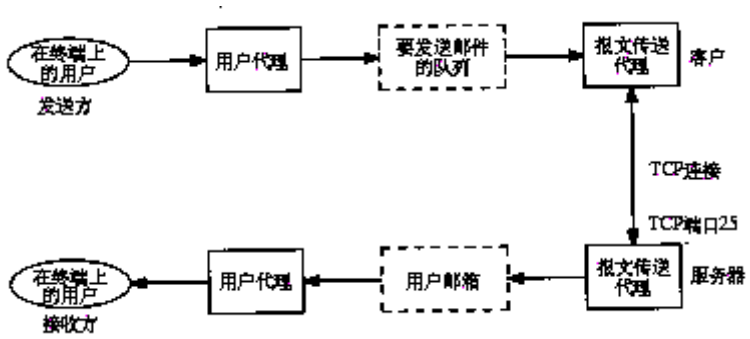


图 2.1 用 T C P / I P 交换电子邮件的示意图

用户与用户代理（user agent）打交道，启动用户代理，键入主题（subject）及报文的正文等。在一行上键入一个句点结束报文。用TCP进行的邮件交换是由报文传送代理MTA（Message Transfer Agent）完成的。用户代理把邮件传给MTA，由MTA进行交付。

最小SMTP实现支持8种命令。

HELO：标识自己。参数必须是完全合格的的客户主机名。

MAIL：标识出报文的发起人。

RCPT：标识接收方。如果有多个接收方，可以发多个RCPT命令。

DATA：发送邮件报文的内容。报文的末尾由客户指定，是只有一个句点的一行。

QUIT：结束邮件的交换。

RSET：异常中止当前的邮件事务并使两端复位。丢掉所有有关发送方、接收方或邮件的存储信息。

VRFY：使客户能够询问发送方以验证接收方地址，而无需向接收方发送邮件。通常是系统管理员在查找邮件交付差错时手工使用的。

NOOP：除了强迫服务器响应一个OK应答码（200）外，不做任何事情。

电子邮件由三部分组成：

1) 信封（envelope）是MTA用来交付的。可由SMTP命令指明，例如：

MAIL From: <xx@computer.njtu.edu.cn>
RCPT To: <estevens@noao.edu>
RFC 821指明了信封的内容及其解释，以及在一个TCP连接上用于交换邮件的协议。
2) 首部由用户代理使用。
首部字段如： Received、Message-Id、From、Data、Reply-To、X-Phone、X-Mailer、To和Subject。每个首部字段都包含一个名，紧跟一个冒号，接着是字段值。RFC 822指明了首部字段的格式的解释（以X-开始的首部字段是用户定义的字段，其他是由RFC 822定义的）。
3) 正文（body）是发送用户发给接收用户报文的内容。RFC 822 指定正文为NVT ASCII文字行。当用DATA命令发送时，先发送首部，紧跟一个空行，然后是正文。用DATA命令发送的各行都必须小于1000字节。

用户代理接收我们指定为正文的部分，加上一些首部字段，并把结果传到MTA。MTA加上一些首部字段，加上信封，并把结果发送到另一个MTA。
内容（content）通常用于描述首部和正文的结合。内容是客户用DATA命令发送的。

