Network Integrated

Project Practice

网络综合项目实践

郑娟　主编

暨南大學出版社
JINAN UNIVERSITY PRESS

网络综合项目实践

郑娟　主编

暨南大學出版社
JINAN UNIVERSITY PRESS

中国·广州

图书在版编目（CIP）数据

网络综合项目实践/郑娟主编. —广州：暨南大学出版社，2015.7
ISBN 978-7-5668-1422-7

Ⅰ.①网… Ⅱ.①郑… Ⅲ.①计算机网络 Ⅳ.①TP393

中国版本图书馆 CIP 数据核字(2015)第 098005 号

出版发行：暨南大学出版社

地　址：中国广州暨南大学
电　话：总编室（8620）85221601
　　营销部（8620）85225284　85228291　85228292（邮购）
传　真：（8620）85221583（办公室）　85223774（营销部）
邮　编：510630
网　址：http://www.jnupress.com　http://press.jnu.edu.cn

排　版：广州市天河星辰文化发展部照排中心
印　刷：广东广州日报传媒股份有限公司印务分公司

开　本：787mm×1092mm　1/16
印　张：13.5
字　数：347 千
版　次：2015 年 7 月第 1 版
印　次：2015 年 7 月第 1 次

定　价：32.00 元

前　言

新形势下的中职教育以培养高素质的劳动者为目标，以就业为导向，以能力为本位，把实践教学和技能训练作为重要环节。中职教育必须以此为突破口，全面进行教学内容和教学方法的改革与创新，形成独具特色的课程模式、教学方式和评价体系，使教学更具针对性和实效性，才能培养出社会生产一线需要的高素质技能型人才。

基于以上认识，我们采用了新的职教思想——校企合作的课程开发模式，打破传统的基于知识结构的课程架构。对相关企业典型岗位工作进行调研，以课程定位为核心，以职业工作任务为内容，根据学习主体的心理和智力特点，开展对职业学校学生知识传授和能力培养的工作。

在编写本教材时，我们以若干真实的网络工程案例为背景，按照项目工程实施过程的顺序进行分解，针对学生未来就业岗位上可能遇到的各类网络组建、维护和管理等问题，培养他们的实际操作能力。在项目实施中，我们将网络设备配置及网络操作系统的管理结合在一起，真实地呈现了完整的计算机网络项目。以加强组网工作技能为根本，满足学生组网实践技能的培养需求。

全书以项目形式呈现，将“用户需求—需求分析—方案设计—知识准备—项目实现”几个环节贯穿于每一个项目中，并围绕中小型网络管理工作岗位上的专业人员需要了解的知识，搭建了七大工作场景：SOHO 网络项目、小区网络工程项目、园区网络项目、企业网络项目、中型企业网络项目、电子商务企业网络项目、小型信息安全网络项目。

本书呈现了工程项目的具体实施过程，这一点不同于其他教材。编写本书时，我们假设学生已经掌握了网络的基本概念及设备的基本配置知识，并掌握了网络操作系统的配置与管理，所以建议此书在学生学完上述内容后使用。

由于编写时间仓促，编者水平有限，书中不足之处在所难免，恳请广大读者批评指正。

郑娟

2015 年 6 月 2 日

目　录

项目 1　SOHO 网络项目

1.1　【用户需求】

致远食品公司原是一家入住 SOHO 大厦的新公司，公司职员十几人，业务部门分财务部和市场部。由于资金等因素的限制，且出于管理简单、方便的考虑，致远食品公司构建了工作组模式网络。公司虽接入了因特网，但不对外提供服务。该网络组建的主要目的是实现资源的共享和计算机之间的通信。其硬件设备主要包括文件服务器、客户机、磁盘阵列、打印机、扫描仪、交换机、路由器等。用户可自己决定其计算机上的哪些数据将共享在网络上，并且可决定不同用户对文件的不同访问权限。

