第一篇
教学项目准备

合抱之木，生于毫末；九层之台，起于累土；千里之行，始于足下。

——《老子》

项目 0
项目准备

0.1 教学项目导入

0.1.1 教学项目描述

某知名外企 AAA 公司步入中国，在上海成立了总部。为满足公司经营及管理的需要，现在准备建立公司信息化网络。总部办公区设有市场部、财务部、人力资源部、信息技术部、总经理及董事会办公室等 5 个部门，各部门办公地点并不集中。为了业务的开展需要，又在浦东新区设立了一个分部。

各部门信息点具体需求数目如表 0-1 所示，AAA 公司网络拓扑结构如图 0-1 所示。

表 0-1 各部门信息点具体需求数目

部　　门	信　息　点
市场部	100
财务部	40
人力资源部	17
总经理及董事会办公室	10
信息技术部	13
公司分部	30

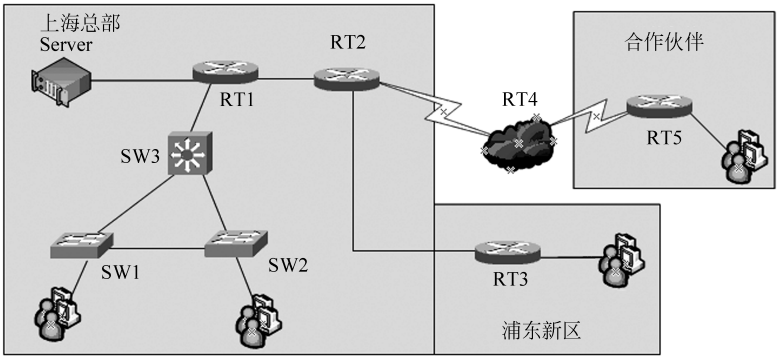

图 0-1 AAA 公司网络拓扑结构

0.1.2 教学项目要求

请根据上面的公司网络拓扑结构及下面的具体要求搭建网络，并将所有设备上的最终

配置结果保存到各自启动配置中。具体要求如下。

1. 网络物理连接

网络物理连接需要的设备及接口情况见表0-2。

表0-2 网络物理连接需要的设备及接口情况

源设备名称	设备接口	目标设备名称	设备接口
SW1	F0/1	SW3	F0/1
SW1	F0/3	SW2	F0/3
SW2	F0/2	SW3	F0/2
SW2	F0/3	SW1	F0/3
SW3	F0/1	SW1	F0/1
SW3	F0/2	SW2	F0/2
SW3	F0/3	RT1	F0/0
RT1	F1/0	RT2	F0/0
RT1	F0/1	Server	
RT2	S1/0	RT4	S1/0
RT2	F0/1	RT3	F0/1
RT3	F0/0	PC4	
RT4	S1/1	RT5	S1/1
RT5	F0/0	PC5	

2. 网络设备配置

(1) 网络设备基本配置

根据表0-3为网络设备配置主机名。

表0-3 网络设备配置主机名

设备名称	配置主机名(Sysname名)	说　明
SW1	SW1	总部接入层交换机
SW2	SW2	总部接入层交换机
SW3	SW3	总部核心层交换机
RT1	RT1	公司总部路由器
RT2	RT2	公司出口路由器
RT3	RT3	分部路由器
RT4	RT4	公网路由器
RT5	RT5	合作伙伴路由器

(2) VLAN配置

为了做到各部门二层隔离,需要在交换机上进行VLAN划分与端口分配。根据表0-4完成VLAN配置和端口分配。

表 0-4　VLAN 配置和端口分配

VLAN 编号	VLAN 名称	说　　明	端 口 映 射
VLAN 10	Marketing	市场部	SW1 与 SW2 上的 F0/5～F0/10
VLAN 20	Finance	财务部	SW1 与 SW2 上的 F0/11～F0/13
VLAN 30	HR	人力资源部	SW1 与 SW2 上的 F0/14～F0/16
VLAN 40	CEO	总经理及董事会办公室	SW1 与 SW2 上的 F0/17～F0/19
VLAN 50	IT	信息技术部	SW1 与 SW2 上的 F0/20～F0/22
VLAN 1	manage	交换机管理 VLAN	--

(3) 网络可靠性实现

在交换机上配置 RSTP 防止二层环路。

(4) IP 地址的规划与配置

由于公网地址紧张,所以只能在公司的总部和分部使用私网地址。计划使用 10.0.0.0/23 地址段。IP 地址的规划与配置见表 0-5。

表 0-5　IP 地址的规划与配置

区　　域	IP 地址段	网　　关
市场部	10.0.0.0/25	10.0.0.126
财务部	10.0.0.128/26	10.0.0.190
人力资源部	10.0.0.192/27	10.0.0.222
总经理及董事会办公室	10.0.0.224/28	10.0.0.238
信息技术部	10.0.0.240/28	10.0.0.254
公司分部	10.0.1.0/27	10.0.1.30
合作伙伴	10.0.2.0/27	10.0.2.30
交换机管理 VLAN	192.168.100.0/29	—