实验步骤：

一、选择合适的编程语言编程实现基于 smtp 协议的 Email 客户端软件。

二、安装 Email 服务器或选择已有的 Email 服务器，验证自己的 Email 客户端软件是否能进行正常的 Email 收发功能。

实验三 可靠数据传输原理（GBN 或 SR）编程实验

实验目的：

运用各种编程语言实现基于 Go-Back-N 或 SR 的可靠数据传输软件。

实验意义：

通过本实验，使学生能够对可靠数据传输原理有进一步的理解和掌握。

实验背景：

Go-Back-N 的有限状态机模型表示如图 3.1 所示：

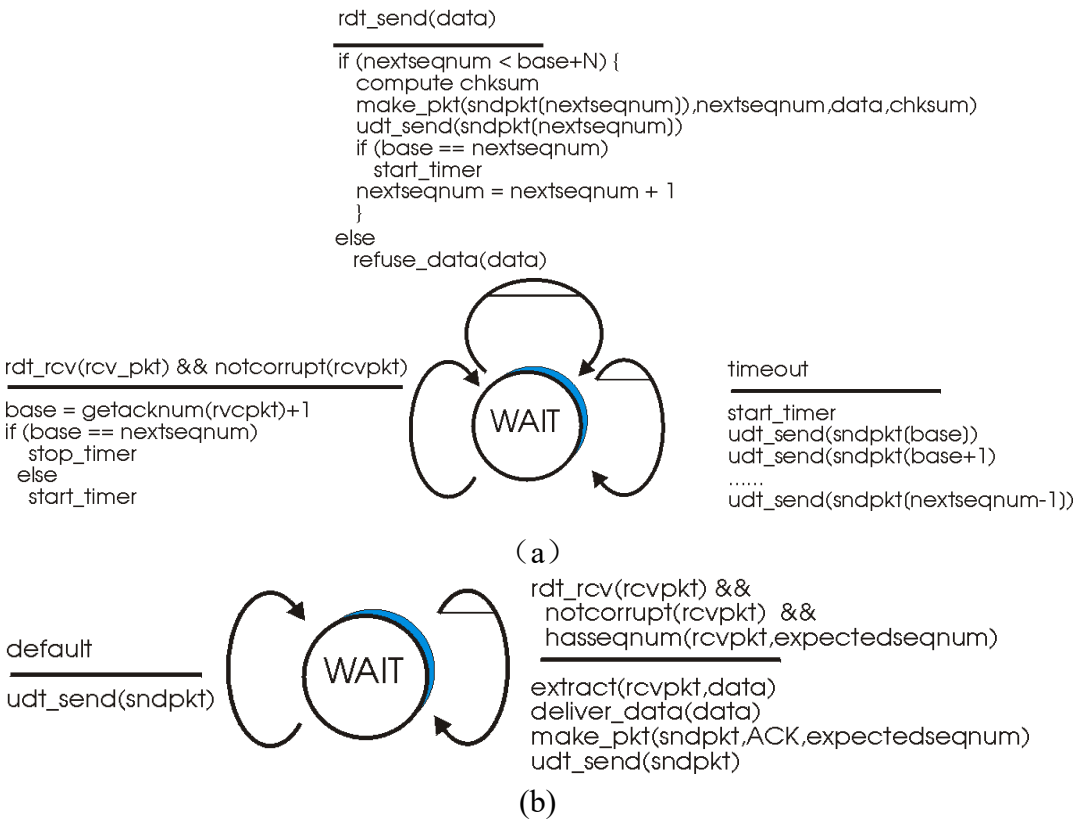


图 3.1 Go-Back-N 的有限状态机模型（a）发送端 (b)接受端

实验步骤：

1，选择合适的编程语言编程实现基于 Go-Back-N 或 SR 的可靠数据传输软件。

2，在实际网络环境或模拟不可靠网络环境中测试和验证自己的可靠数据传

输软件。

实验四 编程实现路由算法

实验目的：

运用各种编程语言实现基于 Dijkstra 算法的路由软件。

实验意义：

通过本实验，使学生能够对路由原理和路由算法有进一步的理解和掌握。

实验背景：

Dijkstra 算法描述如下：

设：

c(i,j): 结点 i 至结点 j 之间链路的代价，若 i,j 不直接相连，则为无穷大。

D(v): 当前从源结点至目的结点 V 之间路由的代价。

p(v): 从源结点至目的结点 V 之间路由中 V 之前的结点

N: 已经知道最优路径的结点集合

```
1 Initialization:
2    N = {A}
3    for all nodes v
4      if v adjacent to A
5        then D(v) = c(A,v)
6        else D(v) = infty
7
8   Loop 9     find w not in N such that D(w) is a minimum
10    add w to N
11    update D(v) for all v adjacent to w and not in N:
12       D(v) = min( D(v), D(w) + c(w,v) )
13    /* new cost to v is either old cost to v or known
14     shortest path cost to w plus cost from w to v */
15  until all nodes in N
```

实验步骤：

1， 选择合适的编程语言编程实现基于 Dijkstra 算法的路由软件。

输入不同的网络拓扑和链路代价测试和验证自己的路由软件。

实验五 交换机 VLAN 实验

实验目的

1. 熟悉 VLAN 的技术背景和原理
2. 熟悉 VLAN 的基本配置方法和配置命令
3. 在交换机上实现 VLAN 的划分

实验意义

通过在实验室搭建 VLAN 实验环境，利用交换机进行 VLAN 配置，使学生进一步熟悉交换机的工作原理和基本配置方法，掌握 VLAN 的划分方法。

实验背景：

VLAN 技术原理

VLAN 技术与局域网息息相关，局域网通常被定义为一个单独的广播域，主要使用 Hub，网桥，或交换机等网络设备连接同一网段内的所有节点，同处于一个局域网之内的网络节点之间可以不通过网络路由器直接通信，而处于不同局域网段之内的设备之间的通信则必须通过网络路由器。

随着网络的不断发展，接入设备的逐渐增多，网络结构日趋复杂，必须使用更多的路由器才能将不同的用户划分到各自不同的广播域中，在不同的局域网中实现网络互连。

这样做的一个缺陷就是随着网络中路由器数量的增多，网络时延逐渐增加，从而导致网络数据传输速率的下降，这主要因为数据在从一处局域网传递到另一处局域网时，必须经过路由器的路由操作，路由器根据数据包中的信息确定数据包的目标地址，然后再选择合适的路径转发出去。

VLAN 又称虚拟局域网，是由位于不同物理局域网段的设备组成。虽然 VLAN 所连接的设备来自不同的网段，但相互之间可以进行直接通信，好象处于同一网段中一样。相比较传统的局域网布局，虚拟局域网更加灵活。为了创建虚拟网络，必须对已有网络拓扑结构进行相应调整。

VLAN 结构如图 5.0 所示。

VLAN 优点：

- 控制网络广播风暴：采用 VLAN 技术，可以将某个交换端口划到某个 VLAN 中，而一个 VLAN 的广播风暴不会影响其他 VLAN 的性能。
- 确保网络安全：共享式局域网之所以很难保证网络安全性，是因为只要用户插入一个活动端口，就能访问网络。而 VLAN 能控制个别用户的访问，控制广播组的大小和位置，甚至能锁定某个设备的 MAC 地址，因此 VLAN 能确保网络的安全性。
- 简化网络管理：网络管理员能借助 VLAN 技术轻松管理整个网络，例如需要为某个项目建立一个工作组网络，其成员可能遍及全国或全世界，而管理员只需几条命令就能在几分钟内建立该项目的 VLAN 网络，该成员访问该 VLAN 网络就像使用本地局域网一样。