致远公司原有 IT 架构规模较小，建立在 Windows 和 Linux 平台上，主要使用 Windows 2000 Professional、Windows XP Professional、Windows Server 2003 和 Linux 操作系统。随着企业规模的扩大，公司的业务增多，公司的经营越来越依赖于企业内部网的办公自动化和企业外部网的资源。公司已经认识到优秀的网络架构能大大提高企业的办公效率并增强企业信息的安全性。

1. 网络搭建部分的需求

（1）按照层次型网络结构进行网络设计和任务实施。

（2）公司根据部门业务进行网段划分。

（3）内部用户利用私网地址访问 Internet 时，需用网络出口设备进行地址转换。

（4）主公司内部采用动态路由协议来简化路由配置时，要求配置简单且适用于小型网络。

（5）主公司只对内网用户提供服务。

（6）适当使用网络访问控制措施，以确保内部网络的安全性。

2. 内部应用系统构建部分的需求

（1）需要添加一台存放公司重要数据的专门服务器，能对不同职能部门的用户提供不同的访问权限。

（2）建立一台 Web 服务器，来展示企业形象，增加公司业务。

（3）由于公司申请了域名，用户需要通过域名来访问公司的主机和服务器。

1.2　【需求分析】

为实现公司目标，首先需要制订网络建设方案，其网络拓扑结构如图 1－1 所示。

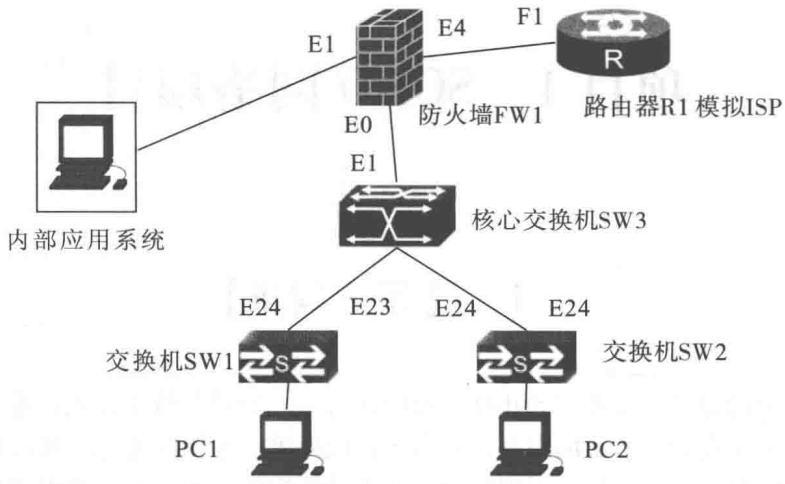

图 1-1 拓扑图

1. 网络搭建部分需求分析

（1）由于公司的网络规模较小，主公司采用二层的网络架构，将核心层和汇聚层合为一层，即保障了业务数据流的畅通，又能实现层次性的网络架构。

（2）公司内部有市场部和财务部，使用 VLAN 技术，将两个部门的交换机划分到不同的 VLAN 中，既可以实现统一管理，又可以保障网络的安全性。

（3）在交换机 SW1 和 SW2 上创建 VLAN 三层接口并配置 IP 地址。

（4）由于主公司的规模较小，网络设备数量少，为了简化管理，采用 RIP 协议。

（5）服务商为公司提供 IP 地址 14.1.196.1，并使用网络地址转换技术，将私有 IP 地址转化为公网地址，使内网用户能访问互联网。

（6）使用访问列表控制技术，使一些常见的危险端口不能访问。

2. 内部应用系统构建部分需求分析

（1）添加一台存放公司重要数据的文件服务器，并通过配置使员工能通过网络访问文件服务器。

（2）所有员工都能读取共享文件夹“市场部”，市场部员工拥有完全控制权限；允许财务部的员工访问共享文件夹“财务部”，并拥有完全控制权限。此服务器放置在离客户端较近的位置，以提高访问速度。为了避免感染 Windows 病毒，服务器选用 Linux 操作系统。

