

网络工程课程设计 教程

国防科学技术大学计算机学院

2018 年 3 月

目录

前言	1
第一章 网络基础知识回顾	2
实验 1.1. 制作网线	2
1. 实验目的	2
2. 实验设备	2
3. 实验任务	2
4. 实验原理	2
5. 实验步骤	3
6. 实验测评	5
实验 1.2. 熟悉思科模拟器	6
1. 实验目的	6
2. 实验设备	6
3. 实验任务	6
4. 实验原理	6
5. 实验步骤	7
6. 实验测评	7
实验 1.3. 构建简单局域网	8
1. 实验目的	8
2. 实验设备	8
3. 实验任务	9
4. 实验原理	9
5. 实验步骤	错误!未定义书签。
6. 实验测评	错误!未定义书签。
思考问题	错误!未定义书签。
第二章 交换机配置	11
实验 2.1. 交换机的 VLAN 间路由	11
1. 实验目的	11
2. 实验设备	11
3. 实验任务	11
4. 实验原理	12
5. 实验步骤	13
6. 实验测评	15
实验 2.2 交换机的端口聚合配置	17
1. 实验目的	17
2. 实验设备	17
3. 实验任务	17
4. 实验原理	17

5. 实验步骤	18
6. 实验评测	19
实验 2.3 交换机的快速生成树配置	20
1. 实验目的	20
2. 实验设备	20
3. 实验任务	20
4. 实验原理	20
5. 实验步骤	21
6. 实验评测	22
实验 2.4 交换机 HSRP 配置实验	23
1. 实验目的	23
2. 实验设备	23
3. 实验任务	23
4. 实验原理	23
5. 实验步骤	24
6. 实验评测	25
思考问题	26
第三章 路由器配置	27
实验 3.1 路由器的基本配置（直连网络）	27
1. 实验目的	27
2. 实验设备	27
3. 实验任务	27
4. 实验原理	28
5. 实验步骤	29
6. 实验评测	30
实验 3.2 静态路由配置实验	31
1. 实验目的	31
2. 实验设备	31
3. 实验任务	31
4. 实验原理	31
5. 实验步骤	32
6. 实验评测	32
实验 3.3 RIP 路由协议配置实验	33
1. 实验目的	33
2. 实验设备	33
3. 实验任务	33
4. 实验原理	33
5. 实验步骤	34
6. 实验评测	34

实验 3.4 OSPF 路由协议配置实验	35
1. 实验目的	35
2. 实验设备	35
3. 实验任务	35
4. 实验原理	35
5. 实验步骤	36
6. 实验评测	37
实验 3.5 实战训练	38
1. 实验目的	38
2. 实验设备	38
3. 实验任务	38
4. 实验原理	38
5. 实验步骤	39
5.1 三层交换机 VLAN 配置	39
5.2 路由器接口 IP 地址配置	39
5.3 路由协议配置	40
6. 实验评测	41
思考问题	41
第四章 服务器相关服务的安装与配置	42
实验 4.1 APACHE 的安装与基本配置	42
1. 实验目的	42
2. 实验要求	42
3. 实验环境	42
4. 实验原理	43
5. 实验步骤	44
5.1 实验准备	44
5.2 编译设置	44
5.3 编译	45
5.4 安装	45
5.5 配置	46
5.6 运行与停止	47
6. 实验评测	47
实验 4.2. 虚拟主机的配置	49
1. 实验目的	49
2. 实验要求	49
3. 实验环境	49
4. 实验原理	49
5. 实验步骤	49
5.1 虚拟主机配置	49
5.2 制作虚拟主机网页	50
6. 实验评测	50

实验 4.3 SMTP 服务器的安装与配置	51
1. 实验目的	51
2. 实验要求	51
3. 实验环境	51
4. 实验原理	52
5. 实验步骤	52
5.1 实验准备	52
5.2 安装设置	53
5.3 编译	53
5.4 安装	53
5.5 配置	54
5.6 用户管理	54
5.7 运行与停止	54
6. 实验评测	55
实验 4.4 POP3 服务器的安装与配置	57
1. 实验目的	57
2. 实验要求	57
3. 实验环境	57
4. 实验原理	57
5. 实验步骤	58
5.1 实验准备	58
5.2 安装设置	58
5.3 编译	59
5.4 安装	59
5.5 配置	59
5.6 用户管理	59
5.7 运行与停止	59
6. 实验评测	60
思考问题	61
第五章 防火墙配置	61
实验 5.1 安全规则配置实验	61
1. 实验目的	61
2. 实验要求	61
3. 实验环境	62
4. 实验原理	62
5. 实验步骤	63
6. 实验评测	63
思考问题	64
第六章 网络工程综合实验	65
1. 实验目的	65

2. 实验要求.....	65
3. 实验环境.....	65
4. 实验步骤.....	66
4.1 WEB 服务.....	66
4.2 邮件服务.....	66
4.3 交换机和路由器.....	67
4.4 防火墙.....	67
5. 实验评测.....	68

前言

网络工程课程设计是《网络工程》课程的实验课程，通过本课程的实践，使学生进一步理解网络工程的主要概念，熟悉目前网络工程建设常用的、主流的网络设备、网络应用系统的工作原理和安装、配置与使用方法，重点培养学生理论联系实际和动手操作的能力，为将来快速适用网络工程建设工作的需要奠定良好的基础。

课程最终要求学员了解或掌握以下网络应用系统和网络设备的安装配置和使用方法，并初步具有网络工程组网方案设计和实施的能力。

■ 交换机

了解交换机的结构与组成、工作原理和主要功能，熟悉其关键指标，掌握主流厂家常规交换机产品安装、配置与使用方法，重点掌握 VLAN 的划分、三层交换的配置等技术。

■ 路由器

了解路由器的结构与组成、工作原理和主要功能，熟悉其关键指标，掌握主流厂家常规路由器安装、配置与使用方法，重点掌握路由协议的选择、路由规则的制定与配置等技术。

■ 防火墙

了解防火墙的结构与组成、工作原理和主要功能，熟悉其关键指标，掌握主流厂家常规防火墙系统安装、配置与使用方法，重点掌握网络安全策略的制定、防火墙安全规则的配置等技术。

■ Web 服务

掌握在某一种网络操作系统（Windows 或 Unix）环境下，目前流行版本的 Web 服务系统的安装、配置与使用方法。

■ EMAIL 服务

掌握在某一种网络操作系统（Windows 或 Unix）环境下，目前流行版本的 SMTP 和 POP3 服务系统的安装、配置与使用方法。

本课程适用于计算机应用、网络工程等专业，要求预修 Linux/Unix 操作系统、计算机网络原理、网络工程等课程，建议本课程设计以小组为单位实施，每组 4-8 人。

第一章 网络基础知识回顾

实验 1.1. 制作网线

1. 实验目的

掌握制作 EIA/TIA 568B 标准制作直连线的方法；了解网线的内部结构。

2. 实验设备

- 网线钳 1 把（每组三个）
- 网线测试仪 1 只（每组两个）
- 双绞线 1 根、两只 RJ-45 水晶头（每人）

3. 实验任务

每人使用实验设备制作一根 1m 左右网线，使用测线仪测试网线各端口连通情况，并做好记录，使用自己制作的网线连接电脑与交换机，观察并记录连通情况。

4. 实验原理

（1）非屏蔽双绞线的内部结构

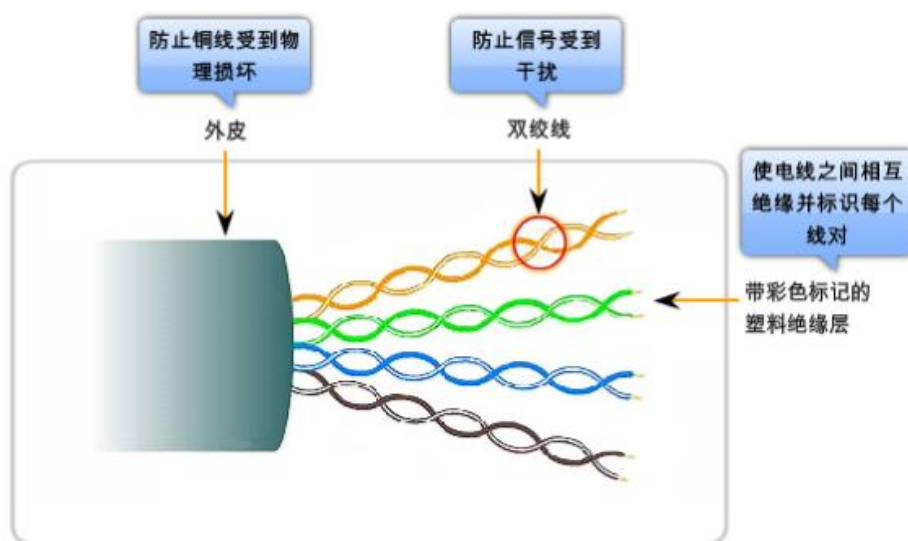


图 1-1 UTP 内部结构

Unshielded Twisted Paired 非屏蔽双绞线，简称 UTP。UTP 内部有四对不同颜色标记的双绞线，每对双绞线以固定间隔绞合在一起，绞合的作用是为抵消电脉冲传输过程中所形成的电磁场。外皮包裹着四对双绞线，防止内部铜线受到物理损伤。如图 1-1 所示。

(2) 非屏蔽双绞线与 RJ45 连接标准

EIA/TIA 制定的布线标准规定了不同颜色的 4 对双绞线与 RJ45 针脚连接。其中 EIA/TIA 568A 标准规定的线序为绿白、绿、橙白、蓝、蓝白、橙、棕白、棕，EIA/TIA 568B 标准规定的线序为橙白、橙、绿白、蓝、蓝白、绿、棕白、棕，如图 1-2 所示。国内普遍使用 EIA/TIA 568B 标准。

在 10Mb/s 和 100Mb/s 的以太网中只使用两对线，1、2 用于发送，3、6 用于接收。

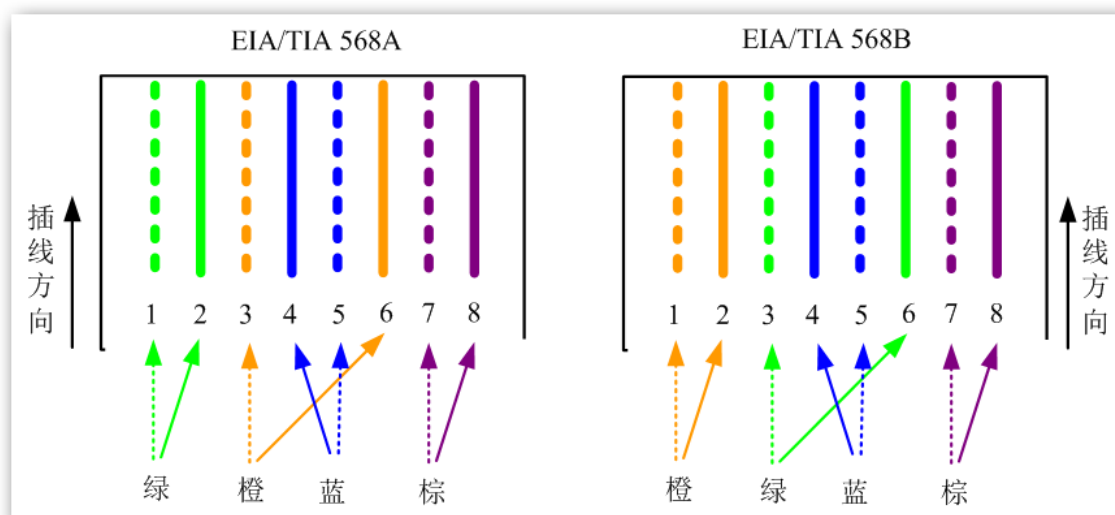
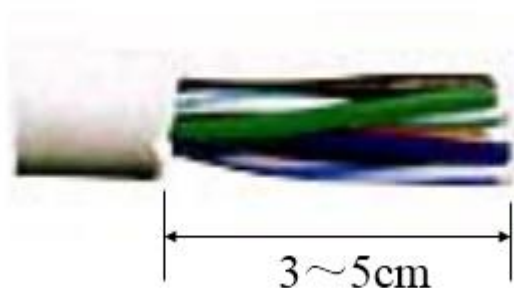


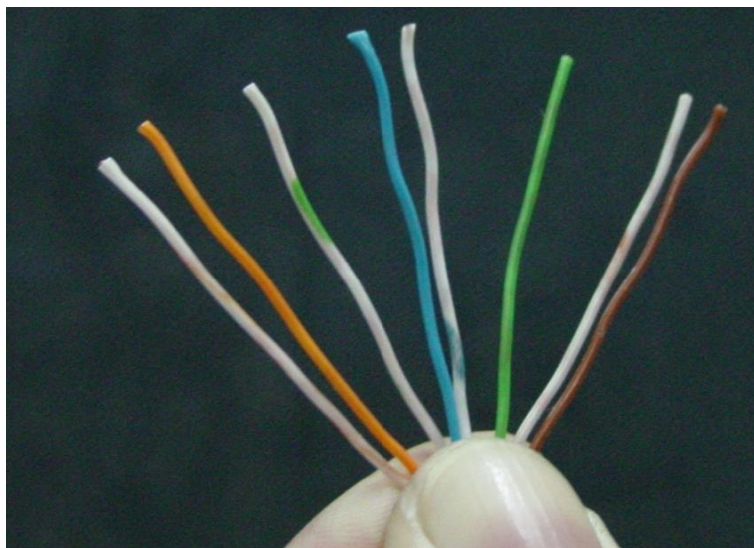
图 1-2 EIA/TIA 568A 和 EIA/TIA 568B 线序

5. 实验步骤

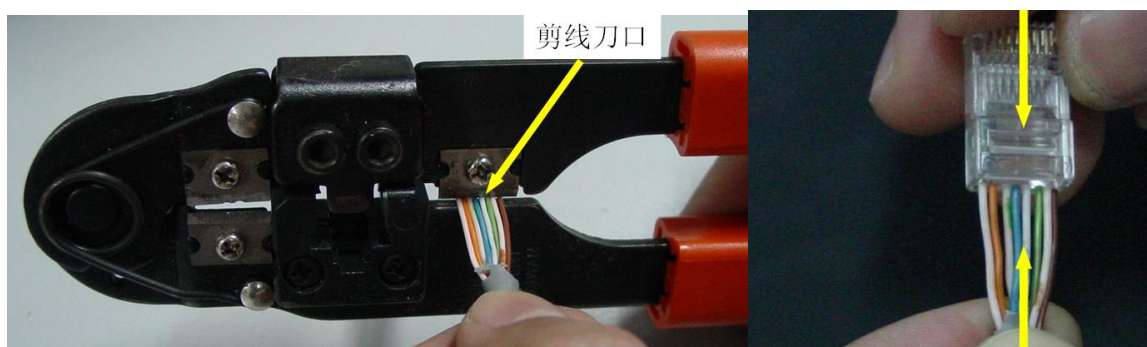
第一步：用网线钳前部剥线器剥除双绞线外皮 3~5 cm。



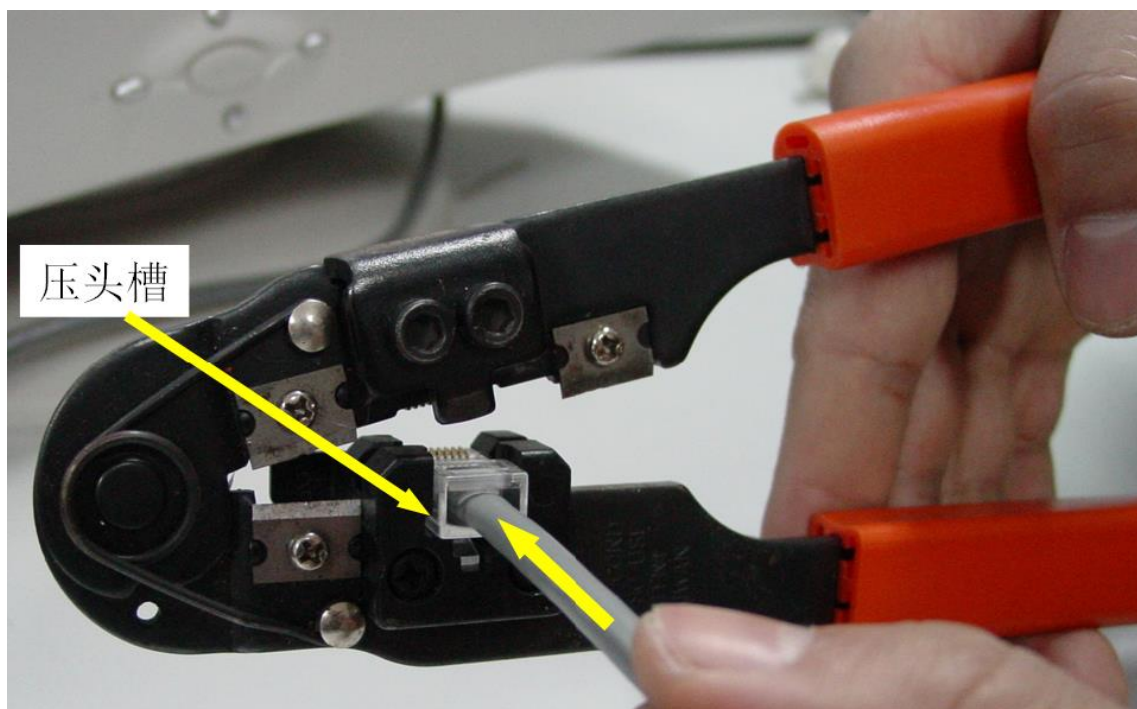
第二步：分离每一对线，将其弄直，将它们按白橙/橙/白绿/蓝/白蓝/绿/白棕/棕顺序排列。注意：绿色线应该跨越蓝色对线。