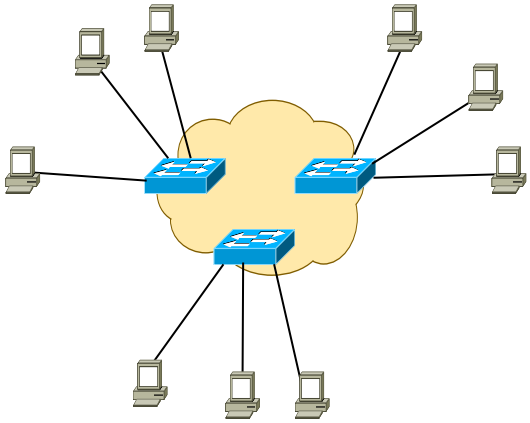


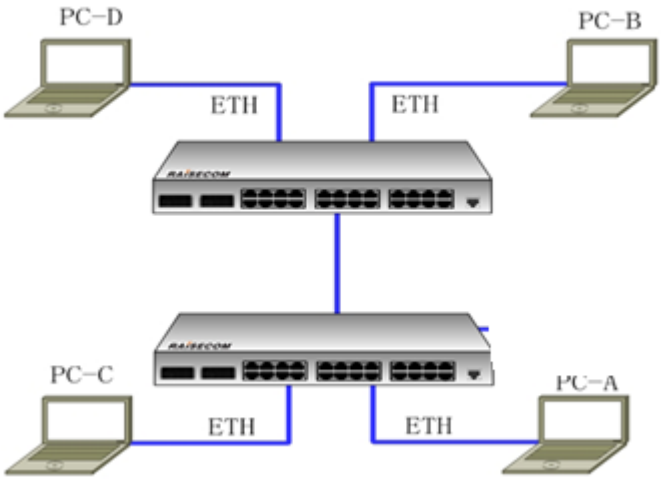
图 5.0 VLAN 结构

虽然 VLAN 在网络传输速度和网络时延方面有了很大的改善，其中仍然存在很多不足，最突出的是所有的网络节点都处在同一个广播域中，大大增加了网络中所有设备之间的数据流量，随着网络的不断扩充，有可能出现广播风暴，导致整个网络无法使用。

VLAN 的划分方式：

- 基于端口的 VLAN：它是划分 VLAN 最简单最有效的方法，这实际上是某些交换端口的集合，网络管理员只需管理和配置交换端口，而不管端口连接什么设备。
- 基于 MAC 地址的 VLAN 划分：只有网卡才分配有 MAC 地址，实际上是将某些服务器和工作站划分于某个 VLAN。实际上该 VLAN 是个 MAC 地址的集合，管理员只需管理和配置 MAC 地址。
- 基于第三层的 VLAN：该方法是采用在路由器上最常用的方法，即 IP 子网 IPX 网络号等。
- 基于策略的 VLAN：该方法的核心是采用什么样的策略，目前常用策略有：按 MAC 地址，按 IP 地址，按以太网协议类型，按网络的应用等。

实验拓扑



图注:PC_A 接 port 16 口， PC_C 接 port 32 口， PC_B 接 port 16， PC_D 接 port 32；两台交换机之间接 port 46

实验器材

DPtech LSW3600 交换机两台(LSW-A, LSW-B)

PC 四台

网线五根

[配置线一根]

实验步骤及详细配置

1、 依照组网图连接各设备。为不影响结果，建议删除交换机的所有配置并重启交换机。按图中要求相联设备，并依次设置 PC(A,B,C,D)的 ip 地址为 192.168.1.1/24、192.168.1.2/24、192.168.1.3/24、192.168.1.4/24，测试互通性。

2、 配置命令如下：

（1）配置交换机 LSW-A：

```
/* 进入配置模式*/
<DPTECH> conf-mode

/* 配置 VLAN */
[DPTECH] vlan 10                /*进入 vlan 配置模式*/
[DPTECH-vlan10] exit            /*退出 vlan 配置模式*/
[DPTECH] vlan 20
[DPTECH-vlan20] exit

/* 配置 VLAN 添加端口 */
[DPTECH] interface gige0_16
[DPTECH-gige0_16] switchport access vlan 10
[DPTECH-gige0_16] exit
[DPTECH] interface gige0_32
[DPTECH-gige0_32] switchport access vlan 20
[DPTECH-gige0_32] exit
[DPTECH] interface gige0_46
[DPTECH-gige0_48] switchport mode trunk
[DPTECH-gige0_48] switchport trunk allowed vlan 10, 20
[DPTECH-gige0_48] exit
```

（2）配置交换机 LSW-B：

/* 进入配置模式*/

<DPTECH> conf-mode

/* 配置 VLAN */

[DPTECH] vlan 10 /*进入 vlan 配置模式*/

[DPTECH-vlan10] exit /*退出 vlan 配置模式*/

[DPTECH] vlan 20

[DPTECH-vlan20] exit

/* 配置 VLAN 添加端口 */

[DPTECH] interface gige0_16

[DPTECH-gige0_16] switchport access vlan 10

[DPTECH-gige0_16] exit

[DPTECH] interface gige0_32

[DPTECH-gige0_32] switchport access vlan 20

[DPTECH-gige0_32] exit

[DPTECH] interface gige0_46

[DPTECH-gige0_46] switchport mode trunk

[DPTECH-gige0_46] switchport trunk allowed vlan 10, 20

[DPTECH-gige0_46] exit

完成上述配置后，测试各 pc 之间的连通性。

以下为选做：

（3）继续配置交换机 LSW-A：

[DPTECH] interface gige0_16

[DPTECH-gige0_16] switchport mode hybrid

[DPTECH-gige0_16] switchport hybrid allowed vlan 10, 20 untagged

[DPTECH-gige0_16] exit

测试 pc 之间的连通性

3、 交换机端口共有三种工作模式：access、trunk 和 hyblid。

Access 类型的端口只能属于 1 个 VLAN，一般用于连接计算机的端口；

Trunk 类型的端口可以允许多个 VLAN 通过，可以接收和发送多个 VLAN 的报文，一般

用于交换机之间连接的端口；

Hybrid 类型的端口可以允许多个 VLAN 通过，可以接收和发送多个 VLAN 的报文，可以用于交换机之间连接，也可以用于连接用户的计算机。

Hybrid 端口和 Trunk 端口在接收数据时，处理方法是一样的，唯一不同之处在于发送数据时：Hybrid 端口可以允许多个 VLAN 的报文发送时不打标签，而 Trunk 端口只允许缺省 VLAN 的报文发送时不打标签。