（3）申请域名空间 zhiyuan.com，并添加一台独立支持 ASP 语言的 Web 服务器，其域名为 www.zhiyuan.com，并能限制客户端连接数量，保证 Web 服务器的服务质量。该服务器放置在内部网络，为保证 Web 服务器的安全，只为内网和外网的用户提供服务。

（4）添加一台 DNS 服务器，使员工能通过域名访问公司的内网数据。

1.3　【方案设计】

项目需求分析完成后，确定供货合同，网络公司就开始具体的实施流程了。需求分析分为网络搭建、内部应用系统构建两大部分，分别施工。本项目具体介绍了每个部分的施工流程。

1. 网络搭建部分实施方案

首先根据需求分析，选择网络中的应用设备，再根据拓扑图把设备部署到相应的位置，并按拓扑图进行设备连接。主要任务包括：

（1）内部接入层设置：按公司部门名称规划并配置交换网络中的VLAN；启用生成树协议来避免网络环路；配置网络中所有设备相应的IP地址，同时测试线路两端的连通性。

（2）路由层设置：在内网部分启动RIP协议。

（3）接入互联网设置：配置NAT，保证内网用户能访问Internet。

（4）网络安全防护设置：使用访问列表控制技术，使一些常见的危险端口不能访问。

2. 内部应用系统构建部分实施方案

首先根据需求分析来购置服务器，服务器到位后，安装服务器操作系统。根据网络拓扑图将各部件部署到相应的位置后，按下面的顺序进行配置：

（1）文件服务器系统配置。

（2）Web服务器系统配置。

（3）DNS服务器系统配置。

1.4　【知识准备】

1. VLAN简介

虚拟局域网VLAN（Virtual Local Area Network）是交换机端口的逻辑组合。VLAN工作在开放式系统互联（OSI）的第二层。VLAN之间的通信是通过第三层的路由器来完成的。VLAN有以下优点：

（1）控制网络的广播问题：每一个VLAN都是一个广播域；一个VLAN上的广播不会扩散到另一个VLAN。

（2）简化网络管理：当VLAN中的用户位置移动时，网络管理员只需设置几条命令即可。

（3）提高网络的安全性：VLAN能控制广播；VLAN之间不能直接通信。

定义交换机的端口在什么类型的VLAN上的常用方法有：

（1）基于端口的VLAN：管理员把交换机某一端口指定为某一VLAN的成员。

（2）基于MAC地址的VLAN：交换机根据节点的MAC地址，决定将其放置于哪个VLAN中。

2. RIP 简介

动态路由协议包括距离向量路由协议和链路状态路由协议。RIP（Routing Information Protocol）协议即路由信息协议，是使用最广泛的距离向量路由协议。RIP 协议是为小型网络环境设计的，因为这类协议的路由学习及路由更新将产生较大的流量，占用过多的带宽。

RIP 协议是由 Xerox 公司在 20 世纪 70 年代开发的，最初定义在 RFC1058 中。RIP 协议用两种数据包传输更新和请求，每个有 RIP 协议功能的路由器在默认情况下每隔 30 秒利用 UDP520 端口向与它直连的网络邻居广播（RIPv1）或组播（RIPv2）进行路由更新，因此路由器不知道网络的全局情况。如果路由更新在网络上传播慢，将会导致网络收敛较慢，造成路由环路。为了避免路由环路，RIP 协议采用水平分割、毒性逆转、定义最大跳数、闪式更新、抑制计时五个机制来避免路由环路。

RIP 协议分为版本 1 和版本 2。不论是版本 1 还是版本 2，都具备下面的特征：

（1）是距离向量路由协议。

（2）使用跳数（Hop Count）作为度量值。

（3）默认路由更新周期为 30 秒。

（4）管理距离（AD）为 120。

（5）支持触发更新。

（6）最大跳数为 15 跳。

（7）支持等价路径，默认 4 条，最大 6 条。

（8）使用 UDP520 端口进行路由更新。

而 RIPv1 和 RIPv2 的区别如表 1 - 1 所示。

表 1 - 1　RIPv1 和 RIPv2 的区别

RIPv1	RIPv2
在路由更新的过程中不携带子网信息	在路由更新的过程中携带子网信息
不提供认证	提供明文和 MD5 认证
不支持 VLSM 和 CIDR	支持 VLSM 和 CIDR
采用广播更新	采用组播更新
是有类别（Classful）路由协议	是无类别（Classless）路由协议