第三步：将上述网线钳剪齐，长度约为 14mm。再将双绞线的每一根线依序放入 RJ-45 接头的引脚内，第一只引脚内应该置放白橙色线，注意弹片端朝下。



第四步：从水晶头正面目视每根双绞线已经放置正确并到达底部位置之后，可用网线钳用力压 RJ-45 接头，使水晶头内部的金属片恰好刺破双绞线的包皮与内部金属线良好接触。



第五步：重复第一步到第四步，再制作另一端的 RJ-45 接头。完成后的连接线两端的 RJ-45 接头，引脚和颜色完全一样。

6. 实验测评

用网线测试仪检测该 RJ-45 接头的双绞线是否可用。测试仪由两部分组成。线缆的两端接头分别插入测试仪的两部分中。线路两端的测试仪上的 LED 依次同时发光则说明线路正常；如果有某个或某些灯不亮或次序不对，则说明线路有问题。

如果接触不良，则需要尝试用网线钳用力压两端水晶头，使它们良好接触。

如果发现线序不对请将某端水晶头剪掉，重新按实验步骤，再制作一个 RJ-45 接头。

实验 1.2. 熟悉思科模拟器

1. 实验目的

熟悉思科模拟器的操作方法；熟悉直连线和交叉线的不同应用场景。

2. 实验设备

- 思科模拟器 Cisco Packet Tracer（软件）

3. 实验任务

每人在自己电脑上安装 Cisco Packet Tracer，在模拟器中完成实验 1-2.pka，按照提示完成各设备之间的连线，并检测结果。

4. 实验原理

非屏蔽双绞线类型

根据应用场合不同，非屏蔽双绞线有三种类型：直通线、交叉线和全反线。直通线主要用来连接不同类型的设备，如交换机和计算机、集线器和计算机、交换机和路由器。交叉线主要用来连接相同类型的设备，如交换机和交换机、交换机和集线器、计算机和路由器、计算机和计算机。全反线主要用来交换机和路由器的配置。如图 1-3 所示。

现在很多设备能够自适应，直接用直连线也能连接相同类型的设备，但是有些型号较老的设备仍然需要遵循直通线和交叉线的应用场合规律。在思科模拟器中也需要严格遵循此规律。

电缆类型	标准	应用
以太网直通电缆	两端均为 T568A 或两端均为 T568B	连接网络主机与交换机或集线器之类网络设备。
以太网交叉电缆	一端为 T568A， 另一端为 T568B	连接两台网络主机。 连接两台网络中间设备（交换机与交换机或路由器与路由器）。
全反电缆	Cisco 私有	使用适配器连接工作站串行端口与路由器控制台端口。

图 1-3 电缆类型

5. 实验步骤

参考 1-2.pka 中的活动步骤完成实验。

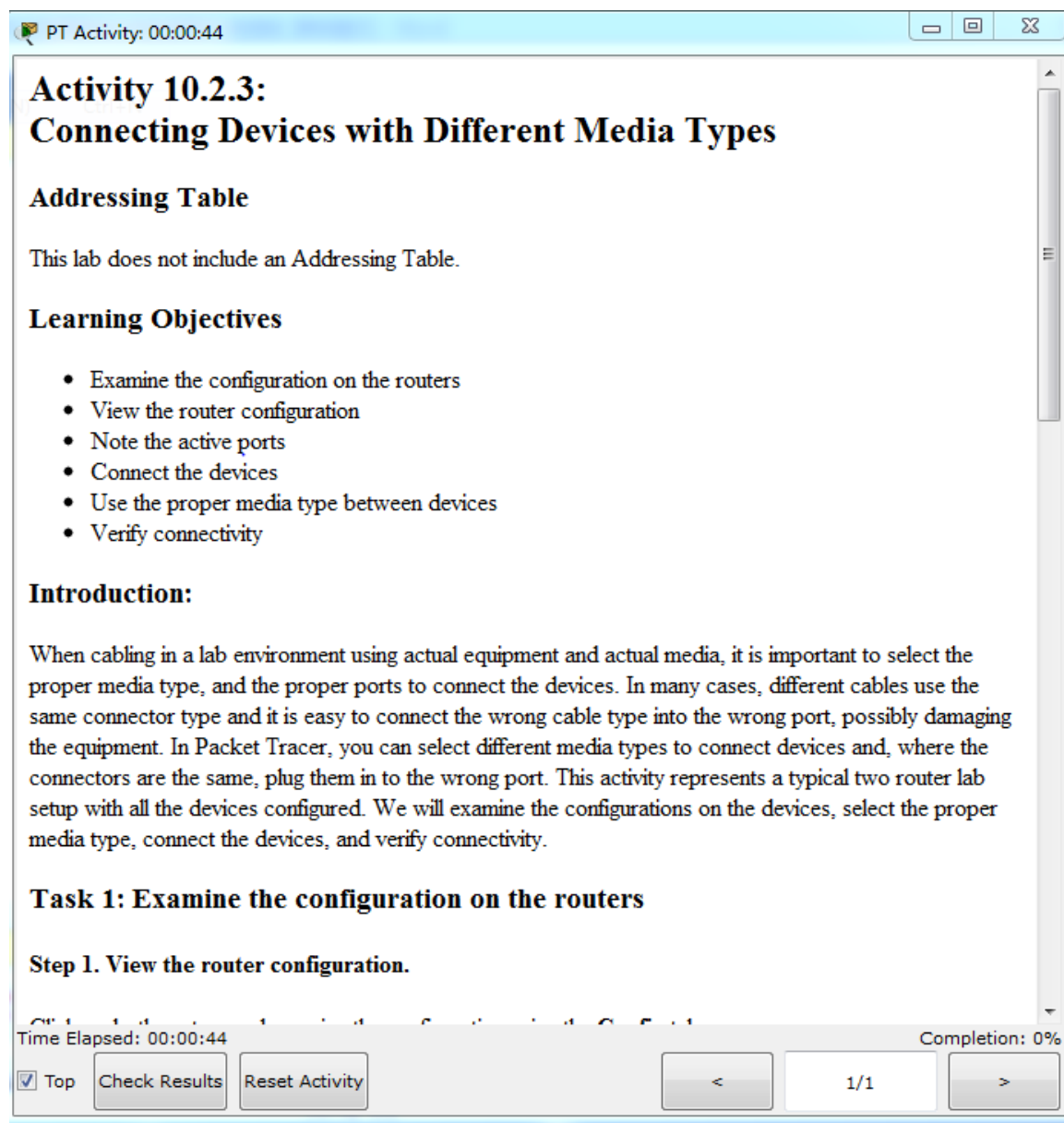


图 1-4 实验任务图

6. 实验测评

点击图 1-4 中左下角的 Check Results 按钮，如果全部完成则显示 100%，如果有错误请按照测评结果提示返回修改。

实验 1.3. 构建简单局域网

1. 实验目的

掌握用交换机、路由器进行简单局域网组建的方法，了解交换机、路由器的配置界面。

2. 实验设备

- 思科模拟器 Cisco Packet Tracer（软件）

3. 实验原理

本实验模拟一个公司的内部局域网的组建。该公司有两个部门：PCA、PCB 属于部门 1，PCC、PCD 属于部门 2。首先，用交换机 S1、S2 分别将这两个部门的所有电脑连接起来组成两个局域网，并规划两个网段，此时实现了部门内的互联互通。而要实现部门之间的互联互通，就需要用路由器将两个局域网连接起来，通过路由转发来实现。

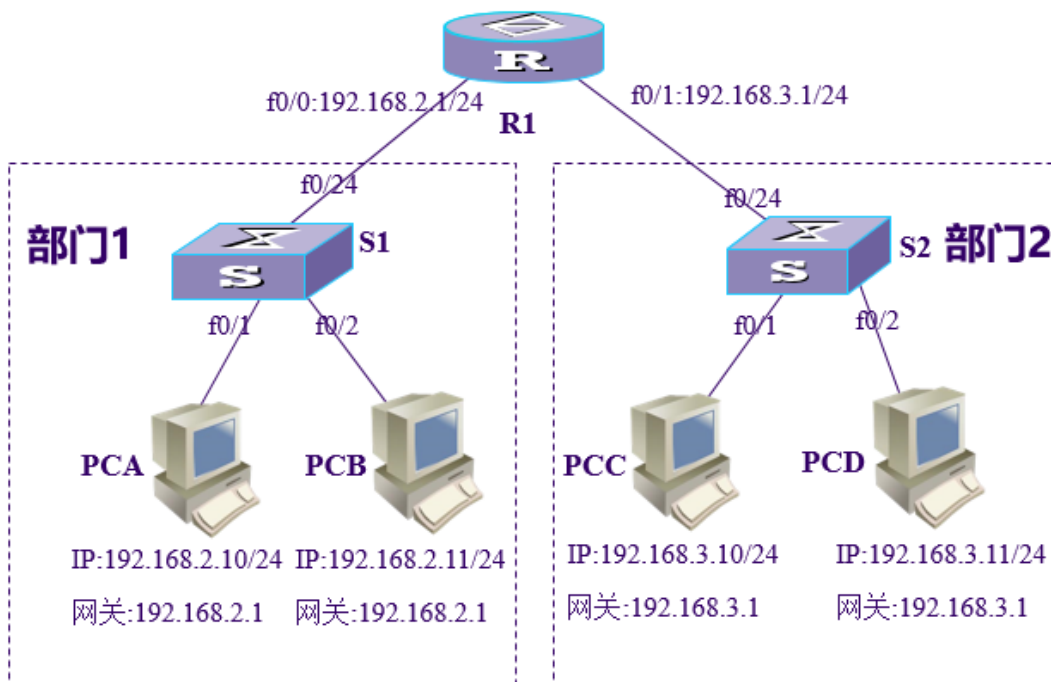


图 1-5 简单组网实验组网图

关于 IP 地址的规划，我们给两个部门分别分配专用地址 192.168.2.0/24 和

192.168.3.0/24.

所谓专用地址就是 RFC1918 规定的三个网段的专用地址 (private address) ，这些地址只能用作私网地址而不能作为公网地址。

10.0.0.0-10.255.255.255

172.16.0.0-172.31.255.255

192.168.0.0-192.168.255.255

这些地址只能用于一个机构的内部通信，而不能用于与因特网上的主机通信。

并规定了在因特网中的所有路由器，对目的地址是专用地址的数据报一律不进行转发。

4. 实验步骤

步骤 1 在电脑中按照默认设置安装 Cisco Packet Tracer。

步骤 2 在 Cisco Packet Tracer 中按照图 1 构建网络拓扑图，路由器选择型号 2811，交换机选择型号 2960，并给 PCA、PCB、PCC 和 PCD 四台电脑配置 IP 和网关。

在各台计算机上使用 ping 命令检查网络的连通情况，并将结果填入下表：

		所用命令	能否 ping 通
同一网段	PCA ping PCB		
	PCC ping PCD		
不同网段	PCB ping PCC		
	PCD ping PCA		

步骤 3 配置路由器 R1 的接口 IP 地址，参考命令如下。

Continue with configuration dialog? [yes/no]: no	#不进入配置对话
Router>en	#进入特权模式
Router#config t	#进入全局配置模式
Router(config)#int fa0/0	#进入接口配置模式
Router(config-if)#ip add 192.168.2.1 255.255.255.0	#配置 IP
Router(config-if)#no shut	#启用端口

```
Router(config)#int fa0/1                                #进入接口配置模式
Router(config-if)#ip add 192.168.3.1 255.255.255.0      #配置 IP
Router(config-if)#no shut                                #启用端口（注意回车确认命令）
```

再次在各台计算机上使用 ping 命令检查网络的连通情况，并将结果填入下表：

		所用命令	能否 ping 通
同一网段	PCA ping PCB		
	PCC ping PCD		
不同网段	PCB ping PCC		
	PCD ping PCA		

• **思考题：**

步骤 2 和步骤 3 的结果有何不同，为什么？如果把图中路由器 R1 接口 E0/0 的 IP 地址改为 192.168.4.1/24，请写出 4 台主机间的连通情况，并解释原因。

4. 实验原理

(1) 交换机的命令模式

交换机配置命令主要以下几种模式：

- 一般模式：提示符为>，只能进行查看交换机的基本信息 show、ping、telnet 等操作；
- 特权模式：提示符为#，除了一般模式的操作外，可以进入各种操作配置模式；
- 全局模式：提示符为 (config) # ，可以对交换机的全局参数进行配置；
- 接口模式：提示符为 (config-if) # ，对交换机的接口进行配置。

具体如下图所示，键入问号 (?)，交换机就可以列出当前的模式，以及该命令模式可以使用的命令种类。

工作模式		提示符	启动方式
用户模式		Switch>	开机自动进入
特权模式		Switch#	Switch>enable
配置模式	全局模式	Switch(config)#	Switch#configure terminal
	VLAN模式	Switch(config-vlan)#	Switch(config)#vlan 100
	接口模式	Switch(config-if)#	Switch(config)#interface Fa0/0
	线程模式	Switch(config-line)#	Switch(config)#line console 0

在某模式下只能执行当前模式允许的命令，交换机的命令不能跨模式执行。

从一般模式进入特权模式：

switch>enable

输入密码后即可进入特权操作模式。

从特权模式进入全局模式：

switch#config terminal

从全局模式进入接口模式：

switch (config) #interface 接口编号 (例如：fastethernet 0/1)

输入 exit 将从当前模式返回到上一级模式，输入 end 或 Ctrl+Z 将直接返回到特权模式。

(2) 帮助信息

- 命令速查：在任意命令模式下，输入 ? 将列出在当前模式下可以进行的操作命令及其功能说明：如：

```
switch>?
disable  Turn off privileged commands
enable  Turn on privileged commands
exit     Exit from the EXEC
.....
```

- 命令帮助：在任意一个命令后面输入 `?` 将列出该命令后面所需的参数，如：
`switch#show ?`
- 命令简写：交换机的命令在没有二义性的前提下可以简写，如：
`switch#conf t` 代表 `config terminal` 命令
- 命令补齐：当输入一个命令时如果不记得后面的拼写规则或参数时，可以按 `TAB` 键自动将命令或参数补齐，如：
`switch#con` 按键盘的 `TAB` 键后将自动补齐为 `config`。

5. 实验步骤

第一步：完成网络连接图

参考图 2-1，在思科模拟器中完成网络连接图（无需标记文字），注意交换机和 PC 之间用直连线，交换机和交换机之间用交叉线连接。

第二步：配置 SW1

以下为 SW1 配置命令，其中加粗斜体字为需要输入的命令，斜体字为交换机提示信息，! 后是说明文字。

```
Switch>en
Switch #config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch (config)#hostname SW1
! 将交换机命名为 SW1
SW1(config) #vlan 10
SW1(config-vlan) #name test10
SW1(config-vlan) #exit
! 创建 VLAN 编号为 10，命名为 test10
SW1(config)vlan 20
SW1(config-vlan) name test20
SW1(config-vlan) exit
! 创建 VLAN 编号为 20，命名为 test20
SW1(config)int fa0/2
SW1(config-if)sw access vlan 10
SW1(config-if)exit
! 将接口 fa0/2 加入 VLAN 10
SW1(config)int fa0/10
SW1(config-if)sw access vlan 20
```