实验结果及截图

1　依照拓扑图连接各设备，测试各 pc 连通性如图 5.1 及图 5. 2 所示。

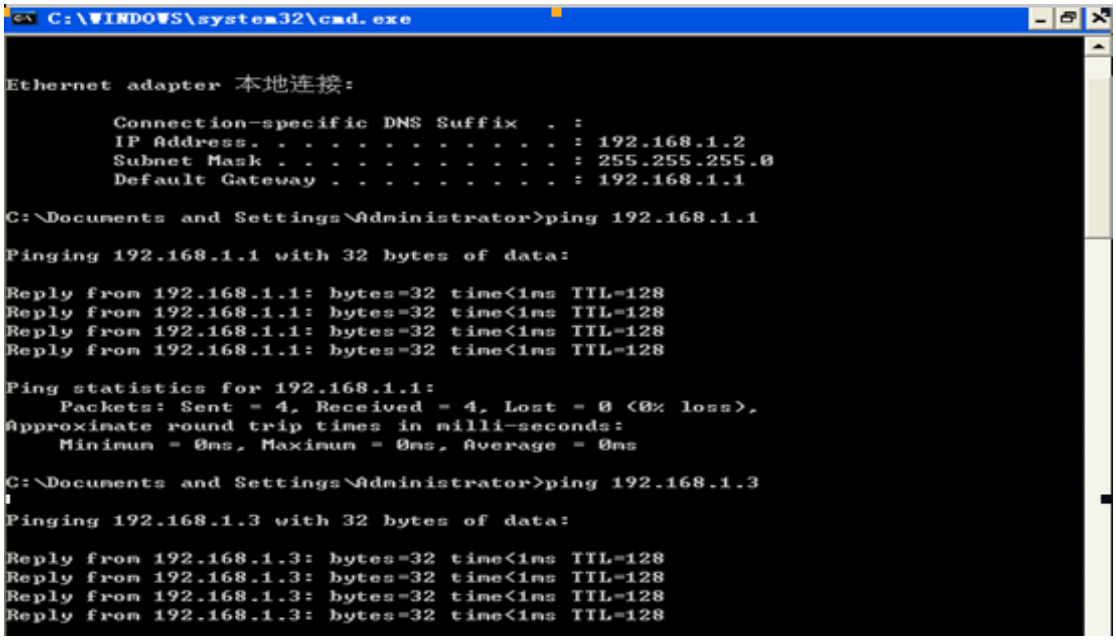


图 5.1　PC_A ping 主机 PC_B、PC_C 可 ping 通

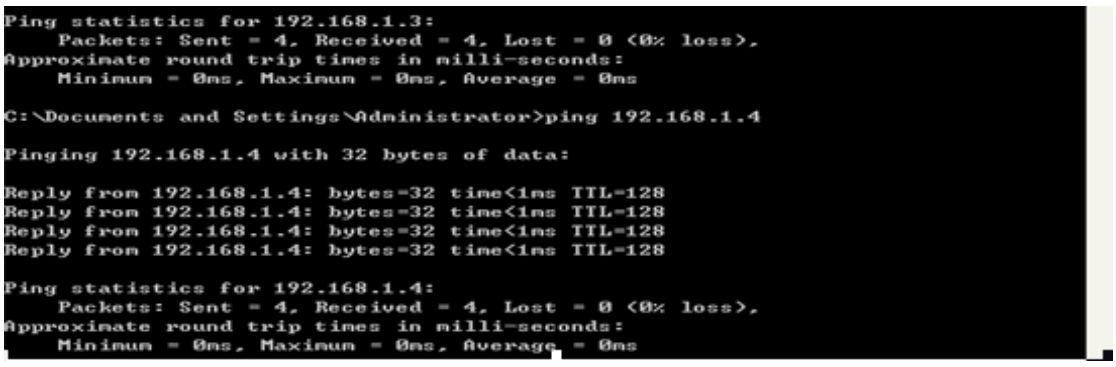


图 5.2　PC_A　ping PC_D 可 ping 通

2　两台交换机均进行如图 5.3 所示的命令配置

```
Raisecom(config)#vlan 10
Raisecom(config-vlan)#state active

Set successfully
Raisecom(config-vlan)#exit
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport access vlan 10

Set successfully
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport access vlan 20

Set successfully
Raisecom(config-port)#exit
Raisecom(config)#interface port 24
Raisecom(config-port)#switchport mode trunk

Set successfully
Raisecom(config-port)#switchport trunk allowed vlan 10,20
Please input 'yes' to confirm set allowed vlan:yes
Set successfully
Raisecom(config-port)#exit
Raisecom(config)#_
```