3. NAT 简介

NAT 是一个 IETF 标准，即允许一个机构以一个地址出现在 Internet 上。NAT 技术使得一个私有网络可以通过 Internet 注册 IP 以连接到外部。位于 Inside 网络和 Outside 网络中的 NAT 路由器在发送数据包之前，负责把内部 IP 地址翻译成外部合法 IP 地址。NAT 将每个局域网节点的 IP 地址转换成一个合法 IP 地址，反之亦然。它也可以应用于防火墙技术，即把个别 IP 地址隐藏起来不被外界发现，对内部网络设备起到保护的作用。同时，它还可以帮助网络超越地址的限制，合理地安排公有 Internet 地址和私有 IP 地址的使用。

NAT 有三种类型：静态 NAT、动态 NAT 和端口地址转换（PAT）。

（1）静态NAT中，内部网络里的每个主机都被永久映射成外部网络里的某个合法的地址。静态地址转换将内部本地地址与内部合法地址进行一对一的转换，且需要指定和哪个合法地址进行转换。如果内部网络有E-mail服务器或FTP服务器等可以为外部用户提供的服务，这些服务器的IP地址必须采用静态地址转换，以便外部用户可以使用这些服务。

（2）对于动态NAT而言，首先要定义合法地址池，然后采用动态分配的方法映射到内部网络。动态NAT是动态一对一的映射。

（3）PAT是把内部地址映射到外部。

4. ACL简介

访问控制列表简称为ACL，它使用包过滤技术，在路由器上读取第三层及第四层包头中的信息，如源地址、目的地址、源端口、目的端口等，并根据预先定义好的规则对包进行过滤，从而达到访问控制的目的。ACL分很多种，不同场合应用不同种类的ACL。

（1）标准ACL是通过使用IP包中的源IP地址进行过滤，表号范围为1～99或1300～1999。

（2）扩展ACL比标准ACL具有更多的匹配项，功能更加强大，可以针对包括协议类型、源地址、目的地址、源端口、目的端口、TCP连接建立等在内的条件进行过滤，表号范围100～199或2000～2699。

在访问控制列表的学习中，要特别注意以下两个术语：

（1）通配符掩码：它是一个32比特位的数字字符串，规定了当一个IP地址与其他的IP地址进行比较时，该IP地址中哪些位应该被忽略。通配符掩码中的“1”表示忽略IP地址中对应的位，而“0”则表示该位必须匹配。两种特殊的通配符掩码是“255.255.255.255”和“0.0.0.0”，前者等价于关键字“any（Any）”，而后者等价于关键字“host（Host）”。

（2）Inbound和Outbound：当在接口上应用访问控制列表时，用户要指明访问控制列表是应用于流入数据还是流出数据。

总之，ACL的应用非常广泛，它可以实现如下功能：

（1）拒绝或允许流入（或流出）的数据流通过特定的接口。

（2）为DDR应用定义感兴趣的数据流。

（3）过滤路由更新的内容。

（4）控制对虚拟终端的访问。

（5）提供流量控制。

1.5　【项目实现】网络搭建部分实现

1.5.1　网络设备的选择

采购人员依据需求分析、公司现阶段的节点数和预算进行综合分析后，采购了一台神州数码DCRS-5650交换机，保证了核心设备具备快速转发数据的能力；采购了两台神州数

码 DCS-3950 二层交换机，保证了接入层交换机为百兆网络接口，并能进行初步的接入控制；采购了一台神州数码 DCR-2626 路由器，保证了模拟服务提供商的网络设备拥有足够的性能，并能实现 RIP 协议的所有功能特性；采购了一台 DCFW-1800 防火墙，作为 Internet 接入设备，并且以后可以通过此防火墙进行安全控制。