SW1(config-if)*exit*

！将接口 fa0/10 加入 VLAN 20

SW1(config)*int fa0/24*

SW1(config-if)*sw mode trunk*

SW1(config-if)*exit*

！将接口 fa0/24 设置成 trunk 模式，使其能够通过多种 VLAN 信息。

第三步：配置 SW2

参考 SW1，完成 SW2 的配置。

第四步：配置 SW3

参考 SW1，在 SW3 上完成命名、创建 VLAN 和相关接口的配置。

SW3(config)*ip routing*

！开启交换机路由功能

SW3(config)*int vlan 10*

SW3(config-if)*ip add 192.168.10.1 255.255.255.0*

！为虚拟接口 VLAN10 配置 IP

SW3(config-if)*no shut*

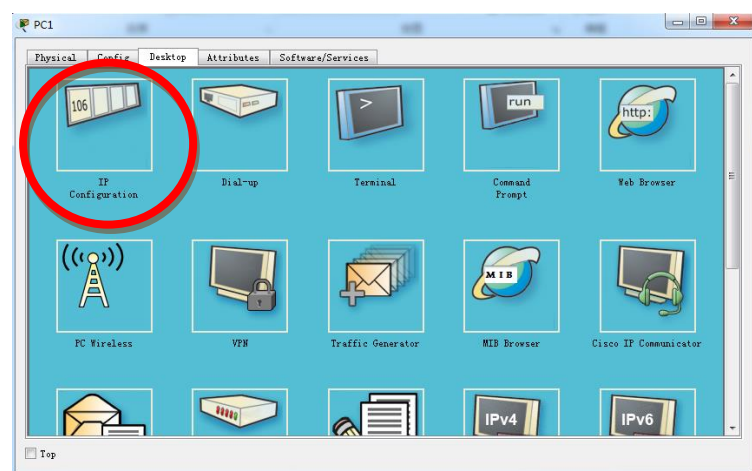
！打开接口

SW3(config-if)*exit*

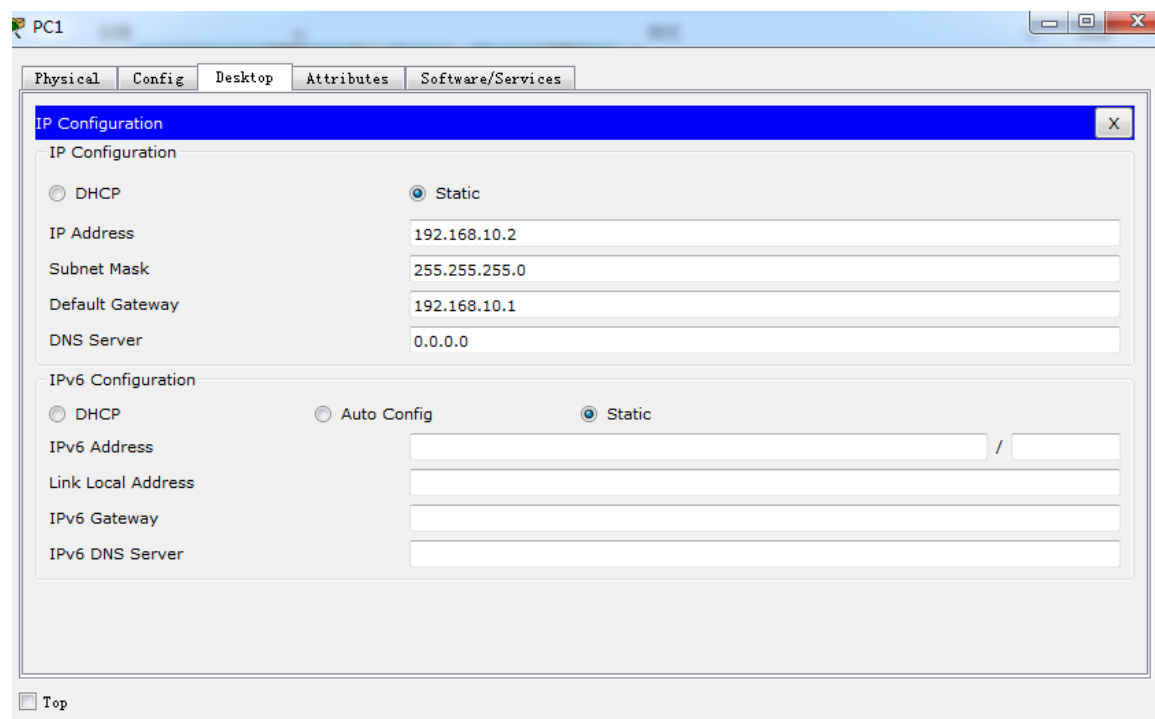
参考 VLAN10 的 IP 配置，完成 VLAN20 的配置

第五步：配置 PC1-4 的 IP

双击 PC1 进入配置界面，选择 IP Configuration:



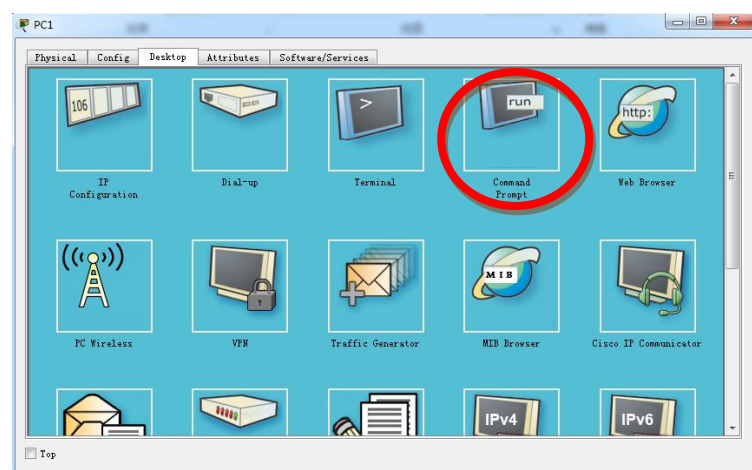
进入如下界面为 PC1 配置相关 IP 信息。



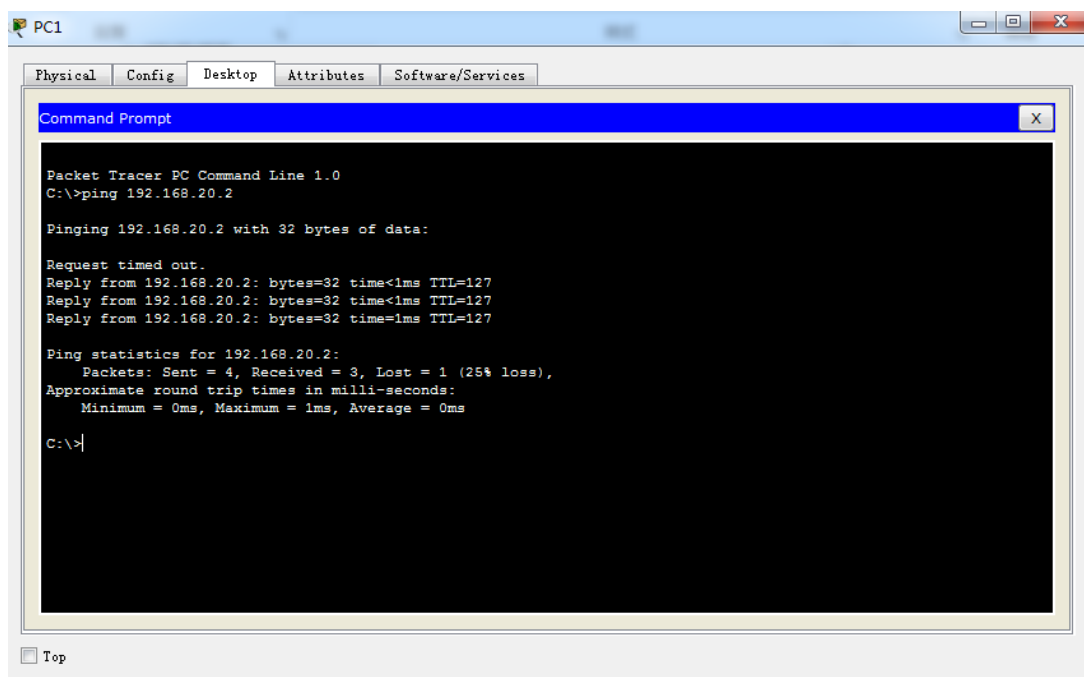
同样方法完成 PC2-4 的 IP 信息配置。

6. 实验测评

双击 PC1 进入配置界面，选择 Command Prompt:



进入如下界面使用 ping 命令测试连通。



注意第一个 ping 包会丢失，因为交换机第一次需要学习 MAC 地址。

在 PC2 上使用 ping 命令，测试到 PC1、PC3、PC4 能否连通。

在 SW1、SW2、SW3 上使用 show vlan，show ip interface brief，show running-config 查看相关配置信息。

如果 PC 之间不能连通，请参考一下步骤排错：

1. 请查看是否 VLAN 内部可以正常通信，如果可以则检查 SW3 的配置；如果 VLAN 内部也不能通信请按照下面步骤排错。
2. 查看网络连线类型是否正确
3. 查看连线端口是否正确
4. 查看 PC 上的 IP 配置是否正确
5. 检查各交换机上的配置是否正确，可以使用命令 reload 重启，重新进行配置。

实验 2.2 交换机的端口聚合配置

1. 实验目的

熟悉交换机端口聚合的概念，掌握交换机端口聚合配置方法，能根据网络可靠性应用需求，将交换机进行端口聚合配置。

2. 实验设备

思科模拟器 Cisco Packet Tracer（软件）

3. 实验任务

在思科模拟器中按照图 2-2 所示完成实验连接图，在两台交换机上配置端口聚合，使 PC1 和 PC2 之间能够通信。

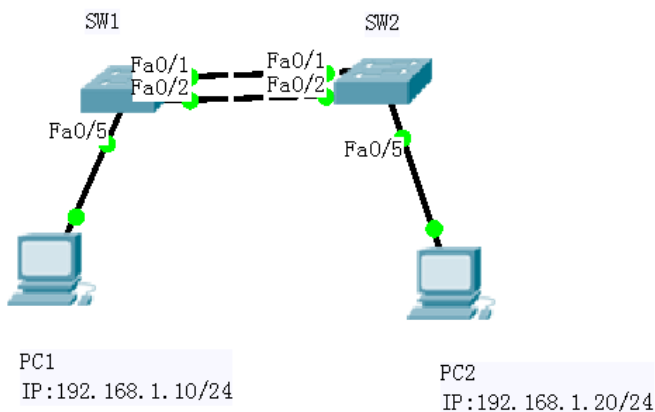
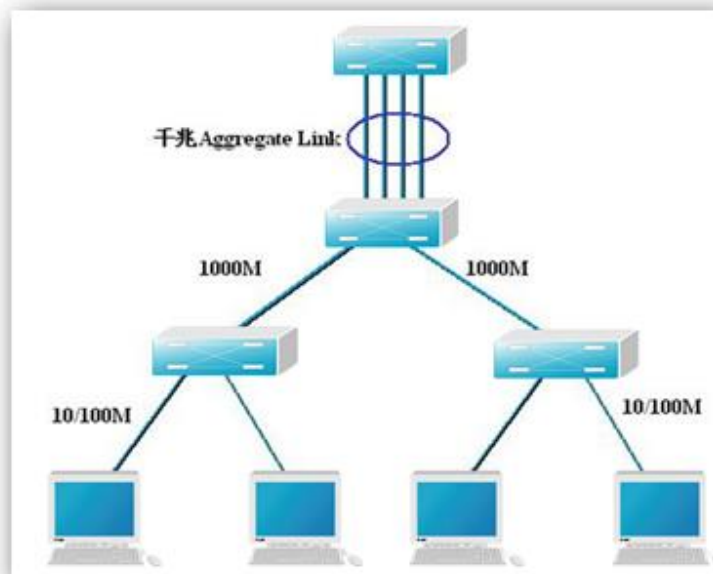


图 2-2 端口聚合配置网络连接图

4. 实验原理

在交换机上把多个物理端口的链路捆绑在一起，形成单一的逻辑连接，这个逻辑连接就被称为聚合端口（Aggregate port），如下图所示。端口聚合一方面增加了级联链路的带宽，另一方面增加了链路的可靠性，当聚合内的某一链路发生故障时也不会影响到网络的通信。



思科 EtherChannel 配置端口聚合：

1. 能够将多个物理端口绑定为一个逻辑端口，能充分利用现有端口来增加带宽。
2. Cisco 交换机最多允许绑定 8 个端口。如果是 100Mbps 端口，汇聚后可达 800Mbit/s；如果是 1000Mbps 端口，汇聚后可达 8Gbit/s。不同品牌交换机可绑定端口数量不同。
3. 绑定后的端口默认继承原来物理接口的配置模式。
4. Cisco 的交换机不仅可以支持第二层 Etherchannel，还可以支持第三层 Etherchannel。
5. 一个 Etherchannel 内所有的端口都必须具有相同的速率和双工模式。

5. 实验步骤

第一步：完成网络连接图

参考图 2-2，在思科模拟器中完成网络连接图（无需标记文字），注意交换机和 PC 之间用直连线，交换机和交换机之间用交叉线连接。

第二步：配置 SW1

以下为 SW1 配置命令，其中加粗斜体字为需要输入的命令，斜体字为交换机提示信息，！后是说明文字。

Switch>**en**

Switch #**config t**

Enter configuration commands, one per line. End with CNTL/Z.

Switch (config)#**hostname SW1**

！将交换机命名为 SW1

SW1 (config)#**int range fa 0/1-2**

！同时选中 fa0/1 和 fa0/2 两个接口，**注意空格。**

SW1 (config-if-range)**channel-group 1 mode on**

SW1 (config-if-range)**no shut**

！将两个接口绑定为一组并指定 on 模式 组号本地有效

SW1 (config-if-range)***int port-channel 1***

SW1 (config-if)***sw mode trunk***

！指定接口模式为 trunk，如不指定，会自动继承物理接口的模式

SW1 (config-if)***exit***

第三步：配置 SW2

参考 SW1，完成 SW2 的配置。

第四步：完成 PC1、PC2 的 IP 配置

参考图 2-2，完成 PC1、PC2 的 IP 配置。

6. 实验评测

1. 在 SW1 上使用命令 show etherchannel 和 show ip interface brief 查看并了解相关配置信息。
2. 在 PC1 上使用命令 ping 测试到 PC2 的网络是否连通。
3. 断开 SW1 和 SW2 之间的任一条链路，再在 PC1 上使用命令 ping 测试到 PC2 的网络是否连通。

实验 2.3 交换机的快速生成树配置

1. 实验目的

掌握交换机快速生成树协议配置配置方法，为将来从事网络工程建设打下基础。

2. 实验设备

思科模拟器 Cisco Packet Tracer（软件）

3. 实验任务

在思科模拟器中按照图 2-3 所示完成实验连接图，在两台交换机上配置 PVST+，使 SW1 为 VLAN 1 的根桥，SW2 为 VLAN2 的根桥，PC1 和 PC2 之间能够通信。

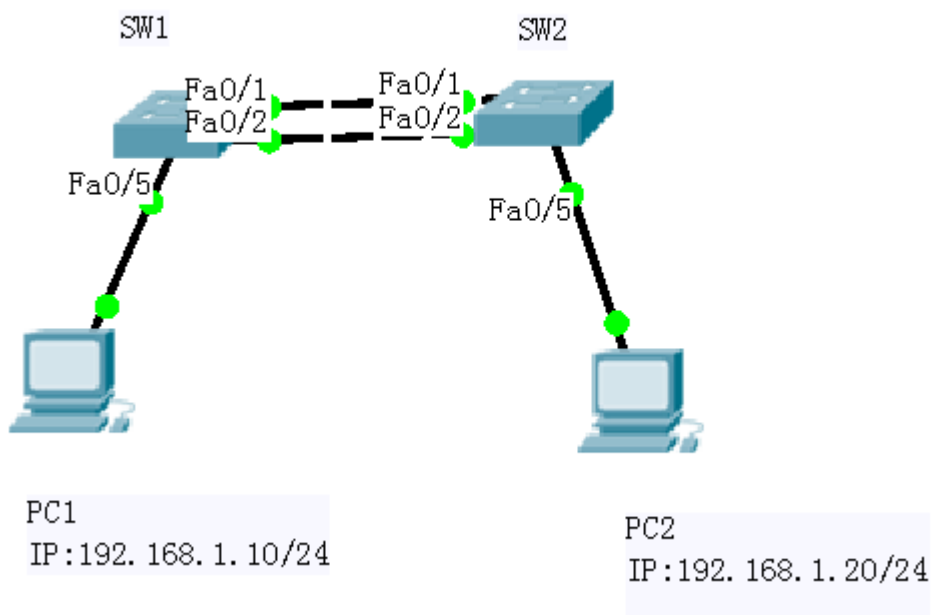
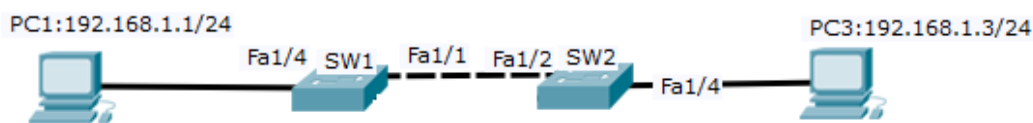


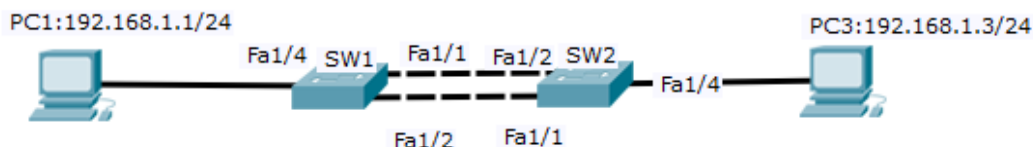
图 2-3 快速生成树配置网络连接图

4. 实验原理

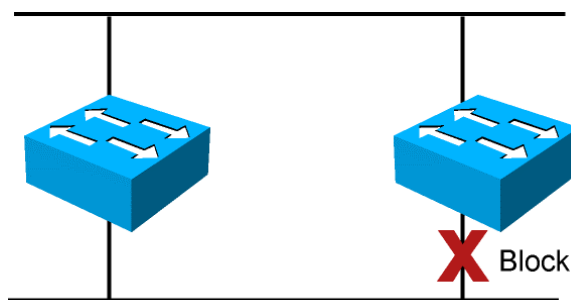
单一的网络环境并不可靠，当 SW1 和 SW2 之间链路发生故障时，PC1 和 PC3 将无法通信，如图所示。



为了解决单一链路故障引起的网络问题,一般在 SW1 和 SW2 之间再增加一条链路,如图所示。



冗余链路虽然解决了单链路故障引起的网络问题,却带来了环路,会造成广播风暴、MAC 地址表不稳定、重复帧拷贝等问题。此时,需要配置 STP 生成树协议来解决环路问题。STP 通过将特定的端口选为 Blocking 状态,来实现无环的拓扑。如下图所示:



思科交换机上可以配置两种生成树协议:

1. **PVST: Per-VLAN Spanning Tree** (每 VLAN 生成树), PVST 是解决在虚拟局域网上处理生成树的 cisco 特有解决方案。PVST 为每个虚拟局域网运行单独的生成树实例。但是此协议和其它厂商设备不能兼容。思科交换机上默认配置此协议。
2. **PVST+: (Per VLAN Spanning Tree Plus, 增强的按 VLAN 生成树)** 是 cisco 解决在虚拟局域网上处理生成树问题的另一个方案。PVST+ 允许 CST (公共生成树)信息传给 PVST,以便与其他厂商对在 VLAN 上运行生成树的实现方法进行操作。

5. 实验步骤

第一步: 完成网络连接图

参考图 2-3, 在思科模拟器中完成网络连接图 (无需标记文字), 注意交换机和 PC 之间用直连线, 交换机和交换机之间用交叉线连接。

第二步: 配置 SW1

以下为 SW1 配置命令，其中加粗斜体字为需要输入的命令，斜体字为交换机提示信息，! 后是说明文字。

Switch>**en**

Switch #**config t**

Enter configuration commands, one per line. End with CNTL/Z.