图 5.3　配置各端口 VLAN ID

3　配置完后测试各 pc 连通性，如图 5.4 和图 5.5 所示（同一 vlan 间互通，不同 vlan 间不通）

```
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\Documents and Settings\Administrator>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

图 5.4　PC_B 可 ping 通 PC_A,但不能 ping 通 PC_C

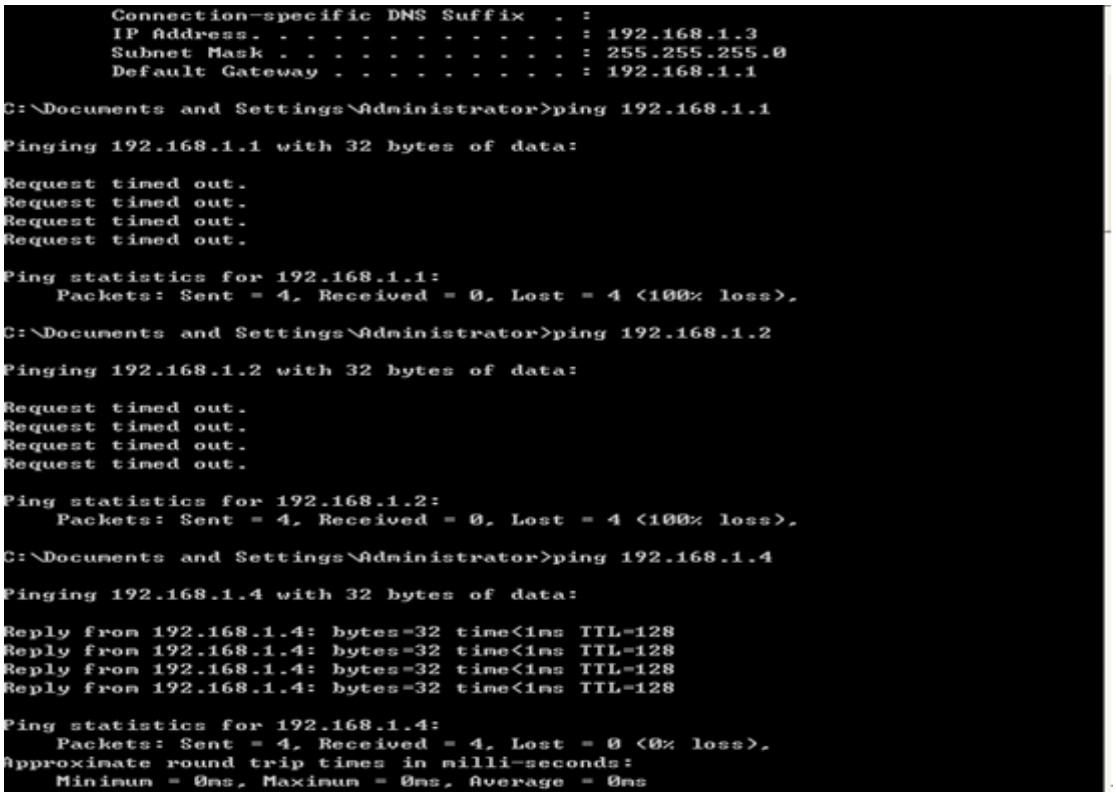


图 5.5　同时 PC_C 可 ping 通 PC_D,但不能 ping 通 PC_A 及 PC_B

4　继续配置交换机 LSW-A　如图 5.6 所示

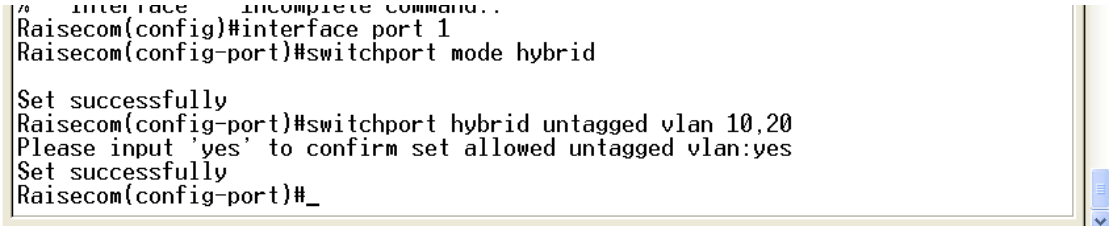


图 5.6　配置端口 1 为 hybrid 模式

5　再测试连通性，如图 5.7 和图 5.8 所示

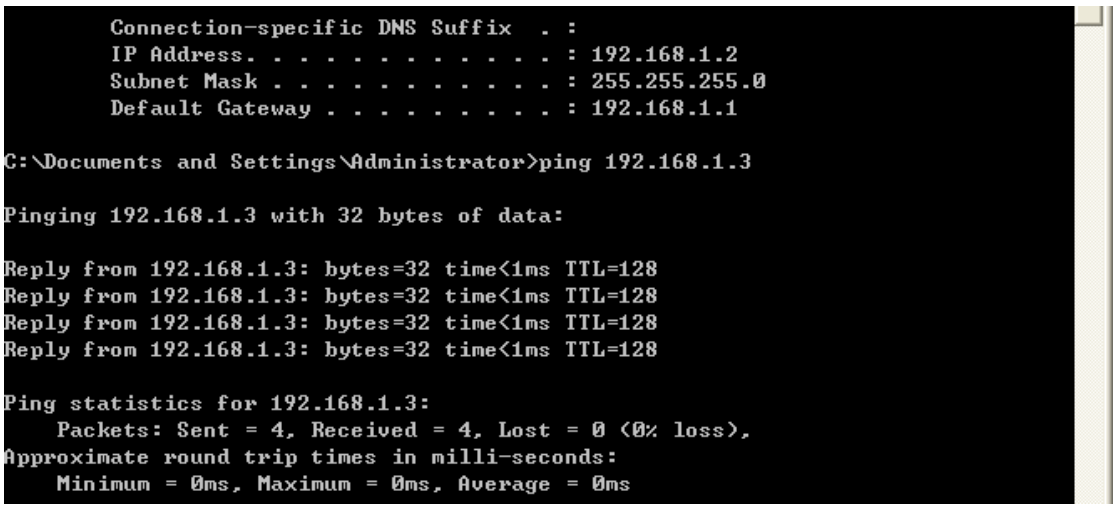


图 5.7　PC_B 可 ping 通 PC_C

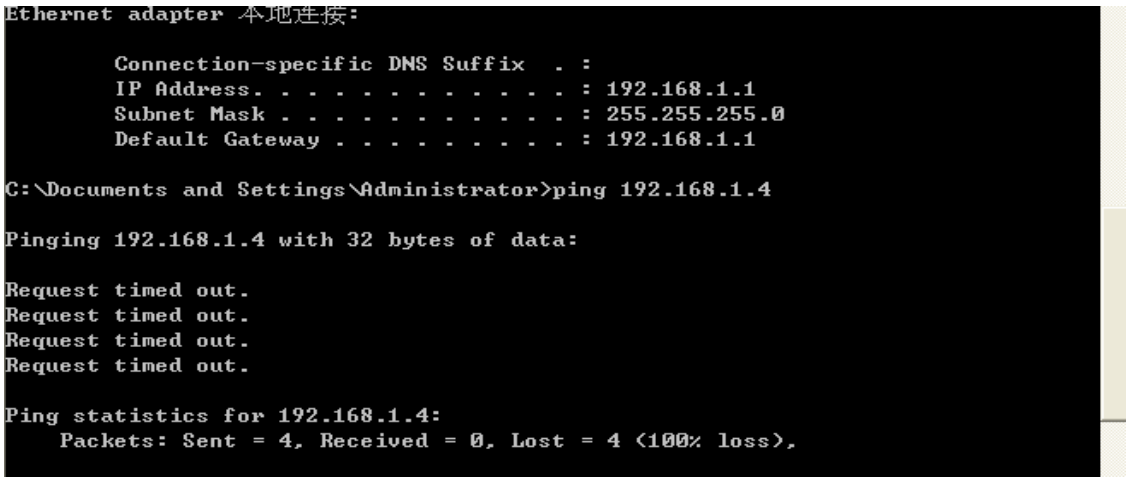
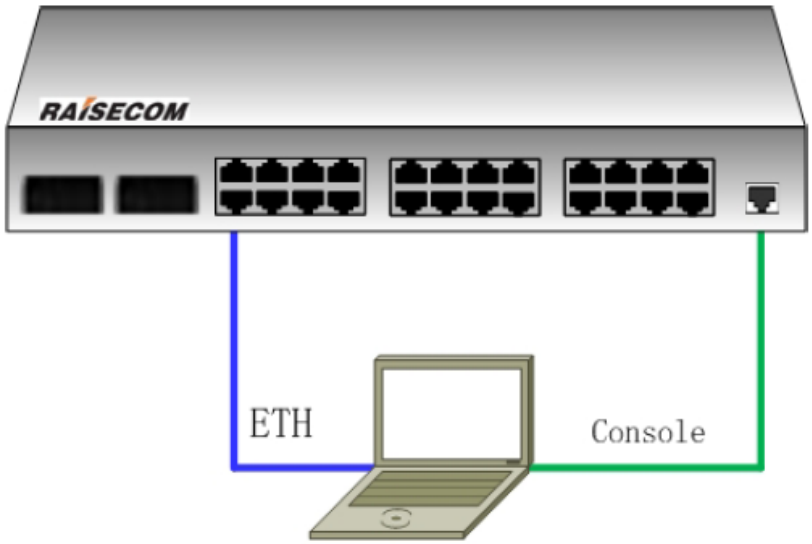


图 5.8　PC_A 仍不可 ping 通 PC_D

补充知识：DPtech LSW3600 交换机基本配置



DPTECH LSW3600 交换机一台，PC 一台，网线一根，console 线一根。

（1）console 口配置管理

最为常用的配置管理方法是通过 console 口进行本地配置管理。在设备初始化或未经其它方式的配置管理，都只能通过 console 口进行本地配置管理。

一、创建管理方式

在 console 配置管理中，我们使用 windows 系统附件中的超级终端仿真程序来完成与交换机的交互。新建超级终端的步骤如下：

(1) 按照以下路径打开超级终端，开始—〉程序—〉附件—〉通讯—〉超级终端，弹出对话框，输入名称后点击确定。

图 连接描述

(2) 再次弹出对话框，在“连接时使用”选项中选择连接交换机对应的 com 口，点击确定。