设备的 IP 地址如表 0-6 所示。

表 0-6　设备的 IP 地址

设　　备	IP 地址
RT4—RT5	202.0.1.0/29
RT2—RT4	202.0.0.0/30

其余设备间互连地址使用 172.16.0.0/24 网段,并使用 30 位掩码,如表 0-7 所示。

表 0-7　其余设备间互连地址

设　　备	IP 地址
SW3—RT1	172.16.0.0/30
RT1—Server0	172.16.10.0/30
RT1—RT2	172.16.1.0/30
RT2—RT3	172.16.2.0/30

(5) 路由配置

公司总部配置为OSPF的骨干区域。公司分部使用静态路由,将公司分部的静态路由引入OSPF中。

(6) 广域网链路配置

RT2与RT4使用广域网串口线连接,使用PPP协议的CHAP验证;为RT4和RT5之间添加PPP协议的PAP验证。

3. 网络安全配置

(1) 控制子网间的访问

在总部路由器RT1上配置扩展的ACL以禁止分部访问公司总部的财务部;在分部路由器RT3上配置标准的ACL以禁止公司总部的市场部访问分部。

(2) 转换网络间的地址

在接入路由器RT2上配置PAT,使总部、分部所有主机(服务器除外)能通过申请到的一组公网地址(202.0.0.0/29)中的地址池202.0.0.2/29～202.0.0.4/29访问Internet,并在RT2上配置静态NAT,使用公网地址202.0.0.5/29将公司总部的WWW、FTP服务器Server0发布到Internet,允许公网用户访问;在合作伙伴路由器RT5上配置PAT,以使用其申请到的唯一公网地址(202.0.1.2/30)接入Internet。

(3) 建立安全隧道

为了传输机要信息,分部与总部总经理及董事会办公室之间采用安全隧道的方式通信。在总部路由器RT1上及分部路由器RT3上配置IPSec VPN,使用ESP加3DES加密并使用ESP结合SHA做HASH计算,以隧道模式封装,设置密钥加密方式为3DES,并使用预共享的密码进行身份验证。

(4) 设备安全访问设置

为网络设备开启远程登录(Telnet)功能,按照表0-8为网络设备配置相应密码,并且只允许信息技术部的工作人员可以通过Telnet访问设备。

表0-8 设备安全访问设置

设备名称(主机名)	远程登录密码
RT1	000000(明文)
RT3	000000(明文)
SW3	000000(明文)
SW2	000000(明文)
SW1	000000(明文)

4. 无线网络配置

合作伙伴计算机设备分散,其中的计算机数目也在逐步增加。在这种情况下,全部用有线网连接终端设施,从布线到使用都会极不方便;有的房间是大开间布局,地面和墙壁已经施工完毕,若进行网络应用改造,埋设缆线工作量巨大,而且位置无法十分固定,导致信息点的放置也不能确定,这样构建一个无线局域网络就会很方便。若整个WLAN完全暴露在一个没有安全设置的环境下,是非常危险的。因此需要在无线接入点或无线路由器上进行安

全设置。

（1）本项目的网络架构为 WLAN 和有线局域网混合的非独立 WLAN。

（2）在无线路由器上进行安全设置。

① SSID 为 rjxy。

② 无线路由器 Wireless Router0 设置 WPA-PSK 密钥验证，密钥为 87654321。

0.2　教学项目分析


网络规划设计实例讲解

本项目是一个有关企业网搭建的网络工程项目。作为一个完整的网络工程项目，从网络系统集成技术角度看，一般工作流程为：网络的规划与设计→网络综合布线→交换机与路由器配置→服务器配置→网络安全配置→无线路由配置→网络故障的分析与排除→网络的测试与验收 8 个步骤。

因本项目中指定了具体的网络规划，未涉及综合布线与服务器配置问题，从而也不再涉及网络验收问题，只保留了网络设备配置相关部分。按工作过程先后顺序，为方便读者学习，将本企业网搭建项目设计成如下 11 个独立的项目：

项目 1　登录与管理交换机

项目 2　实现 VLAN 间通信

项目 3　防止二层环路

项目 4　内外网连接

项目 5　添加静态路由

项目 6　配置动态路由

项目 7　接入广域网

项目 8　控制子网间的访问

项目 9　转换网络地址

项目 10　建立安全隧道

项目 11　无线局域网搭建

第一篇用于教学项目的准备。第二篇中 11 个独立的项目是教学项目的主体。第三篇是一个综合教学项目，是对第二篇知识和技能的提升。第四篇是综合实训。通过这样的设计，读者可以由浅入深、由简单到复杂、由易到难地掌握网络设备的基本配置技能，积累一定的项目经验。