Switch (config)#**hostname SW1**

! 将交换机命名为 SW1

SW1 (config)**vlan 2**

SW1 (config-vlan)**exit**

! 创建 VLAN 2

SW1 (config-if) **int range fa 0/1-2**

! 同时选中 fa0/1 和 fa0/2 两个接口，注意空格。

SW1 (config-if-range)**sw mode trunk**

! 指定接口 fa0/1 和 fa0/2 模式为 trunk

SW1 (config-if-range)**exit**

SW1 (config)**spanning-tree mode rapid-pvst**

! 设置生成树协议为 PVST+

SW1 (config)**spanning-tree vlan 1 priority 4096**

! 将 VLAN 1 的优先级设置为最高（越小越高，以 4096 为一个等级），使 SW1 成为根桥。

SW1 (config)**spanning-tree vlan 2 priority 8192**

! 将 VLAN 2 的优先级设置为次高，使 SW1 成为备份根桥。

SW1 (config)**exit**

第三步：配置 SW2

参考 SW1，完成 SW2 的配置。注意 SW2 为 VLAN1 备份根桥，VLAN2 的根桥。

第四步：完成 PC1、PC2 的 IP 配置

参考图 2-3，完成 PC1、PC2 的 IP 配置。

6. 实验评测

1. 在 SW1 和 SW2 上使用命令 `show spanning-tree` 查看并了解相关配置信息。
2. 在 PC1 上使用命令 `ping` 测试到 PC2 的网络是否连通。
3. 断开 SW1 和 SW2 之间的任一条链路，再在 PC1 上使用命令 `ping` 测试到 PC2 的网络是否连通。

实验 2.4 交换机 HSRP 配置实验

1. 实验目的

掌握交换机 HSRP 配置方法，为将来从事网络工程建设打下基础。

2. 实验设备

思科模拟器 Cisco Packet Tracer（软件）

3. 实验任务

在思科模拟器中按照图 2-2 所示完成实验连接图，在 SW3、SW4 交换机上为 fa0/21 和 fa0/22 配置端口聚合，在 SW3、SW4 交换机上配置 HSRP 协议，使 SW3 或 SW4 损坏后，PC1、PC2、PC3、PC4 之间仍然能够通信。

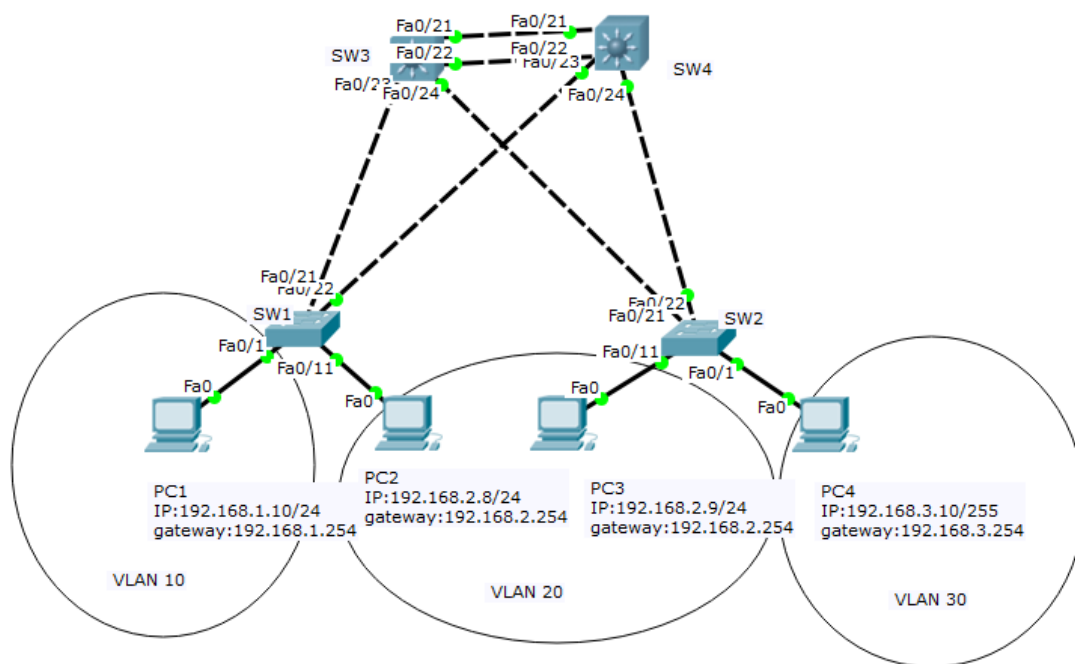
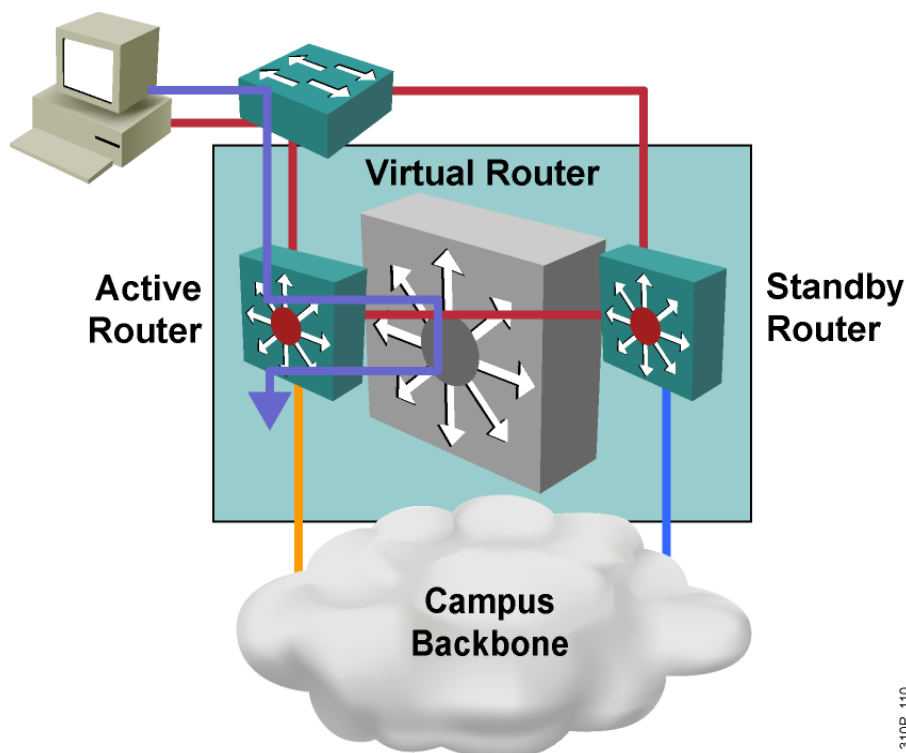


图 2-4 HSRP 配置网络连接图

4. 实验原理

HSRP: Hot Standby Router Protocol,热备份路由器协议是 cisco 平台一种特有的技术，是 cisco 的私有协议。

活动路由器（Active Router）负责转发数据包的路由器。一旦主动路由器出现故障，HSRP 将激活备份路由器（Standby Routers）取代主动路由器。HSRP 协议提供了一种决定使用主动路由器还是备份路由器的机制，并指定一个虚拟的 IP 地址作为网络系统的缺省网关地址。如果主动路由器出现故障，备份路由器（Standby Routers）承接主动路由器的所有任务，并且不会导致主机连通中断现象。如下图所示：



310P_110

5. 实验步骤

第一步：完成网络连接图

参考图 2-4，在思科模拟器中完成网络连接图（无需标记文字），注意交换机和 PC 之间用直连线，交换机和交换机之间用交叉线连接。

第二步：配置 SW1、SW2

请参考前面实验在 SW1、SW2 上命名、创建 VLAN，划分端口、设置干线模式。

第二步：配置 SW3、SW4

请参考前面实验在 SW3、SW4 上命名、创建 VLAN、划分端口、设置干线模式、开启路由功能、配置各 VLAN 的 IP 地址。

SW3 上的 HSRP 配置说明，其中加粗斜体字为需要输入的命令，斜体字为交换机提示信息！后是说明文字。

SW3(config)#int vlan 10

SW3(config-if)standby 10 ip 192.168.1.254

！设置 HSRP 组号，并设置虚拟路由器的 ip 地址（该地址是 vlan10 的虚拟网关 IP 地址）

SW3(config-if)standby 10 priority 200

！设置本交换机在 HSRP 组的优先级为 200，使交换机成为 vlan10 的活跃路由器

SW3(config-if)standby 10 preempt

! 配置占先权，让其成为本 vlan 的活跃路由器

SW3(config-if)int vlan 20

SW3(config-if)standby 20 ip 192.168.2.254

! 设置 HSRP 组号，并设置虚拟路由器的 ip 地址（该地址是 vlan10 的虚拟网关 IP 地址）

SW3(config-if)standby 20 priority 150

! 设置本交换机在 HSRP 组的优先级为 150，使本交换机成为 vlan 20 的备份路由器

SW3(config-if)int vlan 30

SW3(config-if)standby 30 ip 192.168.3.254

! 设置 HSRP 组号，并设置虚拟路由器的 ip 地址（该地址是 vlan30 的虚拟网关 IP 地址）

SW3(config-if)standby 30 priority 200

! 设置本交换机在 HSRP 组的优先级为 200，使交换机成为 vlan30 的活跃路由器

SW3(config-if)standby 30 preempt

! 配置占先权，让其成为本 vlan 的活跃路由器

参考 SW3 上的 HSRP 配置说明完成 SW4 上的 HSRP 配置。请注意 SW3 上的活跃路由器，SW4 则为备份路由器；SW3 上的备份路由器，SW4 则为活跃路由器。

6. 实验评测

1. 在 SW3 和 SW4 上使用命令用 show standby brief 查看 HSRP 配置信息。
2. 使用命令 ping 测试 PC1、PC2、PC3、PC4 的网络是否连通。
3. 删除 SW3 或 SW4，使用命令 ping 测试 PC1、PC2、PC3、PC4 的网络是否连通。此时再使用命令用 show standby brief 查看 HSRP 配置信息的变化。

思考问题

- (1) 为什么需要对局域网进行 VLAN 划分？划分的原则是什么？
- (2) 故意将交换机组成一个具有环路的网络，在交换机启动和停止 Spanning Tree 协议的情况下，观察网络的运行情况？
- (3) 实验 2-3 中 VLAN1 的流量走哪条线路，VLAN2 的流量走哪条线路，如果断开某条线路会有什么变化？

第三章 路由器配置

目前路由器的生产的厂家有许多，但其功能、配置方法大同小异，本实验以锐捷的产品为例进行介绍。

路由器的配置主要包括基本参数的配置和功能配置，功能配置主要包括局域网 LAN 接口和广域网 WAN 接口配置、路由协议配置和广域网协议的配置。对路由器进行配置一般有两种途径，即通过串口通信进行本地配置和通过网络进行远程配置，但后一种配置方法只有在前一种配置成功后才可进行，下面分别讲述。

实验 3.1 路由器的基本配置（直连网络）

1. 实验目的

通过对路由器安装与配置实验，加深对相关网络设备工作原理理解，掌握其常见产品的安装与配置方法，为将来从事网络工程建设打下基础。

2. 实验设备

思科模拟器 Cisco Packet Tracer（软件）

3. 实验任务

在思科模拟器中按照图 3-1 所示完成实验连接图，按照要求完成配置后在 PC1、PC2、PC3 上测试能连通的网络。

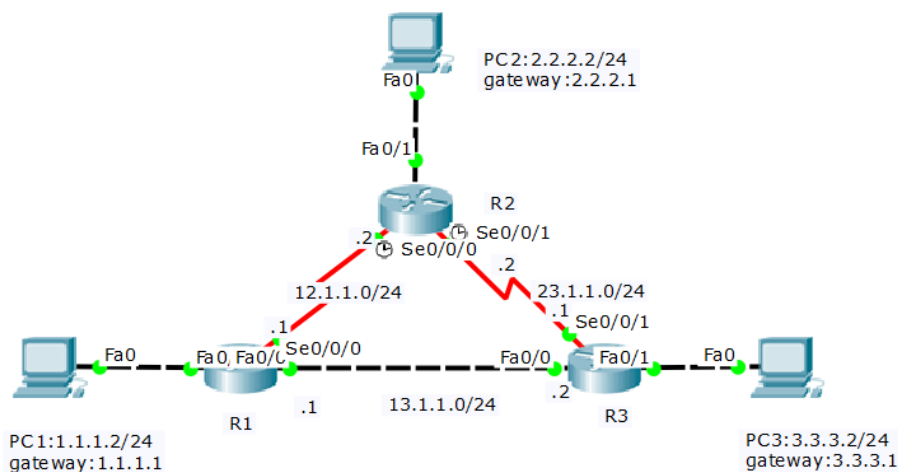


图 3-1 路由器的基本配置网络连接图

4. 实验原理

(1) 路由器的命令模式

路由器配置命令主要有以下几种模式：

- 一般模式：提示符为>，只能进行查看路由器的基本信息 show、ping、telnet 等操作；
- 特权模式：提示符为#，除了一般模式的操作外，可以进入各种操作配置模式；
- 全局模式：提示符为 (config) #，可以对路由器的全局参数进行配置；
- 接口模式：提示符为 (config-if) #，对路由器的接口进行配置。

在某模式下只能执行当前模式允许的命令，路由器的命令不能跨模式执行。

从一般模式进入特权模式：

Router>enable

输入密码后即可进入特权操作模式。

从特权模式进入全局模式：

Router #config terminal

从全局模式进入接口模式：

Router (config) #interface 接口编号 (例如：fastethernet 0/1)

输入 exit 将从当前模式返回到上一级模式，输入 end 或 Ctrl+Z 将直接返回到特权模式。

(2) 帮助信息

- 命令速查：在任意命令模式下，输入 ? 将列出在当前模式下可以进行的操作命令及其功能说明：如：

Router >?

disable Turn off privileged commands

enable Turn on privileged commands

exit Exit from the EXEC

.....

- 命令帮助：在任意一个命令后面输入 ? 将列出该命令后面所需的参数，如：

Router #show ?

- 命令简写：路由器的命令在没有二义性的前提下可以简写，如：

Router #conf t 代表 config terminal 命令

- 命令补齐：当输入一个命令时如果不记得后面的拼写规则或参数时，可以按 TAB 键自动将命令或参数补齐，如：
Router #con 按键盘的 TAB 键后将自动补齐为 config。

5. 实验步骤

第一步：完成网络连接图

参考图 2-4，在思科模拟器中完成网络连接图（无需标记文字），注意交换机和 PC 之间用直连线，交换机和交换机之间用交叉线连接；注意 R2 的 S0/0/0 和 R1 的 S0/0/0 使用串口线 DCE 连接，而且 R2 的 S0/0/0 是 DCE 端需要配置时钟；R2 的 S0/0/1 和 R3 的 S0/0/1 使用串口线 DCE 连接，而且 R2 的 S0/0/1 是 DCE 端需要配置时钟。

第二步：配置 R1、R2、R3

以下为 R1 配置命令，其中加粗斜体字为需要输入的命令，斜体字为交换机提示信息，! 后是说明文字。

Router>*en*

Router#*config t*

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#*hostname R1*

! 将路由器命名为 R1

R1(config)#*int fa0/1*

R1(config-if)#*ip add 1.1.1.1 255.255.255.0*

! 为接口 fa0/1 配置 IP 地址

R1(config-if)#*no shut*

! 启用端口

R1(config-if)#*exit*

R1(config)#*int fa0/0*

R1(config-if)#*ip add 13.1.1.1 255.255.255.0*

! 为接口 fa0/0 配置 IP 地址

R1(config-if)#*no shut*

! 启用端口

R1(config-if)#*exit*

R1(config)#*int s0/0/0*

! 为接口 s0/0/0 配置 IP 地址

R1(config-if)#*ip add 12.1.1.1 255.255.255.0*

R1(config-if)#*no shut*

! 启用端口

R1(config-if)#*exit*

参考 R1 配置完成 R2 和 R3 的配置。注意 R2 接口 DCE 端配置时钟。

DCE 端时钟配置命令：

Router (config-if) #*clock rate 56000*

!在接口模式下配置时钟

第三步：配置 PC1、PC2、PC3 的 IP 信息

参考图 3-1 完成 PC1-3 的 IP 配置，注意网关地址为 PC 所接路由器接口地址。

6. 实验评测

1. 在 R1 上使用命令 `show ip interface brief` 查看接口配置信息。
2. 在 R1、R2 和 R3 上使用命令 `show ip route` 查看路由表中生成的直连路由。
3. 使用命令 `ping` 测试 PC1、PC2、PC3 各自能够连通哪个网段。