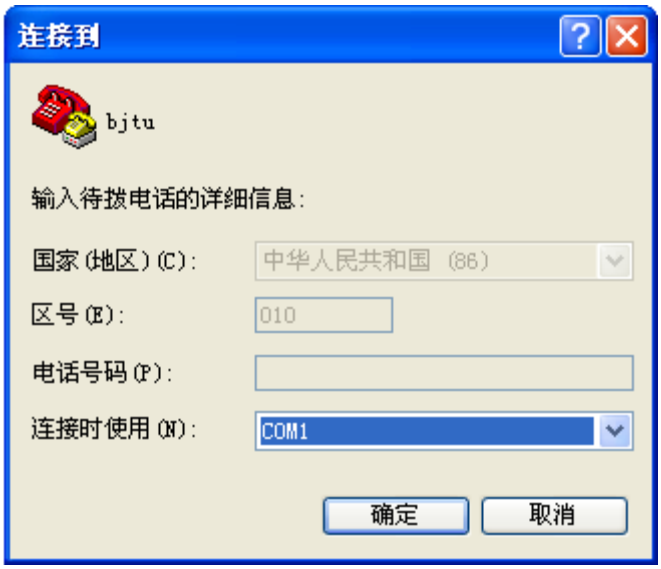


图 连接到

(3) 在 com 属性对话框中选择属性参数如下（点击“还原为默认值”按钮即可）：

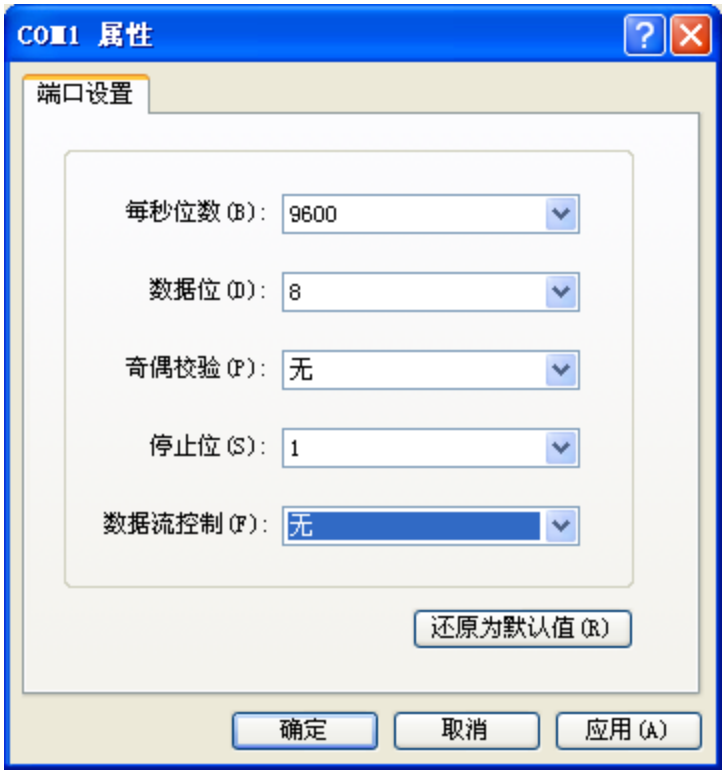


图 COM1 属性

(4) 完成参数配置后，单击“确定”，回车即可与交换机进行交互。

二、DPtech LSW3600 交换机命令行模式

DPtech LSW3600 交换机主要有如下几种模式：

视图		进入方法	显示
用户视图		登录设备的第一个级别的视图	<DPTECH>
配置视图		从用户视图输入 **conf-mode** 命令	<DPTECH>conf-mode [DPTECH]
VLAN 视图		从配置视图输入 **vlan** *vlan-id* 命令	[DPTECH]vlan 10 [DPTECH-vlan10]
接口视图	物理接口视图	从配置视图输入 **interface** *if-name* 命令	[DPTECH]interface gige0_2 [DPTECH-gige0_2]
	VLAN 接口视图	从配置视图输入 **interface vlan-if** *vlan-id* 命令	[DPTECH]interface vlan-if 10 [DPTECH-vlan-if10]
	聚合接口视图	从配置视图输入 **interface bond** *bond-id* 命令	[DPTECH]interface bond 3 [DPTECH-bond3]

在上一级模式可以键入 exit 命令返回到前一级模式，或者键入 end 直接退回到特权用户模式。

（2）DPtech LSW3600 交换机常用配置命令

一、查看当前配置

设备是否正常运行，决定于当前的配置是否正确，所以在配置过程中和故障排除中，查看当前配置是必不可少的操作之一。

<DPTECH> show running-config

二、保存当前设备配置

当前设备配置运行于设备的内存中，如果不进行保存，设备重启后配置将会丢失，所以完成配置后一定要将当前配置进行保存。

<DPTECH> conf-mode

[DPTECH] write file

Configuration is saved to device successfully.

[DPTECH]

三、删除配置信息