1.5.2 规划拓扑结构与 IP 地址

网络工程师根据采购的设备和公司需求，建立了整体网络结构拓扑图（如图 1－1 所示）与 IP 地址规划表（如表 1－2 所示）。

表 1－2 IP 地址规划表

设 备	接 口	IP 地址
FW1	E0/0	192. 168. 1. 1/24
	E0/1	192. 168. 2. 1/24
	E0/4	14. 1. 196. 2/24
R1	F0/0	14. 1. 196. 1/24
SW1	F0/0	192. 168. 1. 2/24
SW2	vlan1	192. 168. 1. 254/24
	vlan10	192. 168. 10. 254/24
	vlan20	192. 168. 20. 254/24
SW3	vlan1	192. 168. 2. 254/24
	vlan10	192. 168. 10. 253/24
	vlan20	192. 168. 20. 253/24

1.5.3 划分 VLAN

步骤 1：在交换机 SW1 和 SW2 上划分各 VLAN，并加入相应的端口。

（1）依照下表，在交换机 SW1 上划分各 VLAN，并加入相应的端口。

表 1－3

VLAN	端口号
vlan10	E0/0/2、E0/0/3
vlan20	E0/0/6、E0/0/8

上表中未提到的端口，放在 vlan1 中。

```
SW1_config#vlan 10                                          //SW1 创建 vlan10
SW1_config_vlan10#switchport interface ethernet 0/0/2-3     // 给 vlan10 加入端口 2-3
SW1_config_vlan10#exit
SW1_config#vlan 20                                          //SW1 创建 vlan20
SW1_config_vlan20#switchport interface ethernet 0/0/6;8
                                                  //给 vlan20 加入端口 6 和端口 8
SW1_config_vlan20#exit                                      //退出配置
                                                  //剩余端口自动加入 vlan1 中
```

（2）依照下表，在交换机 SW2 上划分各 VLAN，并加入相应的端口。

表 1-4

VLAN	端口号
vlan10	E0/0/2、E0/0/3
vlan20	E0/0/6、E0/0/8

上表中未提到的端口，放在 vlan1 中。

```
SW2_config#vlan 10                                          //SW2 创建 vlan10
SW2_config_vlan10#switchport interface ethernet 0/0/2-3     //给 vlan10 加入端口 2-3
SW2_config_vlan10#exit
SW2_config#vlan 20                                          //SW2 创建 vlan20
SW2_config_vlan20#switchport interface ethernet 0/0/6;8
                                                  //给 vlan20 加入端口 6 和端口 8
SW2_config_vlan20#exit                                      //退出配置
                                                  //剩余端口自动加入 vlan1 中
```

步骤 2：在交换机 SW1 上创建 VLAN 三层接口并配置 IP 地址。

（1）依照下表，在交换机 SW1 上创建 VLAN 三层接口并配置 IP 地址。

表 1-5

vlan-interface	IP 地址
vlan-interface1	192. 168. 1. 254/24
vlan-interface10	192. 168. 10. 254/24
vlan-interface20	192. 168. 20. 254/24

配置如下：

```
SW1_config#interface vlan 1                                    //SW1 创建 vlan1 三层接口
SW1_config_if_vlan1#IP address 192. 168. 1. 254   255. 255. 255. 0
                                    //给 vlan1 配置 IP 地址,即交换机的管理地址
SW1_config_if_vlan1#no shutdown                                //开启 VLAN 三层接口
SW1_config#interface vlan 10                                   //SW1 创建 vlan10 三层接口
SW1_config_if_vlan10#IP address 192. 168. 10. 254   255. 255. 255. 0
                                                               //给 vlan10 配置 IP 地址
SW1_config_if_vlan10#no shutdown
SW1_config#interface vlan 20
SW1_config_if_vlan20#IP address 192. 168. 20. 254   255. 255. 255. 0
SW1_config_if_vlan20#no shutdown
```