实验 3.2 静态路由配置实验

1. 实验目的

通过对路由器静态路由的配置实验，加深对相路由器工作原理理解，掌握静态路由的配置方法，为将来从事网络工程建设打下基础。

2. 实验设备

思科模拟器 Cisco Packet Tracer（软件）

3. 实验任务

复制实验 3.1 的文件，在实验 3.1 基础上为三个路由器配置静态路由，按照要求完成配置后在 PC1、PC2、PC3 上测试能连通的网络。

4. 实验原理

所谓静态路由是指路由表中的路由信息是手工添加的，路由器之间不需要进行路由信息交换。静态路由策略适合于网络拓扑结构简单且固定的网络中。

在路由器中静态路由的配置命令一般为：

Router#configure terminal

Router (config) # ip route 目的网络号 网络掩码 下一跳路由器 IP 地址/本地接口

删除静态路由的命令为：

Router# no ip route 目的网络号 网络掩码

路由表中的静态路由在路由表中用 S 标出，包含：网络地址和子网掩码以及路由下一跳 IP 地址或出接口。如下图。在静态或动态路由被使用之前，路由表中必须包含与远程网络相关的直连路由，直连路由在路由表中用 C 标出。如下图。

```

R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

S    192.168.4.0/24 is directly connected, Serial1/0
C    192.168.5.0/24 is directly connected, Loopback0
C    192.168.6.0/24 is directly connected, Loopback1
C    192.168.1.0/24 is directly connected, Serial1/0
S    192.168.3.0/24 [1/0] via 192.168.1.1

```

静态路由配置步骤：

1. 为路由器每个接口配置 IP 地址
2. 确定本路由器有哪些直连网段
3. 确定网络中有哪些属于本路由器的非直连网段
4. 在路由表中添加所有本路由器的非直连网段

5. 实验步骤

复制实验 3.1 文件，在实验 3.1 基础上完成以下步骤

第一步：在 R1 上配置静态路由

R1 配置静态路由示例

```
R1(config)#ip route 23.1.1.0 255.255.255.0 12.1.1.2
```

```
R1(config)#ip route 3.3.3.0 255.255.255.0 13.1.1.2
```

```
R1(config)#ip route 2.2.2.0 255.255.255.0 12.1.1.2
```

或者路由器 1 设置默认路由，即当没有找到到目的网络的路由时，将包转发给默认路由器。

```
R1(config)#ip route 0.0.0.0 0.0.0.0 12.1.1.2
```

参考上述 R1 配置示例，完成 R2 的静态路由配置。

第二步：在 R2 上配置静态路由

参考上述 R1 配置示例，完成 R2 的静态路由配置。

第三步：在 R3 上配置静态路由

参考上述 R1 配置示例，完成 R3 的静态路由配置。

6. 实验评测

1. 在 R1、R2 和 R3 上使用命令用 show ip route 查看路由表。
2. 使用命令 ping 测试 PC1、PC2、PC3 各自能够连通哪个网段。

Router (config)#version 2

！ 设置 RIP 的版本号

5. 实验步骤

复制实验 3.1 文件，在实验 3.1 基础上完成以下步骤

第一步：在 R1 上配置 RIP 协议

R1 配置 RIP 协议示例：

R1(config)#router rip

！ 启动 RIP 协议

R1(config-router)#net 1.0.0.0

！ 申明本设备上直连的网络

R1(config-router)#net 12.0.0.0

！ 申明本设备上直连的网络 1

R1(config-router)#net 13.0.0.0

！ 申明本设备上直连的网络 1

R1(config-router)#version 2

！ 使用 RIP 2 版本

注意：如果申明直连网络错误，请使用命令 `no net` 目的网络号删除申明，否则不能正常运行 RIP 协议，网络无法连通

输入命令 `show run` 查看配置信息中的 RIP 配置是否正确，如果错误，请删除相应的申请，重新配置。

第二步：在 R2 上配置 RIP 协议

参考上述 R1 配置示例，完成 R2 的 RIP 协议配置。输入命令 `show run` 查看配置信息中的 RIP 配置是否正确，如果错误，请删除相应的申请，重新配置。

第三步：在 R3 上配置 RIP 协议

参考上述 R1 配置示例，完成 R3 的 RIP 协议配置。输入命令 `show run` 查看配置信息中的 RIP 配置是否正确，如果错误，请删除相应的申请，重新配置。

6. 实验评测

- 1.在 R1、R2 和 R3 上使用命令用 `show ip route` 查看路由表。
- 2.在 R1 上输入命令 `show ip protocols`，查看 RIP 协议的详细信息。
- 3.在 R1 上运行 `debug ip rip`，查看 rip 协议运行过程。
- 4.使用命令 `ping` 测试 PC1、PC2、PC3 各自能够连通哪个网段。
- 5.断开 R1 和 R2 的链路，再次使用命令 `ping` 测试 PC1、PC2、PC3 各自能够连通哪个网段。

实验 3.4 OSPF 路由协议配置实验

1. 实验目的

通过对路由器 OSPF 协议配置实验，加深对相路由器工作原理理解，掌握 OSPF 路由协议的配置方法，为将来从事网络工程建设打下基础。

2. 实验设备

思科模拟器 Cisco Packet Tracer（软件）

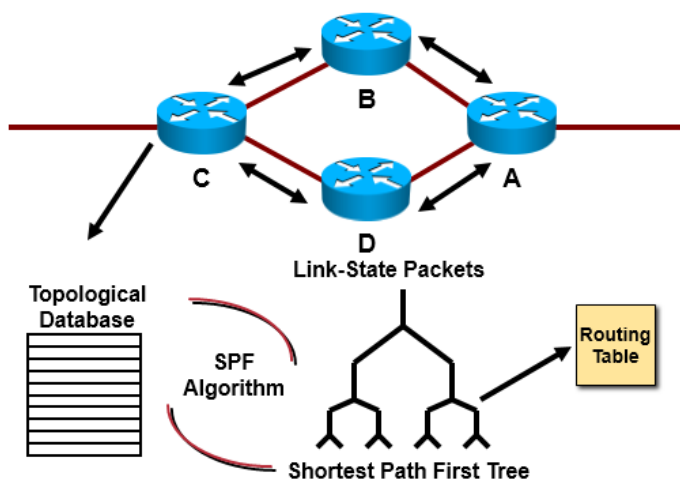
3. 实验任务

复制实验 3.1 的文件，在实验 3.1 基础上为三个路由器配置 OSPF 协议，按照要求完成配置后在 PC1、PC2、PC3 上测试能连通的网络。

4. 实验原理

OSPF（Open Shortest Path First，开放式最短路径优先）协议是目前网络中应用最广泛的路由协议之一。OSPF 属于内部网关路由协议，能够适应各种规模的网络环境，是典型的链路状态（link-state）协议。

OSPF 路由协议通过向全网扩散本设备的链路状态信息，使网络中每台设备最终同步一个具有全网链路状态的数据库（LSDB），然后路由器采用 SPF 算法，以自己为根，计算到达其他网络的最短路径，最终形成全网路由信息，具体过程如图所示。



OSPF 的三张表:

1. 邻居表 (neighbor table): OSPF 用邻居机制来发现和维持路由的存在, 邻居表存储了双向通信的邻居关系 OSPF 路由器列表的信息。
2. 拓扑表 (topology table): OSPF 用 LSA (link state Advertisement 链路状态通告) 来描述网络拓扑信息, 然后 OSPF 路由器用拓扑数据库来存储网络的这些 LSA。
3. OSPF 路由表 (routing table): 链路状态数据库进行 SPF (Dijkstra) 计算, 而得出的 OSPF 路由表。

OSPF 路由协议的配置方法为:

Router#configure terminal

! 启动 OSPF 协议, process-id 为进程号

Router (config)#router ospf process-id

! 申明本路由器上直连的网络号, 并分配区域号

Router (config)#network 目的网络号1 网络1 掩码的反码 area Area-id

.....

Router (config)#network 目的网络号n 网络n 掩码的反码 area Area-id

5. 实验步骤

复制实验 3.1 文件, 在实验 3.1 基础上完成以下步骤

第一步: 在 R1 上配置 OSPF 协议

R1 配置 RIP 协议示例:

R1(config)#router ospf 1

! 启动 OSPF 协议

R1(config-router)#net 1.1.1.0 0.0.0.255 area 0

!申明本路由器上的直连网络, 并分配区域号。

R1(config-router)#net 12.1.1.0 0.0.0.255 area 0

!申明本路由器上的直连网络, 并分配区域号。

R1(config-router)#net 13.1.1.0 0.0.0.255 area 0

!申明本路由器上的直连网络, 并分配区域号。

注意: 如果申明直连网络错误, 请使用命令 **no net** 目的网络号删除申明, 否则不能正常运行 OSPF 协议, 网络无法连通

第二步: 在 R2 上配置 OSPF 协议

参考上述 R1 配置示例, 完成 R2 的 OSPF 协议配置。输入命令 **show run** 查看配置信息中的 RIP 配置是否正确, 如果错误, 请删除相应的申请, 重新配置。

第三步: 在 R3 上配置 OSPF 协议

参考上述 R1 配置示例, 完成 R3 的 OSPF 协议配置。输入命令 **show run** 查看配置信息中的 RIP 配置是否正确, 如果错误, 请删除相应的申请, 重新配置。

6. 实验评测

- 1.在 R1、R2 和 R3 上使用命令用 `show ip route` 查看路由表。
- 2.在 R1 上输入命令 `show ip protocols`，查看 OSPF 协议的详细信息。
- 3.使用命令 `ping` 测试 PC1、PC2、PC3 各自能够连通哪个网段。
- 4.断开 R1 和 R2 的链路，再次使用命令 `ping` 测试 PC1、PC2、PC3 各自能够连通哪个网段。

实验 3.5 实战训练

1. 实验目的

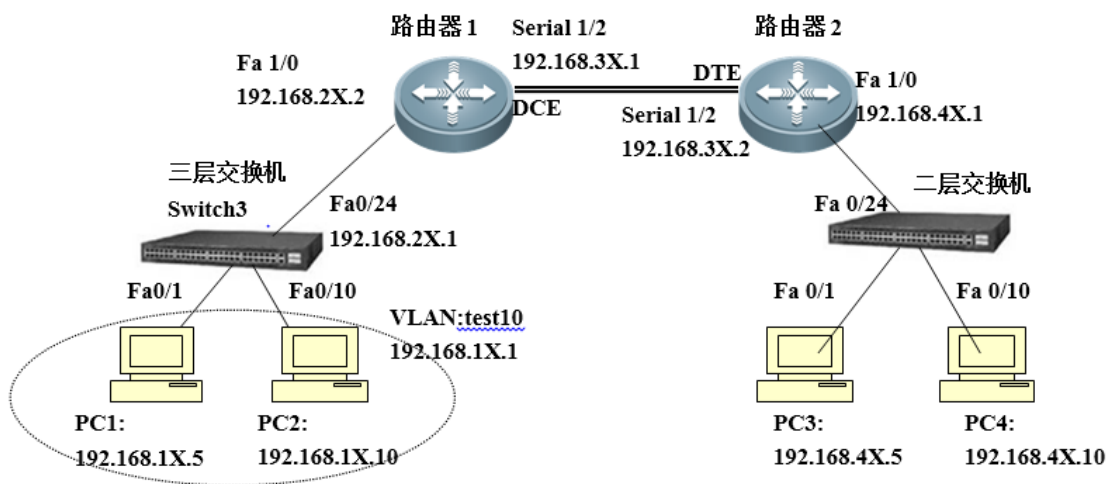
加深对路由器工作原理理解，掌握不同路由协议的配置方法，为将来从事网络工程建设打下基础。

2. 实验设备

- 用于配置和测试的计算机四台以上（安装 Windows 操作系统）；
- 路由器二台；
- 二层交换机二台；
- 三层交换机一台；
- V.35 电缆一对（V.35 DCE 和 V.35 DTE 电缆各一根）。

3. 实验任务

在实际机柜中使用设备分组完成下面的网络连接图，并选择合适路由协议，完成相关配置，使各 PC 之间能够连通。



实验 3-5 实战训练网络连线图

4. 实验原理

参考本单元其它实验。

5. 实验步骤

5.1 三层交换机 VLAN 配置

在三层交换机上配置两个 VLAN（test10 和 test20）：

```
switch3#configure terminal
switch3 (config)#vlan 10                ! 创建一个编号为 10 的 VLAN
switch3 (config-vlan)#name test10        ! 将编号为 10 的 VLAN 命名为 test10

switch3 (config)#vlan 20                ! 创建一个编号为 20 的 VLAN
switch3 (config-vlan)#name test20        ! 将编号为 20 的 VLAN 命名为 test20

switch3 (config)#interface fa0/1         ! 选中 fa0/1
switch3 (config-if)#switchport access vlan 10 ! 将 fa0/1 加入到 test10

switch3 (config)#interface fa0/10        ! 选中 fa0/10
switch3 (config-if)#switchport access vlan 10 ! 将 fa0/1 加入到 test10
switch3 (config)#interface fa0/24        ! 选中 fa0/24
switch3 (config-if)#switchport access vlan 20 ! 将 fa0/1 加入到 test20

switch3 (config)#interface vlan 10
switch3 (config-if)#ip address 192.168.1X.1 255.255.255.0
switch3 (config-if)#no shutdown          ! 激活 VLAN 10
switch3 (config-if)#exit

switch3 (config)#interface vlan 20
switch3 (config-if)#ip address 192.168.2X.1 255.255.255.0
switch3 (config-if)#no shutdown          ! 激活 VLAN 20
switch3 (config-if)#exit

switch3#show vlan                        ! 查看 VLAN 的创建情况
```

5.2 路由器接口 IP 地址配置

(1) 路由器 1 网络接口配置

```
router1#configure terminal
router1 (config)#interface fa 1/0        ! 选中 fa1/0
router1 (config-if)#ip address 192.168.2X.2 255.255.255.0
router1 (config-if)#no shutdown          ! 激活 fa1/0
router1 (config-if)#exit

router1 (config)#interface serial 1/2    ! 选中 fa1/0
```

```
router1 (config-if)#ip address 192.168.3X.1 255.255.255.0
router1 (config-if)#clock rate 64000
router1 (config-if)#no shutdown          ! 激活 serial 1/2
router1 (config-if)#exit
```

```
router1#show ip interface brief
```

(2) 路由器 2 网络接口配置

```
router2#configure terminal
router2 (config)#interface serial 1/2          ! 选中 fa1/0
router2 (config-if)#ip address 192.168.3X.2 255.255.255.0
router2 (config-if)#no shutdown                ! 激活 serial 1/2
router2 (config-if)#exit
```

```
router2 (config)#interface fa 1/0              ! 选中 fa1/0
router2 (config-if)#ip address 192.168.4X.1 255.255.255.0
router2 (config-if)#no shutdown                ! 激活 fa1/0
router2 (config-if)#exit
```

```
router2#show ip interface brief
```

5.3 路由协议配置

下面以 OSPF 协议配置为例

(1) 三层交换机 OSPF 协议配置

```
switch3#configure terminal
switch3 (config)#router ospf                ! 启动 OSPF 协议

! 申明本设备上直连的网络，并分配区域号
switch3 (config)#network 192.168.1X.0 0.0.0.255 area 0
switch3 (config)#network 192.168.2X.0 0.0.0.255 area 0
switch3 (config)#end
```

(2) 路由器 1 OSPF 协议配置

```
router1 #configure terminal
router1 (config)#router ospf                ! 启动 OSPF 协议

! 申明本设备上直连的网络，并分配区域号
router1 (config)#network 192.168.2X.0 0.0.0.255 area 0
router1 (config)#network 192.168.3X.0 0.0.0.255 area 0
router1 (config)#end
```

(3) 路由器 2 OSPF 协议配置

```
router2 #configure terminal
```

```
router2 (config)#end
```

第四章 服务器相关服务的安装与配置

Web 服务是 Internet 最基本的服务之一，目前提供 Web 服务的软件主要有 Windows 环境下的 IIS 和 Unix 环境下的 Apache，由于 Apache 的稳定性、源代码开放性、可扩展性和免费等特点，Apache 是目前使用最广的 Web 服务器系统，大多数网站的 Web 服务器系统都采用的是 Apache，据权威机构最新统计，目前 Apache 的市场份额超过 70%。

Apache 由“The Apache Software Foundation”维护，其官方网站地址为：<http://www.apache.org/>，目前最新版本为 Apache 2.2，可以运行在所有的 Unix（如 Linux/Sco unix/Solaris/HP Unix/IBM AIX 等）和 Windows 等操作系统下，在官方网站 <http://httpd.apache.org/download.cgi> 或镜像网站上可以下载最新版本的源代码或执行代码。

邮件系统是目前应用最广的 Internet 服务，它在信息交流方面给人们的工作和生活带来了极大的便利。Sendmail 和 qpopper 是目前使用较多的 SMTP 和 POP3 邮件服务器，特别适合于非专业邮件服务企业的邮件收发服务。

本章学习 WEB 服务器和邮件服务器的安装和配置。

实验 4.1 Apache 的安装与基本配置

1. 实验目的

通过对 Apache Web 服务器系统的安装与配置实验，加深对 HTTP 协议、HTML 语言的理解，掌握 Apache 服务器的安装与配置方法，为将来从事网络工程建设打下基础。

2. 实验要求

下载 Apache WEB 服务器源代码，在 Linux 环境下，编译生成执行代码，并进行安装和基本配置，然后设计一个用于测试的网页，分别在本机和网络中其它计算机上访问该测试网页，测试 Apache Web 服务器系统工作是否正常。