<DPTECH> conf-mode

[DPTECH] configuration clear-all

Warning: clear database, and then reboot the system.

Are you sure? (Y/N): y

[DPTECH]

四、重启交换机

某些时候需要重启交换机，比如升级操作或者是我们在开始实验的时候。

<DPTECH> reboot

This command will reboot the device. Current configuration will be lost, save current configuration? [Y/N]: y

Configuration is saved to device successfully.

This command will reboot the device. Continue? [Y/N]: y

五、查看系统版本

<DPTECH> show version

注意事项

（1）在输入交换机命令时要保证 console 线（交换机控制线）和交换机的连接。

（2）在联系到多台 PC 或者是交换机的实验中，最好把 PC 机的 windows 防火墙关闭，否则可能导致两台 PC 机在实验环境下 ping 不通。

（3）在每个实验之前最好删除交换机配置并重启交换机，防止对实验结果造成影响。

实验六 RIP 配置实验

实验目的

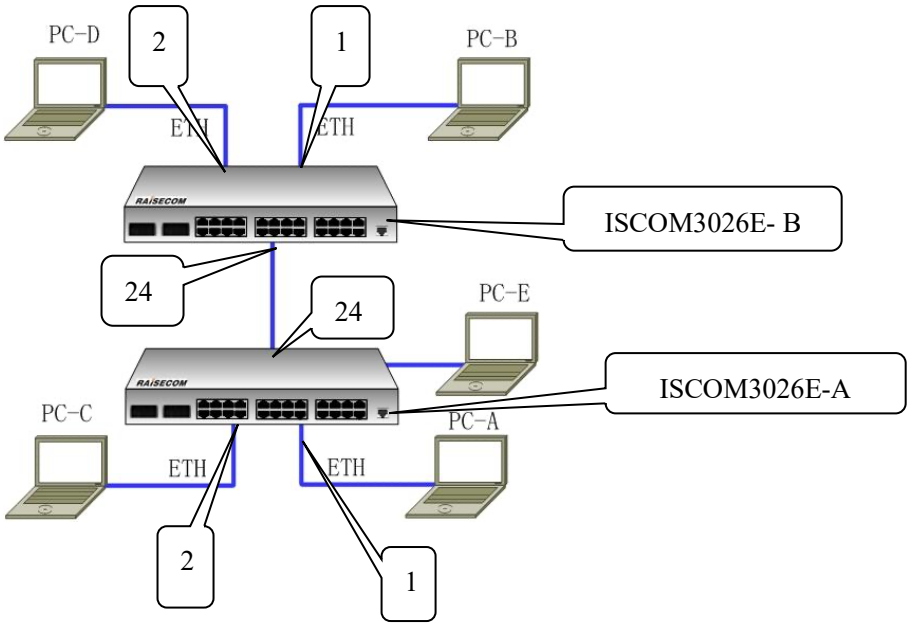
掌握 RIP 原理

掌握 RIP 的基本配置

实验内容

对两台支持三层路由功能的 DPtech 交换机进行 RIP 的配置

实验拓扑



设备清单

DPtech LSW3600 交换机两台（必需支持三层路由功能）

PC 五台

网线七根

[配置线一根]

实验详细步骤

1. 依照组网图连接各设备。将 PC_A 的地址设置为 192.168.1.2/24，PC_C 的地址设置为 192.168.1.3/24，PC_E 的地址设置为 192.168.1.4/24，网关为 192.168.1.1；PC_B 的地址设置为 192.168.2.2/24，PC-D 的地址设置为 192.168.2.3/24，网关为 192.168.2.1。
2. 配置交换机
   1) 配置交换机 LSW- A