（2）验证。

VLAN 三层接口之间相互 PING，能够 PING 通，即完成该步骤。

步骤 3：在交换机 SW2 上创建 VLAN 三层接口并配置 IP 地址。

（1）依照下表，在三层交换机 SW2 上创建 VLAN 三层接口并配置 IP 地址。

表 1-6

vlan-interface	IP 地址
vlan-interface1	192. 168. 2. 254/24
vlan-interface10	192. 168. 10. 253/24
vlan-interface20	192. 168. 20. 253/24

配置如下：

```
SW2_config#interface vlan 1                                    //SW2 创建 vlan1 三层接口
SW2_config_if_vlan1#IP address 192. 168. 2. 254   255. 255. 255. 0
                                    //给 vlan1 配置 IP 地址,即交换机的管理地址
SW2_config_if_vlan1#no shutdown                                //开启 VLAN 三层接口
SW2_config#interface vlan 10                                   //SW2 创建 vlan10 三层接口
SW2_config_if_vlan10#IP address 192. 168. 10. 253   255. 255. 255. 0
                                                               //给 vlan10 配置 IP 地址
SW2_config_if_vlan10#no shutdown
SW2_config#interface vlan 20
SW2_config_if_vlan20#IP address 192. 168. 20. 253   255. 255. 255. 0
SW2_config_if_vlan20#no shutdown
```

（2）验证。

VLAN 三层接口之间相互 PING，能够 PING 通，即完成该步骤。同时，电脑能 PING 通所有 vlan1、vlan10、vlan20 三层接口的 IP 地址。

步骤 4：跨交换机的相同 VLAN 互通。

（1）要求将两台三层交换机 SW1 和 SW2 的端口 E0/0/24 与交换机 SW3 互连，并将该端口设置成骨干端口，确保跨交换机的相同 VLAN 可以互通。

```
SW1_config#interface ethernet 0/0/24
SW1_config_ethernet0/0/24#switchport mode trunk          //将端口 24 设置为 trunk 模式
SW1_config_ethernet0/0/24#switchport trunk allowed VLAN all
                                                  //设置端口 trunk,允许所以 VLAN 通过
SW2_config#interface ethernet 0/0/24
SW2_config_ethernet0/0/24#switchport mode trunk
SW2_config_ethernet0/0/24#switchport trunk allowed VLAN all
SW3_config#interface ethernet 0/0/23
SW3_config_ethernet0/0/23#switchport mode trunk
SW3_config_ethernet0/0/23#switchport trunk allowed VLAN all
SW3_config#interface ethernet 0/0/24
SW3_config_ethernet0/0/24#switchport mode trunk
SW3_config_ethernet0/0/24#switchport trunk allowed VLAN all
```

（2）验证。

交换机 SW1 的 vlan1 三层接口与交换机 SW2 的 vlan1 三层接口之间相互 PING，能够 PING 通；交换机 SW1 的 vlan2 三层接口与交换机 SW2 的 vlan2 三层接口之间相互 PING，能够 PING 通，即完成该步骤。

1.5.4　配置 RIP 协议

1. 设置防火墙 FW1

步骤 1：打开“网络”选项卡中“路由”菜单下的“目的路由列表”，出现如图 1－2 所示的界面。

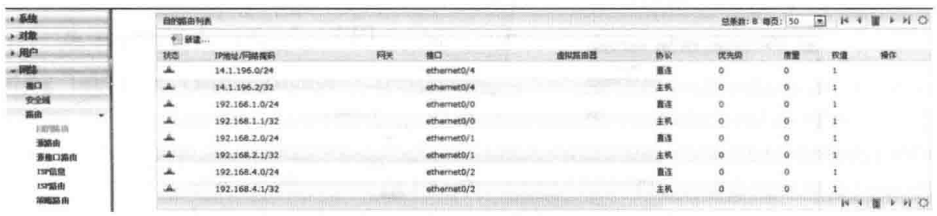

图 1－2　目的路由列表