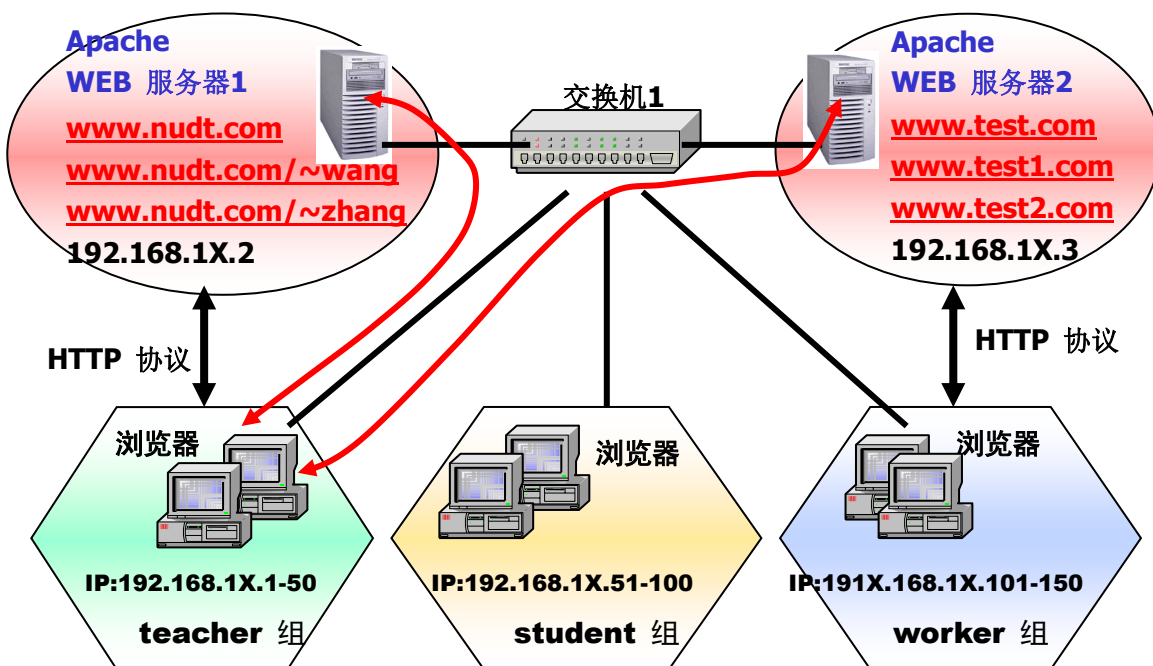
3. 实验环境

（1）实验设备

- PC 服务器（Linux 操作系统，安置 GCC）2 台；
- 交换机 1 台；
- PC 机若干台；
- Apache 源代码安装包 `Apache-2.0.49.tar.gz`。

(2) 网络拓扑

如图 1-1 所示，其中 IP 地址中的 X 表示实验工作台的编号（下同）。



(图 4-1 WEB服务器配置实验拓扑图)

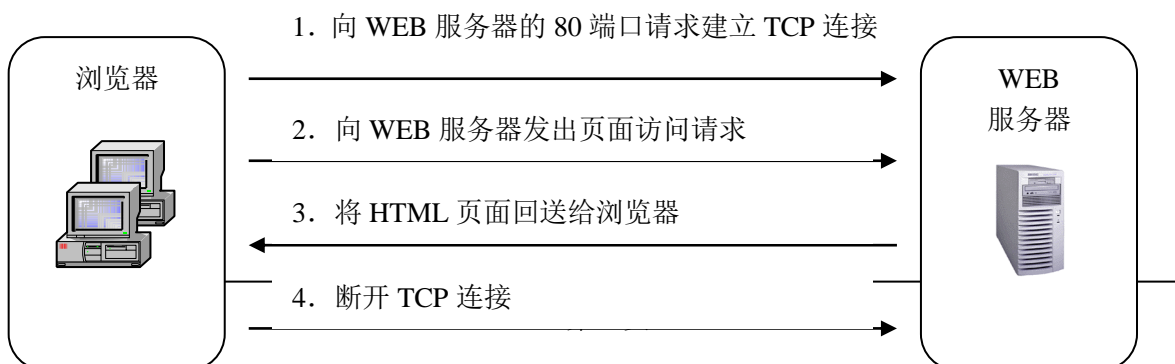
4. 实验原理

Web 服务采用 HTTP 协议（Hypertext Transfer Protocol，即超文本传输协议）在客户端与服务之间进行通信，其服务端的 TCP 端口缺省为 80，客户端与服务器的通信过程如图 1-2 所示：

(1) 客户端（浏览器）请求与 Web 服务器建立 TCP 连接，连接建立以后，向 Web 服务器发出访问请求（如 get）。根据 HTTP 协议，该请求中包含了客户端的 IP 地址、浏览器的类型和请求的 URL 等一系列信息；

(2) Web 服务器收到请求后，将客户端要求访问的页面内容（采用 HTML: Hypertext Markup Language，即超文本标记语言编写）返回到客户端，浏览器将页面显示出来。如果出现错误，如请求的页面不存在等，则返回错误代码；

(3) 客户端断开与 Web 服务器的连接，本次通信结束。如果客户端还需访问其它页面，则重复上述过程，也就是说 HTTP 协议采用的是“短连接”。



(图 4-2 浏览器与Web 服务器通信过程)

5. 实验步骤

5.1 实验准备

(1) 下载源代码

Apache 最新版本的源代码可以从 Apache Software Foundation 网站上：<http://httpd.apache.org/download.cgi> 或其镜像站点下载，本书附带的光盘上包括了 Apache-2.0.49 版本的原代码。

(2) 源代码解包

将下载的安装包 `Apache-2.0.49.tar.gz` 复制到某一个用户目录下（下面以 `/usr/src/` 目录为例介绍），然后用以下命令解压：

```
$ cd /usr/src
$ tar xvfz Apache-2.0.49.tar.gz
```

将会在 `/usr/src/` 目录下创建 `/httpd-2.0.49` 子目录，该目录下包含 apache 的所有源代码和相关文档。

5.2 编译设置

Apache 是一个由多模块组成的安装包，其功能可以根据不同的应用需求进行裁剪，另外，Apache 还可以在不同的操作系统环境下安装，由于不同的操作系统其编译库可能不完全相同，所以必须设置好当前操作系统下编译参数，此外，还需要设置好 Apache 系统的安装目录，这些工作可以通过 `/httpd-2.0.49` 目录下的 `configure` 脚本来进行裁剪和检测，并形成下一步编译的 `Makefile` 文件。

执行 `./configure --help` 可显示 Apache 可以设置的参数或裁剪的模块及其简要说明：

```
$ cd /usr/src/httpd-2.0.49
$ ./configure --help
```

除了以下几个参数可能需要更改外，一般情况下，使用系统默认的设置就可以了。

(1) 安装路径名

Apache 默认的安装路径名为 `/usr/local/apache`，如果需要，你可以通过 `--prefix` 参数指定一个其他安装目录（如 `/usr/local/Web`）：

```
--prefix=/usr/local/Web
```

(2) 功能模块

基本服务器安装包中包含了最常用的功能模块，如果要安装某扩展功能模块，

则需要在编译时指定包含之, 同样, 对于某个基本功能模块 (在 Apache 文档中有模块清单备查, 其中状态为“Base”的为基本模块), 如果不需要安装, 则必须明确地禁用它:

编译并包含模块 MODULE:

```
--enable-MODULE
```

编译并包含用空格分隔的多个模块 MODULE-LIST:

```
--enable-modules=MODULE-LIST
```

禁止编译并包含模块 MODULE:

```
--disable-MODULE
```

编译并包含用空格分隔的 MODULE-LIST 成动态库 DSO:

```
--enable-mods-shared=MODULE-LIST
```

一般情况下使用默认模块设置就可以了, 下面的命令将配置基本的安装模块并告诉编译器将 Apache 安装在 `/usr/local/apache` 目录下:

```
$ cd /usr/src/httpd-2.0.49    (注: 如果当前已进入 httpd-2.0.49 目录,
    则省去本命令, 下同)
```

```
$ ./configure --prefix=/usr/local/apache
```

5.3 编译

根据 `./configure` 配置的模块和检测到编译参数 (保存在 Makefile 中) 执行以下命令就可以对 Apache 源代码进行编译:

```
$ cd /usr/src/httpd-2.0.49
```

```
$ make
```

对一个具有基本配置的 Apache 进行编译, 一般需要运行 3 分钟左右, 实际需要的时间因硬件和选择的模块数量不同会有较大差异。

正常情况下, 编译能顺利完成, 但如果操作系统或 C 语言编译器有问题, 则可能终止编译过程, 此时需要根据报告的错误进行相应的处理。

5.4 安装

如果编译正常完成, 就可以将 Apache 安装到上述 `--prefix` 指定的目录中 (如 `/usr/local/apache`), 命令如下:

```
$ cd /usr/src/httpd-2.0.49
```

```
$ make install
```

安装完成后, 可以清除编译生成的中间文件 (`.o`), 以释放磁盘空间:

```
$ cd /usr/src/httpd-2.0.49
```

```
$ make clean
```

注意: 如果由于某种原因, 需要重新 `./configure` 和编译时, 一定要 `make clean` 清除上次编译生成的中间文件, 否则编译器不会重新编译已有的文件, 导致重新编译无效。

5.5 配置

Apache 的运行配置文件放在 `/usr/local/apache/conf/httpd.conf` 中，通过编辑该文件控制 Apache 服务器运行，在 `/usr/local/apache/docs/manual/` 有 Apache 使用手册，在 <http://httpd.apache.org/docs/> 有完整的配置指令参考。

```
$ cd /usr/local/apache/conf
```

```
$ vi httpd.conf
```

通常需要修改配置文件 `httpd.conf` 中以下几个参数：

(1) 修改服务器名称

指定 HTTP 服务器的域名和服务端口：

```
ServerName www.test.com:80
```

如果已为你的服务器注册了域名 `www.test.com`，则可以通过该名字在网络上访问 WEB 服务器，但如果你没有注册域名，则只能通过你的 IP 地址访问你的 HTTP 服务器。

在注册域名前，为了能在本机上通过域名 www.test.com 访问该 Web 服务器，可以在本机的 `/etc/hosts` 文件尾部增加一项本地域名与 IP 地址对应表，以便在本机上测试访问 `www.test.com` 服务器（假设 HTTP 服务所在的机器 IP 地址为 192.168.1X.2，X 为你所在的实验组号）：

```
$vi /etc/hosts
```

```
192.168.1X.2 www.test.com
```

(2) 修改服务端口

缺省情况下，http 服务的 socket 服务端口为 80，你可以通过参数 **Listen** 修改：
Listen 80

(3) 修改文档目录

你的网页默认情况下是放在安装目录下的 `htdocs` 中（如：`/usr/local/apache/htdocs`），你可以通过参数 **DocumentRoot** 修改：

```
DocumentRoot /usr/local/apache/htdocs
```

(4) 修改出错信息、日志目录

HTTP 服务器出错信息和访问日志默认是放在安装目录中的 `logs/error_log` 和 `access_log` 中，你可以通过参数 **ErrorLog** 修改存放位置：

```
ErrorLog logs/error_log
```

日志的级别有 `debug/info/notice/warn/error/crit/alert/emerg`，可以通过参数 **LogLevel** 修改日志的级别：

```
LogLevel warn
```

你可以指定记录客户访问本服务器的日志目录和格式，将来可以用以分析服务器被访问的情况：

```
CustomLog logs/access_log common
```

(5) 修改支持的语言和编码

Apache 支持多种语言和编码，根据需要，可以指定网页默认的语言：

```
DefaultLanguage zh-CN
```

指定网页支持的语言和优先级别：

```
AddLanguage zh-CN .zh-cn
```

```
AddLanguage en .en
```

```
LanguagePriority zh-CN en
```

指定网页默认的字符集和支持的字符集：

```
AddDefaultCharset GB2312
```

```
AddCharset GB2312 .gb2312 .gb
```

5.6 运行与停止

可以执行以下命令手工启动你的 Apache HTTP 服务器：

```
$ cd /usr/local/apache/bin
```

```
$ ./apachectl start
```

然后可以通过以下命令来检查 HTTP 服务器进程(缺省时有 5 个，可配置)：

```
$ ps -A|grep httpd
```

HTTP 服务启动和运行时根据前面设置的参数写日志文件，你可以这样来动态观察 Apache 的启动与运行过程日志信息和出错信息：

```
tail -f /usr/local/apache/logs/access_log
```

```
tail -f /usr/local/apache/logs/error_log
```

如果 HTTP 服务器进程已运行，则你可以在本机上用 <http://localhost/> 或 <http://127.0.0.1/> 来访问你的测试网页了，这个网页位于 `/usr/local/apache/htdocs/`。

如果在其他机器上需要访问该服务器，则必须输入 <http://192.168.25.188> 才能访问。

注意，必须修改 HTTP 服务器上防火墙系统的设置（进入应用程序/系统设置/安全级别的设置界面），允许信任 HTTP 服务，否则无法访问该 HTTP 服务。

最后。你可以停止 HTTP 服务器：

```
$ cd /usr/local/apache/bin
```

```
$ ./apachectl stop
```

还可以编辑启动文件 `apache`，并将该文件放到 `/etc/rc.d/rc.local/init.d/`目录下，系统开机时自动启动 Web 服务器。

6、实验评测

按照上述步骤安装并配置 Apache 服务器，然后启动 Apache Web 服务后，并进行以下测试，以判断 Web 服务是否正常：

(1) 在服务器上测试

在服务器上启动浏览器，输入 <http://localhost/> 或 <http://192.168.1X.2> 或 <http://www.test.com>，能看到如图 1-3 所示的 Apache 默认测试网页（中文），如果看不到或显示的页面不是上图内容，则说明配置有问题。

自己设计一个测试网页，替代系统原来的网页，重复上述测试，如果能看到你设计的测试内容，则说明 Web 服务器工作正常。

(2) 在局域网内测试

在局域网另外一台计算机上启动浏览器，输入 <http://192.168.1X.2>，如果能看到你设计的测试内容，则说明 Web 服务器工作正常。

同样，在一台 Linux 机器上 `/etc/hosts` 文件尾部增加一项域名与 IP 地址对应表，以便能通过域名访问 www.test.com 服务器：

192.168.1X.2 www.test.com



(图 4-3 Apache 测试网页)

然后在浏览器中输入 <http://www.test.com>，应同样能看到你设计的测试内容。

在 Windows 机器只需要类似修改文件 `C:\WINDOWS\system32\drivers\etc\hosts`，也可以访问上述测试网页。

实验 4.2. 虚拟主机的配置

为了提供 WEB 服务，传统上必须自己设立一台 WEB 服务器，并连接到 Internet 上，从维护能力和资金上都有一定的要求。这一问题完全可以通过虚拟主机来解决。

所谓虚拟主机就是在同一台服务器上，同时提供多个 Web 服务，而且不同的服务互不干扰，对外就表现为多个不同的 WEB 服务器。

1. 实验目的

通过在 Apache 服务器系统上虚拟主机服务的配置实验，加深对虚拟主机服务的理解，掌握 Apache 服务器上虚拟主机服务的配置方法。

2. 实验要求

在 Apache 服务器上配置三个虚拟主机服务，三个虚拟主机的域名为 www.test1.com、www.test2.com、www.test3.com，设计三个不同的用于测试的网页，分别在本机上和网络中另一台主机上访问上述三个虚拟主机。

3. 实验环境

实验环境同实验 4.1。

4. 实验原理

实验原理同实验 4.1。

5. 实验步骤

在完成实验 4.1 的基础上，按以下步骤进行：

5.1 虚拟主机配置

为了在 Apache 服务器上配置虚拟主机服务，必须修改 Apache 的配置文件 /usr/local/apache/conf/httpd.conf 的以下内容：

允许启用基于名字虚拟主机服务（去掉命令前面的注解符 #）：
`NameVirtualHost * :80`

增加虚拟主机 1（域名为 `www.test1.com`）：

```
<VirtualHost *:80>
    ServerAdmin webmaster@www.test1.com
    DocumentRoot /usr/local/apache/htdocs/test1
    ServerName www.test1.com
    ErrorLog logs/test1/error_log
    CustomLog logs/test1/access_log common
</VirtualHost>
```

5.2 制作虚拟主机网页

根据上面虚拟主机文档目录 `DocumentRoot`，在 `/usr/local/apache/htdocs/` 目录下手工创建虚拟主机 `test1` 的子目录：

```
$cd /usr/local/apache/htdocs
$mkdir test1
```

设计虚拟主机 `test1` 的测试页面，并放置到目录 `/usr/local/apache/htdocs/test1` 下，或者将缺省的测试页面下列文件从 `/usr/local/apache/htdocs` 目录复制到 `test1` 中：

`apach_pb2_ani.gif`, `apach_pb2.png`, `apach_pb2.gif`, `apach_pb.png`,
`apach_pb.gif`, `index.html.var`, `index.html.zh-CN.gb2312`。

然后，在 `/etc/hosts` 文件中增加一项本地域名与 IP 地址对应表，以便能在本机上测试访问 `www.test1.com` 服务器：

```
192.168.1X.2 www.test1.com
```

创建日志文件夹 `logs/test1`。

重复上述步骤，同样可以设置虚拟主机 2（域名为 `www.test2.com`）和虚拟主机 3（域名为 `www.test3.com`）。

6. 实验评测

设计三个虚拟主机的测试主页，分别放在 `/usr/local/apache/htdocs/test1`、`test2`、`test3` 目录中，在服务器上的浏览器中分别访问 <http://www.test1.com>、<http://www.test2.com>、<http://www.test3.com>，如果能看到你设计的网页，则说明虚拟主机配置成功。