```
/* 进入配置模式*/
<DPTECH> conf-mode

/* 配置 VLAN */
[DPTECH] vlan 10                /*进入 vlan 配置模式*/
[DPTECH-vlan10] exit            /*退出 vlan 配置模式*/
[DPTECH] vlan 100
[DPTECH-vlan100] exit

/* 配置 VLAN 添加端口 */
[DPTECH] interface gige0_16
[DPTECH-gige0_16] switchport access vlan 10
[DPTECH-gige0_16] exit
[DPTECH] interface gige0_32
[DPTECH-gige0_32] switchport access vlan 10
[DPTECH-gige0_32] exit
[DPTECH] interface gige0_46
[DPTECH-gige0_46] switchport mode trunk
[DPTECH-gige0_46] switchport trunk allowed vlan 10, 100
[DPTECH-gige0_46] exit

/* 配置 VLAN 接口 IP 地址 */
[DPTECH] interface vlan-if 10
[DPTECH-vlan-if10] ip address 192.168.10.1 255.255.255.0
[DPTECH-vlan-if10] exit
[DPTECH] interface vlan-if 100
```

[DPTECH-vlan-if100] ip address 192.168.100.1 255.255.255.0

[DPTECH-vlan-if100] exit

/* 配置 RIP 路由 */

[DPTECH]router rip

[DPTECH-rip] network 192.168.10.0/24

[DPTECH-rip] network 192.168.100.0/24

[DPTECH-rip] exit

2) 配置交换机 LSW-B：

/* 进入配置模式*/

<DPTECH> conf-mode

/* 配置 VLAN */

[DPTECH] vlan 20

[DPTECH-vlan20] exit

[DPTECH] vlan 100

[DPTECH-vlan100] exit

/* 配置 VLAN 添加端口 */

[DPTECH] interface gige0_16

[DPTECH-gige0_16] switchport access vlan 20

[DPTECH-gige0_16] exit

[DPTECH] interface gige0_32

[DPTECH-gige0_32] switchport access vlan 20

[DPTECH-gige0_32] exit

[DPTECH] interface gige0_46

[DPTECH-gige0_46] switchport mode trunk

[DPTECH-gige0_46] switchport trunk allowed vlan 20, 100

[DPTECH-gige0_46] exit

/* 配置 VLAN 接口 IP 地址 */

[DPTECH] interface vlan-if 20

[DPTECH-vlan-if20] ip address 192.168.20.1 255.255.255.0

[DPTECH-vlan-if20] exit

[DPTECH] interface vlan-if 100

[DPTECH-vlan-if100] ip address 192.168.100.2 255.255.255.0

[DPTECH-vlan-if100] exit

/* 配置 RIP 路由 */

[DPTECH]router rip

[DPTECH-rip] network 192.168.10.0/24

[DPTECH-rip] network 192.168.20.0/24

[DPTECH-rip] exit

完成上述配置后，测试各 pc 之间的连通性。

3. 配置完成后，在各交换机上查看路由表，能够看到其他交换机发布的路由信息，使用 **show ip route** 命令，可以通过查看路由表项检查 RIP 连接的建立是否正常；可以通过查看 RIP 路由的状态检查 RIP 通信是否正常，如下图所示：

LSW-A:

```
Raisecom#show ip route
Codes: C - Connected, S - Static, R - RIP, O - OSPF
------------------------------------------------------------
C   192.168.1.0[255.255.255.0],is directly connected , Interface 0
R   192.168.2.0[255.255.255.0],Via 192.168.100.2
C   192.168.100.0[255.255.255.0],is directly connected , Interface 1
Total route count: 3
Raisecom#
```

LSW-B:

```
Raisecom#show ip route
Codes: C - Connected, S - Static, R - RIP, O - OSPF
------------------------------------------------------------
R   192.168.1.0[255.255.255.0],Via 192.168.100.1
C   192.168.2.0[255.255.255.0],is directly connected , Interface 0
C   192.168.100.0[255.255.255.0],is directly connected , Interface 1
Total route count: 3
Raisecom#Without input, scrn will close in 10 mintues 0 seconds
```

当 RIP 连接正常建立后，路由器会学习到相应的 RIP 路由，路由表中会显示两条以字母“R”开头的路由。一条 RIP 路由包含了以下信息：

1） 路由器如何获悉信息（R—来自 RIP 协议）；

2） 目标网络及相应掩码；

3） 路由的下一跳；

比如 LSW-A 的路由表中:R 192.168.20.0[255.255.255.0].Via 192.168.10.2 一项 R 表明该信息获取来自 RIP 协议，目标网络为 192.168.20.0，子网掩码

255.255.255.0，路由的下一跳为 192.168.100.2，同时 PC 机应能 ping 通对方不同网段的网关，比如：

用 PC-B 去 ping PC-A,PA-C

```
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.2.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.2.1

C:\Documents and Settings\Administrator>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=126
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

用 PC-A 去 ping　PC-B，PB-D

```
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\Documents and Settings\Administrator>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time<1ms TTL=126
Reply from 192.168.2.3: bytes=32 time<1ms TTL=126
Reply from 192.168.2.3: bytes=32 time<1ms TTL=126
Reply from 192.168.2.3: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

此时还没有将 PC-E 划入到 vlan10 中，所以 PC-B 不能 ping 通 PC-E

```
C:\Documents and Settings\Administrator>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

将 PC-E 所连的 port 3 划入到 vlan10 中之后，再用 PC-B 去 ping PC-E 就能 ping 通了，结果如下图所示：

注：

RIP 是“路由信息协议（Routing Information Protocol）”的缩写。RIP 是目前应用最为广泛的内部网关协议之一，它采用的是著名的距离向量算法。RIP 是距离向量协议族中最简单的一种，它的路由选择主要是基于其到达最后目标站点的中间跳距（hop）数，通常用 metric 的大小来衡量。RIP 认为，路由器到它的直连网络的跳距数（hop）为 0，metric 的值为 1；到经过一个路由器就可到达的网络的跳距数（hop）为 1，metric 的值为 2；其余依次类推。RIP 支持的最大路径开销为 15，当 metric 大于等于 16 时，RIP 认为路径开销为无穷大，目的网络不可达。

RIP 是基于 UDP（User Datagram Protocol）数据报的协议。运行 RIP 的网关或主机在进行路由交换过程中要通过 UDP 的 520 端口收发报文。在 RIP 协议中，每个参与路由交换的路由器每隔一定时间（缺省为 30 秒）向其邻近路由器发送路由更新报文。如果路由器经过大约六个更新周期（缺省为 180 秒）未收到路由的更新信息就将这条路由置为无效。如果在接下来的一段时间（缺省为 300 秒）仍未收到这跳路由的更新信息，就将其从路由表中删除。为提高性能，对网络拓扑结构的变化做出及时有效的反映，RIP 协议支持水平分割，大大缩短了收敛的时间。同时，对路由信息的变更采用触发更新。

DPtech LSW3600 交换机同时支持 RIPv1 和 RIPv2。其中 RIPv2 支持明文认证、可变长掩码和无类域间路由选择。