在网络中的另一台 linux 计算机的 `/etc/hosts` 文件尾部增加三项域名与 IP 地址对应表：

```
192.168.1X.2 www.test1.com
192.168.1X.2 www.test2.com
192.168.1X.2 www.test3.com
```

然后在浏览器中分别访问 <http://www.test1.com>、www.test2.com、www.test3.com 应该同样能看到你设计的三个虚拟主机的测试内容。

注：在当前版本中，如果启用了虚拟主机服务，则访问 www.test.com 时将变为访问第一个虚拟主机 www.test1.com。

实验 4.3 SMTP 服务器的安装与配置

1. 实验目的

通过对 Sendmail 服务器系统的安装与配置实验，加深对 SMTP 协议的理解，掌握 Sendmail 邮件服务器的安装与配置方法，为将来从事网络工程建设打下基础。

2. 实验要求

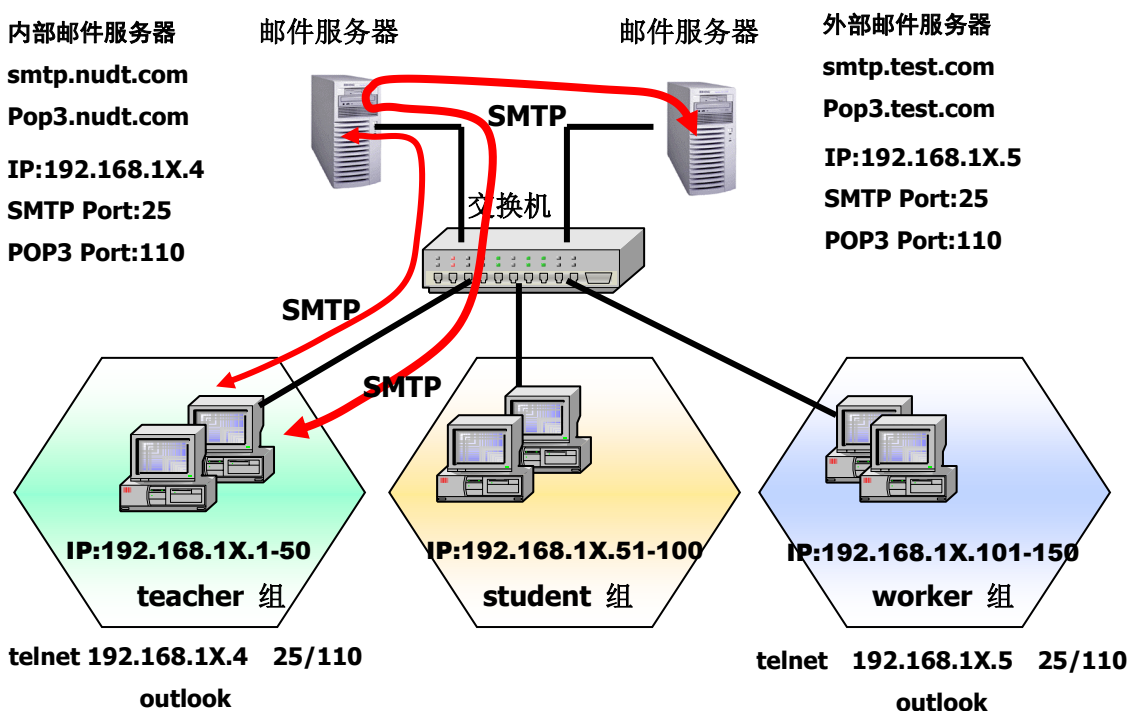
下载 Sendmail 服务器源代码，在 Linux 环境下，编译生成执行代码，并进行安装和配置，然后创建二个测试帐号，分别在本机和网络中其它计算机上使用测试帐号发送邮件，测试 Sendmail 服务器系统工作是否正常。

3. 实验环境

(1) 实验设备

- PC 服务器 2 台 (Linux 操作系统);
- 交换机 1 台;
- PC 机若干台;
- SMTP 源代码安装包 sendmail-8.13.0.tar.gz。

(2) 网络拓扑 如图 3-1 所示。



(图 4-4 邮件服务器配置实验连接图)

4. 实验原理

(1) SMTP 是一种邮件传输协议, SMTP 主要有两个目的, 其一是将授权客户提交的电子邮件从客户机传输到 SMTP 服务器; 其二是将本 SMTP 服务器上客户的邮件传输到另一个 SMTP 服务器;

(2) SMTP 服务器在 TCP 协议 25 号端口监听连接请求, 客户端与服务器之间的通信过程如下:

- 客户端请求与 SMTP 服务器建立 TCP 连接;
- 客户端发送 HELO 命令以标识发件人自己的身份;
- 服务器端回应欢迎信息;
- 客户端发送 MAIL FROM 命令标识邮件发送者的邮件地址;
- 服务器端以 OK 作为响应;
- 客户端发送 RCPT TO 命令标识电子邮件的接收人, 可以有多个 RCPT TO;
- 服务器端以 OK 作为响应;
- 客户端用命令 DATA 邮件正文开始;
- 客户端用以 “.” 表示邮件正文结束, 并将邮件发送出去;
- 客户端用 QUIT 命令结束此次通信并退出。

表 3.1 是 SMTP 客户端与 SMTP 服务器端通信的协议:

表 4.1: SMTP 通信协议

命令	简要描述
HELO	用于标示邮件中“Received:”信息的头部
MAIL FROM:	用于标示邮件发送者的邮件地址
RCPT TO:	用于标示邮件接收者的邮件地址
DATA	用于表示邮件正文的开始
.	必须单独一行出现, 表示邮件正文结束
HELP	命令帮助
QUIT	结束本次发送过程

5. 实验步骤

5.1 实验准备

(1) 下载源代码

Sendmail 最新版本的源代码可以从 <http://www.sendmail.org> 或其镜像站点下载, 本书附带的光盘上包括了 sendmail 8.13.0 版本的原代码。

(2) 源代码解包

将下载的安装包 sendmail-8.13.0.tar.gz 复制到某一个用户目录下 (下面以 /usr/src/ 目录为例介绍), 然后用以下命令解压:

```
$ cd /usr/src
$ tar xvfz sendmail-8.13.0.tar.gz
```

将会在 /usr/src/ 目录下创建 /sendmail-8.13.0 子目录，该目录下包含 sendmail 的所有的源代码和相关文档。

5.2 安装设置

首先用超级用户在 /etc 下创建 mail 目录(如果原来安装过 sendmail, 则可先把原来的 mail 目录备份: # mv mail mail.bak) :

```
# cd /etc
# mkdir mail
```

进入安装包所在目录:

```
# cd /usr/src/sendmail-8.13.0
# cd cf/cf
```

编辑 generic-linux.mc.mc 文件，在该文件中间位置增加以下四行，将避免在发送邮件时对发送地址和接收地址进行 DNS 解析:

```
FEATURE(accept_unresolvable_domains)
FEATURE(relay_entire_domain)
FEATURE(nocanonify)
define('confDONT_PROBE_INTERFACES')
```

选择与安装机器上操作系统（这里选 LINUX）相同的配置文件:

```
# cp generic-linux.mc sendmail.mc
```

生成配置文件 sendmail.cf, submit.cf ,并复制到安装目录/etc/mail:

```
# make install-cf
```

5.3 编译

```
# cd /usr/src/sendmail-8.13.0
# make
```

5.4 安装

通过执行安装程序，可以把编译后的执行文件 sendmail 安装到 /usr/sbin/, 把配置文件 sendmail.cf, submit.cf, statistics, helpfile 安装到目录 /etc/mail 中:

```
# cd /usr
# mkdir man          //创建联机帮助目录
# cd man
# mkdir man8
# mkdir man5
# mkdir man1
```

```
# cd /usr/src/sendmail-8.13.0
# make install      //执行安装程序
```

安装完成后, 可以清除编译生成的中间文件 (.o), 以释放磁盘空间:

```
$ make clean      //清除中间文件
```

5.5 配置

Sendmail 的配置文件放在/etc/mail/sendmail.cf 中, 配置文件比较复杂, 不过一般只需要修改几个地方就可以了, 其他选项都使用默认设置。

编辑 sendmail.cf 文件, 查找 Cw 选项, 在原来的 Cw localhost 之后加上 Sendmail 服务器主机名如 test.com:

```
Cwlocalhost    test.com
```

上述工作也可通过编辑/etc/mail/ 目录中文件名为 local-host-names 的文件来完成:

```
# vi local-host-names
localhost
test.com
```

另外还需要修改 AliasFile 选项, 让其指向/etc/ aliases 的别名库:

```
AliasFile=/etc/aliases
```

如果希望限制每个收发的邮件大小, 如允许收发 1MB 的邮件, 可以修改选项:
0 MaxMessageSize=1000000

5.6 用户管理

在 Linux 中添加一个操作系统用户就会有一个电子邮件帐户, 不需要特别设置, 可以通过该用户和密码用 Sendmail 发送邮件。

```
# /usr/sbin/useradd abc      //增加一个操作系统用户
# /usr/bin/passwd abc       //为用户 abc 设置密码
# /usr/sbin/useradd xyz
# /usr/bin/passwd xyz
```

5.7 运行与停止

```
# ps -A|grep sendmail      //查看原来是否已运行 sendmail
# kill -9 nnnn             //如果原来已运行且进程号为 nnnn, 则停止该进程
```

```
# cd /usr/sbin
# ./sendmail -bd -q30m     //启动 sendmail
```

其中, -bd 表示以 daemon 方式运行, q30m 表示每隔 30 分钟处理邮件队列,

可通过帮助系统查看 sendmail 的所有选项:

```
#man sendmail
```

Sendmail 运行时的日志文件放在 /var/log/maillog 中, 启动后可通过以下命令来跟踪查看, 以发现问题:

```
# tail -f /var/log/maillog &
```

如果日志不详细, 可修改 sendmail.cf 中的 LogLevel 选项, 值越大越详细:

```
0 LogLevel=9
```

Sendmail 将收到的邮件保存在目录/var/spool/mail/中, 每个用户一个文件, 例如, /var/spool/mail/abc 中保存用户 abc 的邮件 (如有的话)。

通过以下命令可以把 sendmail 进程 (假设进程号为 nnnn) 的停下来:

```
# ps -A|grep sendmail
# kill -9 nnnn
```

6. 实验评测

Sendmail 正常运行后, 可以通过运行以下命令进行测试 (假设邮件服务器的 IP 地址为 192.168.25.188), 其中 ‘→’ 表示人输入的命令, ‘←’ 表示 sendmail 返回的信息:

```
# telnet 192.168.1X.4 25          //25 为 SMTP 服务端口
←Trying 192.168.1X.4...
←Connected to www.test.com (192.168.1X.4).
←Escape character is '^]'.
←220 localhost.localdomain ESMTP Sendmail 8.13.0/8.13.0; Mon, 30
Aug 2004 16:22:19 +0800
```

```
→help
```

```
←214-2.0.0 This is sendmail version 8.13.0
```

```
←214-2.0.0 Topics:
```

```
←214-2.0.0          HELO          EHLO          MAIL          RCPT
DATA
```

```
←214-2.0.0          RSET          NOOP          QUIT          HELP
VERFY
```

```
←214-2.0.0          EXPN          VERB          ETRN          DSN
AUTH
```

```
←214-2.0.0          STARTTLS
```

```
→helo mail.test.com
→mail from:abc@test.com
→rcpt to:xyz@test.com
→data
→1234567890abcdefg
→.
←Message accepted for delivery
→quit
```

通过上述命令, 将以 abc@test.com 的身份向 xyz@test.com (在该服务器上必须存在 xyz 这个用户) 发一份内容为 1234567890abcdefg 的邮件。

如果上述操作能正确完成, 则表明 sendmail 服务器能正常工作, 可以通过 outlook 等客户端程序发送邮件了。

实验 4.4 POP3 服务器的安装与配置

目前使用很广的 POP3 邮件接收系统有如 Qpopper, IPOP 等, 下面简单介绍 QPopper 的安装与配置。

1. 实验目的

通过对 Qpopper 服务器系统的安装与配置实验, 加深对 POP3 协议的理解, 掌握 POP3 邮件服务器系统的安装与配置方法, 为将来从事网络工程建设打下基础。

2. 实验要求

下载 Qpopper 服务器源代码, 在 Linux 环境下, 编译生成执行代码, 并进行安装和配置, 使用测试帐号 abc 和 xyz, 分别在本机和网络中其它计算机上先使用 Sendmail 发送邮件, 然后再通过 Qpopper 接收邮件, 测试 Qpopper 服务器系统工作是否正常。

3. 实验环境

(1) 实验设备

- PC 服务器 2 台 (Linux 操作系统);
- 交换机 1 台;
- PC 机若干台;
- POP3 服务器源代码安装包 Qpopper4.0.5.tar.gz。

(2) 网络拓扑

如图 4-4 所示。

4. 实验原理

(1) POP3 是脱机模型的电子邮件协议, POP3 客户端程序与 POP3 服务器建立 TCP 连接 (端口号为 110) 并查询是否有新的电子邮件, 若有则将该客户所有新邮件逐个下载到客户机, 以便客户阅读;

(2) POP3 客户端与 POP3 服务器之间通信的协议如下表所示:

表 4.2: POP3 通信协议

命令	简要描述
USER username	输入用户帐号（注：并非邮件地址）
PASS password	输入该帐号对应的密码
STAT	返回邮箱的统计资料，如邮件总数和总字节数
LIST MsgNo	返回邮件数量和每个邮件的大小
RETR MsgNo	从服务器上收取编号为 MsgNo 的邮件
DELE MsgNo	删除服务器上编号为 MsgNo 的邮件
TOP MsgNo	服务器将返回由参数标识的邮件前 n 行内容
RSET	服务器将重置所有标记为删除的邮件，用于撤消 DELE 命令
UIDL MsgNo	返回邮件的唯一标识符
NOOP	服务器返回一个工作正常的响应
QUIT	结束本次接收通信过程

5. 实验步骤

5.1 实验准备

(1) 下载源代码

Qpopper 最新版本的源代码可以从 <http://www.eudora.com/qpopper> 站点下载，本书附带的光盘上包括了 qpopper4.0.5 版本的原代码。

(2) 源代码解包

将下载的安装包 qpopper4.0.5.tar.gz 复制到某一个用户目录下（下面以 /usr/src/ 目录为例介绍），然后用以下命令解压：

```
$ cd /usr/src
```

```
$ tar xvfz qpopper4.0.5.tar.gz
```

将会在 /usr/src/ 目录下创建 /qpopper4.0.5 子目录，该目录下包含 Qpopper 的所有源代码和相关文档。

5.2 安装设置

进入安装包所在目录：

```
$ cd /usr/src/qpopper4.0.5
```

```
$ ./configure --help //可查看配置选项
```

指定安装目录为 /usr/local/qpopper

```
$ ./configure --prefix=/usr/local/qpopper --enable-standalone
```


5.3 编译

```
$ cd /usr/src/qpopper4.0.5
$ make
```

5.4 安装

首先,手工创建有关目录:

```
$ cd /usr/local
$ mkdir qpopper
$ mkdir qpopper/sbin
$ mkdir qpopper/man
$ mkdir qpopper/man/man8
```

执行安装命令,把 compile 出来的执行文件 popper 复制到 /usr/local/qpopper/sbin/中:

```
$ cd /usr/src/qpopper4.0.5
$ make install
```

安装完成后,可以清除编译生成的中间文件(.o),以释放磁盘空间:

```
$ make clean
```

5.5 配置

Qpopper 不需要做特殊的设置,使用默认的设置即可。

5.6 用户管理

在 Unix 中添加一个操作系统用户就会有一个电子邮件帐户,不需要特别设置,可以通过该用户和密码用 popper 收邮件。

5.7 运行与停止

运行 Qpopper:

```
$ cd /usr/local/qpopper/sbin
$ ./popper
```

popper 运行起来后,将会形成日志文件,缺省时在 /var/log/messages 中,启动后可通过命令来查看,以发现问题:

```
$ tail -f /var/log/messages &
```

如果日志不详细,还可以通过在 ./configure 中参数--enable-low-debug 提供详细的运行日志。

停止 Qpopper:

```
$ ps -A|grep popper      //假设进程号为 nnnn
$ kill -9 nnnn
```

6. 实验评测

Qpopper 运行起来后, 可以通过以下命令进行测试(假设邮件服务器的 IP 地址为 192.168.1X.4), 其中 ‘→’ 表示人输入的命令, ‘←’ 表示 Qpopper 返回的信息:

```
$ telnet 192.168.1X.4 110      //110 为 POP3 服务端口
←Trying 192.168.1X.4...
←Connected to www.test.com (192.168.1X.4).
←Escape character is '^]'.
←+OK Qpopper (version 4.0.5) at test starting.
```

//输入用户名

```
→user xyz
←+OK Password required for xyz.
```

//输入用户口令

```
→pass test123
←+OK xyz has 2 visible messages (0 hidden) in 1069 octets.
```

//查看邮件数量, 显示有两份邮件及每个邮件的大小:

```
→list
←+OK 2 visible messages (1069 octets)
←1 530
←2 539
←.
```

//收取第 1 份邮件

```
→retr 1
←+OK 530 octets
←Return-Path: <xyz@test.com>
←Received: from nsl.test.com (www.test.com [192.168.1X.4])
←by localhost.localdomain (8.13.0/8.13.0) with ESMTP id i79Q0013316
←for <xyz@test.com>; Mon, 30 Aug 2004 17:26:24 +0800
←Subject:
←From: abc abc@test.com
←To: xyz@test.com
.....
←1234567890abcdefg
←.
```

```
//收取第 2 份邮件
→retr 2
.....
//删除第 1 份邮件
→dele 1
←+OK Message 1 has been deleted.

//删除第 2 份邮件
→dele 2
←+OK Message 2 has been deleted.
```

```
//退出
→quit
```

通过上述命令将以 xyz@test.com 的身份登录邮件服务器，收取或删除邮件。

如果上述操作能正确完成，则表明 POP3 服务器能正常工作，可以通过 outlook 等 POP3 客户端程序接收邮件。

思考问题

- (1) 在 SendMail 邮件系统中，用户的邮件通过什么形式保存在什么地方？
- (2) 如果某用户收到了一个特别大的垃圾邮件，导致用户邮箱空间满，作为邮件服务器管理员应如何处理？

第五章 防火墙配置

实验 5.1 安全规则配置实验

1. 实验目的

通过对防火墙系统的安装与安全规则配置实验，加深对防火墙系统工作原理理解，掌握其常见产品的安装与配置方法，为将来从事网络工程建设打下基础。

2. 实验要求

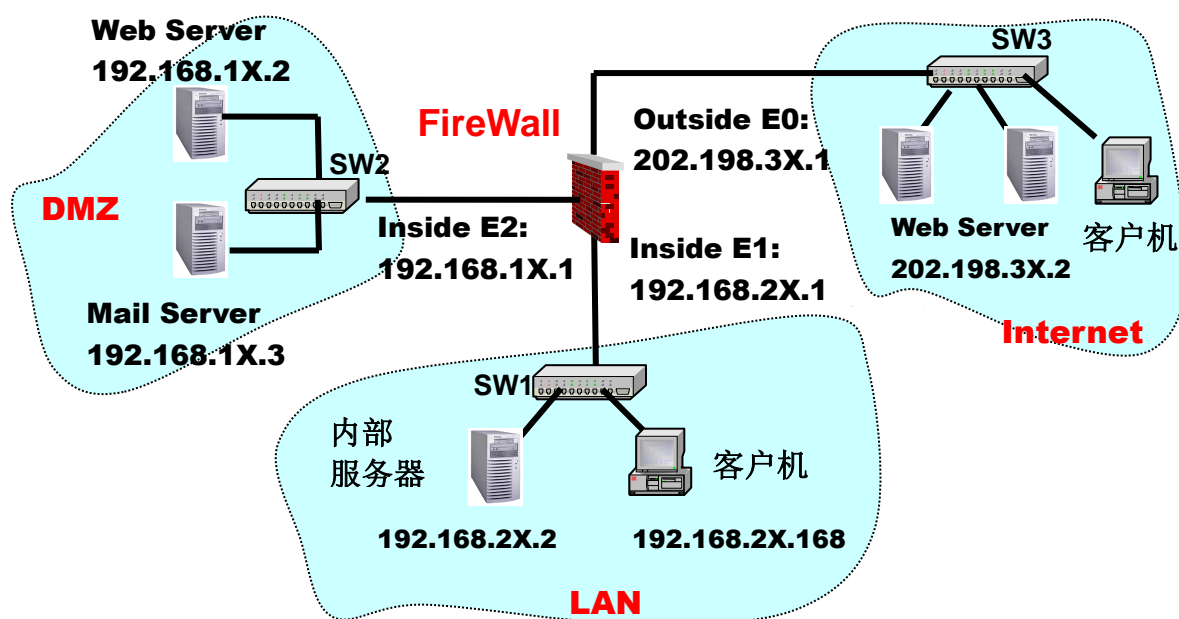
通过本实验，熟悉防火墙的有关概念和基本功能，掌握防火墙包过滤、静态地址转换、动态地址影射、端口影射等安全规则用途和配置方法。

3. 实验环境

(1) 实验设备

- 用于配置和测试的计算机七台；
- 三端口防火墙系统一台；
- 直连网线若干根；
- RS-232C 串行通信线一根。

(2) 网络拓扑



(图 5-1 防火墙配置实验网络拓扑图)

4. 实验原理

(1) 包过滤访问控制

包过滤访问控制是防火墙的主要功能部分，防火墙有 permit 和 deny 两种访问控制权限，可控制的网络协议一般有 ip、tcp、udp、icmp 等。

(2) 静态地址转换

如果需要从外网访问内网的一个固定 IP 地址，可以使用静态地址转换，把该内部地址固定转换成一个指定的外部地址。

(3) 动态地址转换

动态网络地址转换（NAT）作用是将内网的私有 IP 地址转换为外网的一组公有 IP 地址，这样，内部网络的用户就可以访问外部网络了。

(4) 端口影射

与静态地址转换的功能类似，允许外部用户通过一个特殊的 IP 地址/端口透过防火墙访问内部指定的内部服务器。该功能可方便发布内部的 www、ftp、mail 等服务器，同时又保持内部服务器的安全性。

5. 实验步骤

(1) 根据图 5-1 防火墙配置实验网络拓扑图，在防火墙上按照实验要求对接口进行相应配置；

(2) 包过滤规则配置

在防火墙上，通过 GUI 界面，按下面安全策略的要求对包过滤规则进行配置：

- 允许 LAN 上任何设备访问通过 80 端口访问 DMZ 中的 Web Server;
- 允许 LAN 上任何设备访问通过 25 和 110 端口访问 DMZ 中的 Mail Server;
- 允许 LAN 上任何设备访问通过 ICMP 协议访问 DMZ 中的任何设备;
- 允许 LAN 上任何设备访问 Internet;
- 允许 Internet 上的任何设备通过 80 端口访问 DMZ 中的 Web Server;
- 允许 Internet 上的任何设备通过 25 和 110 端口访问 DMZ 中的 Mail Server;
- 拒绝 Internet 上的任何设备通过任何端口访问 LAN;
- 拒绝 Internet 上的任何设备通过其它任何端口访问 DMZ;
- 拒绝 DMZ 上的任何设备通过任何其它端口访问 LAN 和 Internet。

(3) 静态地址转换 (NAT) 配置

在防火墙上，通过 GUI 界面，按下面静态地址转换要求进行配置：

- 允许 Internet 上的任何设备通过 IP 为 202.198.3X.100，端口为 80 访问 DMZ 中的 Web Server;
- 允许 Internet 上的任何设备通过 IP 为 202.198.3X.101，端口为 25 和 110 端口访问 DMZ 中的 Mail Server。

(4) 动态地址转换配置

在防火墙上，通过 GUI 界面，按下面动态地址影射要求进行配置：

- 允许 LAN (192.168.2X.0/24) 上任何设备通过公共的地址池 202.198.3X.200——202.198.3X.254 动态地访问 Internet 上的 Web Server。

(5) 端口转换 (PAT) 配置

在防火墙上，通过 GUI 界面，按下面端口影射要求进行配置：

- 允许 Internet 上任何设备同时通过唯一的地址 202.198.3X.168 访问 DMZ 上 Web Server。

6. 实验评测

(1) 按照上述规则要求，用 ping、telnet 和浏览器测试防火墙包过滤规则工作是否按要求正常工作；

(2) 从 Internet 上的客户机上，测试是否能访问 DMZ 中的 Web Server 和 Mail Server；

(3) 从 LAN 上的客户机上，测试是否能通过地址池 202.198.3X.200——202.198.3X.254 访问 Internet 上的 Web Server；

(4) 从 Internet 上的客户机上，测试是否能通过唯一的地址 202.198.3X.168 访

问 LAN 上 Web Server。

思考问题

- (1) 在某防火墙安全规则配置时, 已经允许从 主机 A 到主机 B 通过 ICMP 协议, 但使用 ping 测试时发现从 A 到 B 还是不通, 请问是什么原因?
- (2) 什么是 DMZ, 设置 DMZ 有何意义?

第六章 网络工程综合实验

一个完整的组网工程包括需求分析、方案设计、设备选型与采购、硬件安装与配置、软件安装与配置、系统测试与联调、工程验收等若干个环节，其中硬件与应用系统安装、配置工作量大，技术含量高，是信息系统集成或网络工程的关键环节，其中既涉及到技术上的问题，也涉及到工程组织、协调配合上的问题，一个网络工程师只有通过多次工程的实际锻炼，不断积累经验、吸取教训才能提高自己的水平。

1. 实验目的

通过对常用的组网设备（包括交换机、路由器、防火墙）、常见的网络服务系统（Web 服务、SmtP & Pop3 服务等）的安装与配置与调试实验，加深对上述设备和系统工作原理的理解，初步掌握其安装配置方法，为将来从事网络工程建设打下基础。

2. 实验要求

设计并构建一个小型的校园网络平台，并在该平台上构建 INTERNET 服务平台，该网络工程建成后，将具有以下服务功能（如图 6-1 所示）：

- （1）具有内部 Web 服务功能；
- （2）具有外部 Web 服务代理功能；
- （3）具有邮件收发功能；
- （4）具有对内部核心子网安全保护功能；
- （5）具有简单的网络管理功能。

3. 实验环境

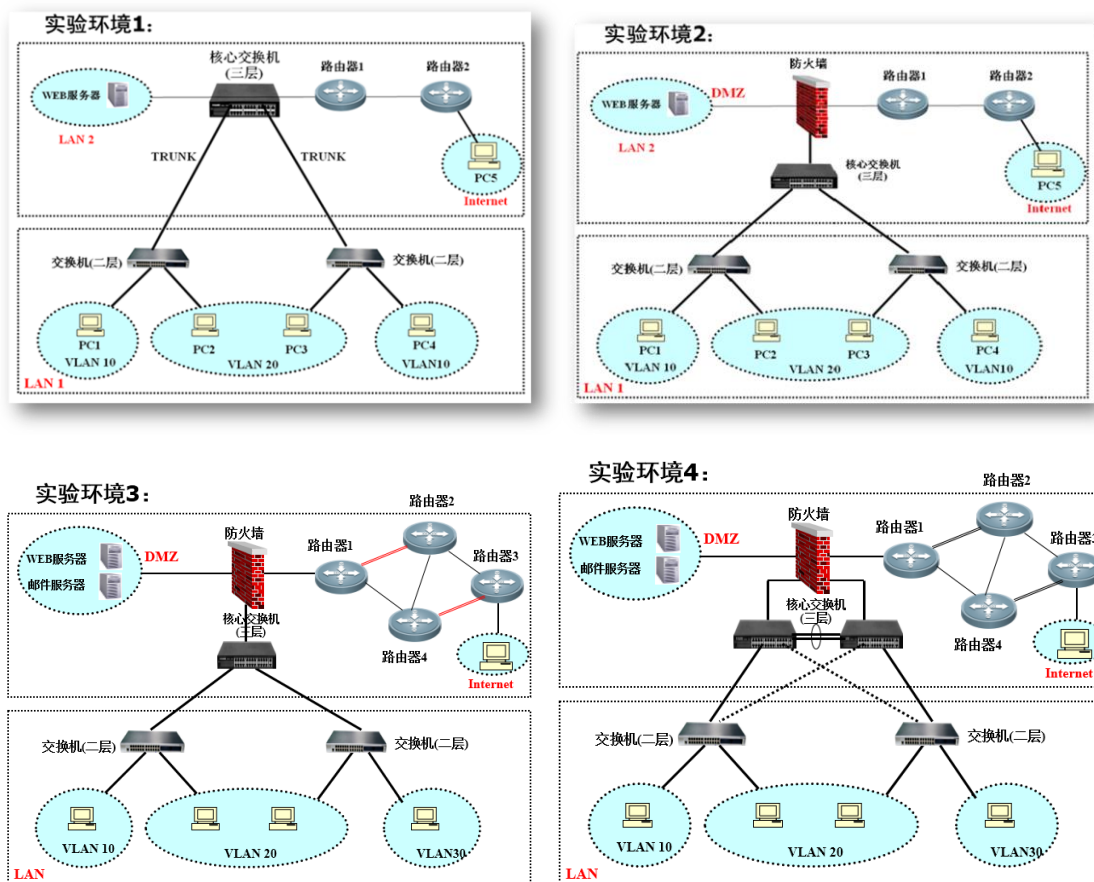
（1）软件清单

OS : Red Hat Linux
WWW : Apache 2.0
SMTP : Sendmail 8.13
POP3 : Qpopper 4.05

（2）硬件设备

三层交换机 : 二台
二层交换机 : 二台
路由器 : 二台
三端口防火墙 : 一台
PC 机 : 八台
RS-232C 串口电缆 : 若干根
直联网线 : 若干根

(3) 网络拓扑
如图 6-1 所示。



(图 6-1 综合实验网络拓扑图)

4. 实验步骤

4.1 WEB 服务

- 建立一个内部 WEB 服务网站: www.test.com , 设计测试网页;
- 在外部网站上提供 3 个虚拟主机服务: www.test1.com, www.test2.com, www.test3.com , 并设计相应的测试网页。

4.2 邮件服务

(1) SMTP 服务器安装与配置

- 安装 SMTP 服务器: 在 Linux 环境下, 使用 sendmail 8.13 源代码, 进行编译、安装和基本配置, 构建 2 个 SMTP 服务器 smtp.nudt.com , smtp.test.com;
- 建立邮件测试帐号: abc@nudt.com, xyz@nudt.com, test@test.com ;

- 向所在邮件服务器上的帐号发送邮件：使用帐号 abc@nudt.com，在 PC 机上通过命令行 telnet smtp.nudt.com 25 和 outlook 向 smtp.nudt.com 服务器上的用户 xyz@nudt.com 发送测试邮件；
 - 向其它邮件服务器上的帐号发送邮件：使用帐号 abc@nudt.com，在 PC 机上通过命令行 telnet smtp.nudt.com 25 和 outlook 向 smtp.test.com 服务器的用户 test@test.com 发送测试邮件；
- (2) SMTP 服务器安装与配置
- 安装 POP3 邮件服务器：在 Linux 环境下，对 Qpopper 4.05 源代码进行编译、安装和基本配置，构建 2 个 POP3 服务器 pop3.nudt.com, pop3.test.com；
 - 使用 POP3 接收邮件：分别使用上述三个邮件帐号：abc@nudt.com, xyz@nudt.com, test@test.com，通过 telnet pop3.nudt.com 110 和 outlook 从两个 POP3 服务器上接收前面发送的测试邮件。

4.3 交换机和路由器

按照网络拓扑图 6-1 的要求，对交换机和路由器进行配置，具体内容包括：

- VLAN 划分与配置
- 链路聚合协议配置
- RSTP 生成树协议配置
- VRRP 协议配置
- 动态路由协议配置

4.4 防火墙

(1) 包过滤规则配置

在防火墙上，通过 GUI 界面，按下面安全策略的要求对包过滤规则进行配置：

- 允许 LAN 上任何设备访问通过 80 端口访问 DMZ 中的 Web Server；
- 允许 LAN 上任何设备访问通过 25 和 110 端口访问 DMZ 中的 Mail；
- 允许 LAN 上任何设备访问通过 ICMP 协议访问 DMZ 中的任何设备；
- 允许 LAN 上任何设备访问 Internet；
- 允许 Internet 上的任何设备通过 80 端口访问 DMZ 中的 Web Server；
- 允许 Internet 上的任何设备通过 25 和 110 端口访问 DMZ 中的 Mail；
- 拒绝 Internet 上的任何设备通过任何端口访问 LAN；
- 拒绝 Internet 上的任何设备通过其它任何端口访问 DMZ；
- 拒绝 DMZ 上的任何设备通过任何其它端口访问 LAN 和 Internet。

(2) 动态地址转换配置 (NAT)

在防火墙上，通过 GUI 界面，按下面动态地址影射要求进行配置：

- 允许 LAN 上任何设备通过公共的地址池 202.198.3X.200—202.198.3X.254 动态地访问 Internet 上的任何设备。

(3) 端口转换配置 (PAT)

在防火墙上，通过 GUI 界面，按下面端口影射要求进行配置：

- 允许 Internet 上的任何设备通过 IP 为 202.198.3X.100，端口为 80 访问 DMZ 中

的 Web Server;

- 允许 Internet 上的任何设备通过 IP 为 202.198.3X.101, 端口为 25 和 110 端口访问 DMZ 中的 Mail Server。

在防火墙上, 通过 GUI 界面, 按下面端口影射要求配置:

- 允许 Internet 上任何设备同时通过唯一的地址 202.198.3X.168 和端口 1000 访问 DMZ 上 Web Server。

5. 实验评测

根据实验要求, 针对每一个实验内容, 参照前面各章节中的评测方法进行验证。

附：参考资料

1、参考资料（网站）：

Apache Web site: www.apache.org

Send mail Web site: www.sendmail.org

Qpopper Web site: www.eudora.com/qpopper

教学与实验安排

序号	章节主题	讲授 课时	实践 课时	实验安排
1	基础知识回顾	2	4	实验1-1、制作网线 实验1-2、熟悉思科模拟器 实验1-3、构建简单局域网
2	交换机	1	7	实验2-1、交换机的VLAN间路由 实验2-2、交换机的端口聚合配置 实验2-3、交换机的快速生成树协议配置 实验2-4、交换机的HSRP配置
3	路由器	1	7	实验3-1、路由器的基本配置（直连网络） 实验3-2、静态路由配置 实验3-3、RIP路由协议配置 实验3-4、OSPF路由协议配置 实验3-5、实战训练
4	服务器	0	4	实验4-1、Apache的安装与基本配置 实验4-2、虚拟主机的配置 实验4-3、SMTP服务器的安装与配置 实验4-4、POP3服务器的安装与配置
5	防火墙	0	4	实验5-1、防火墙基本配置
6	综合设计	2	8	实验6-1、综合实验
	共计	6	34	