绪　论

课程思政

- “博学之，审问之，慎思之，明辨之，笃行之。”培养学生的爱国情怀，具有基本的职业道德和职业素养；在网络管理过程中遵守法律法规、道德规范，树立诚信意识，承担社会责任。
- “莫等闲，白了少年头，空悲切。”坚定文化自信，培养学生的工匠精神、劳动意识和创新思维，通过项目法教学模式，让学生亲身体验项目的设计、管理和实施，培养一定的项目管理能力。

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，在上海浦东新区成立了自己的国内总部。为满足公司经营、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、总经理及董事会办公室、信息技术部 5 个部门，各部门办公地点并不集中。为了业务的开展需要，又在浦西设立了一个分部。

各部门信息点具体需求数目如表 0-1 所示。

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

网络拓扑结构如图 0-1 和图 0-2 所示。

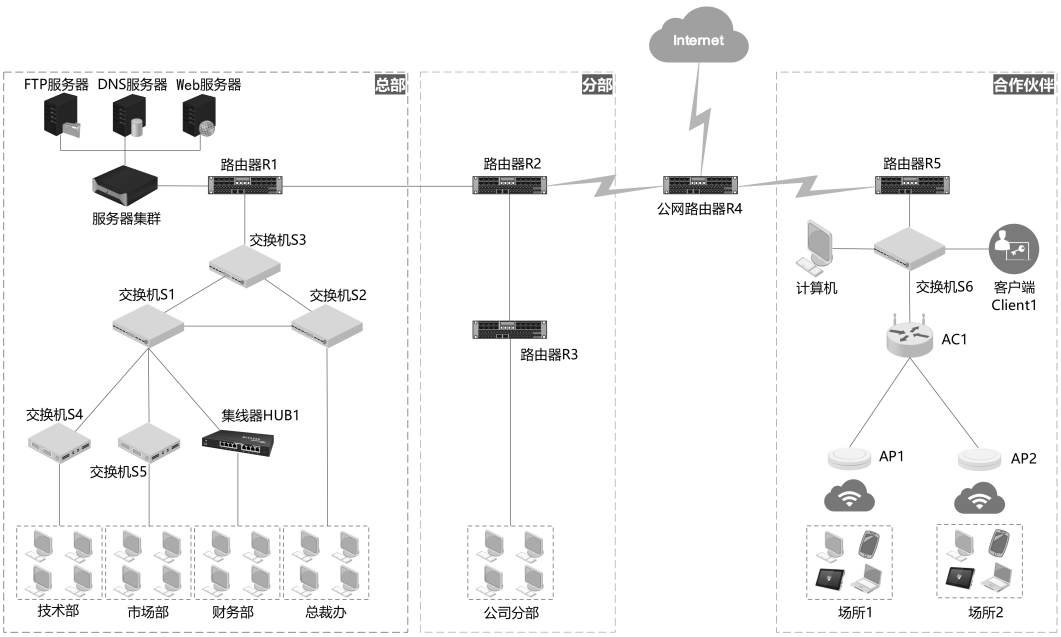

图 0-1　AAA 公司网络拓扑结构一

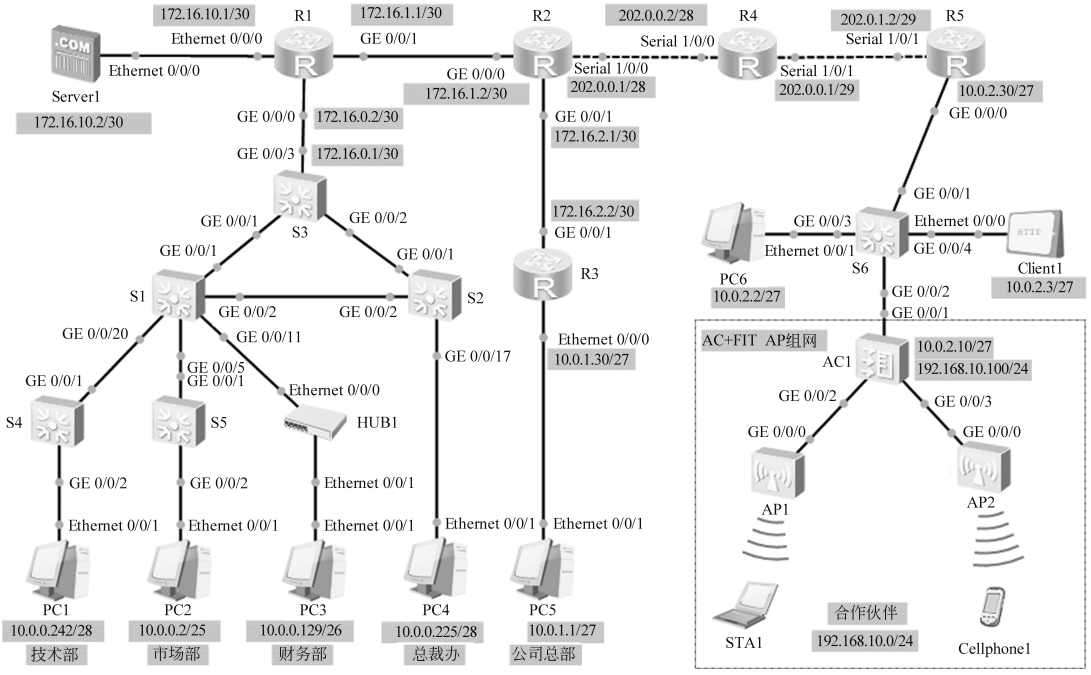

图 0-2　AAA 公司网络拓扑结构二

0.1.2　教学项目要求

请根据图 0-1 和图 0-2 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。

1. 网络物理连接

网络物理连接如表 0-2 所示。

表 0-2 网络物理连接

源设备名称	设备接口	目标设备名称	设备接口
S1	G0/0/1	S3	G0/0/1
S1	G0/0/2	S2	G0/0/2
S2	G0/0/1	S3	G0/0/2
S3	G0/0/3	R1	G0/0/0
R1	G0/0/1	R2	G0/0/0
R1	E0/0/0	Server1	E0/0/0
R2	S1/0/0	R4	S1/0/0
R2	G0/0/1	R3	G0/0/1
R3	E0/0/0	PC4	E0/0/1
S1	G0/0/20	S4	G0/0/1
S1	G0/0/5	S5	G0/0/1
S1	G0/0/11	HUB1	E0/0/0
S4	G0/0/2	PC1	E0/0/0
S5	G0/0/2	PC2	E0/0/0
HUB1	E0/0/1	PC3	E0/0/1
S2	G0/0/17	PC4	E0/0/1
R4	S1/0/1	R5	S1/0/1
R5	G0/0/0	S6	G0/0/1
S6	G0/0/3	PC6	E0/0/1
S6	G0/0/4	Client1	E0/0/0
S6	G0/0/2	AC1	G0/0/1
AC1	G0/0/2	AP1	G0/0/0
AC1	G0/0/3	AP2	G0/0/0

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 网络设备主机名

设备名称	配置主机名	说 明
S1	S1	总部接入层交换机
S2	S2	总部接入层交换机
S3	S3	总部核心层交换机

续表

设备名称	配置主机名	说　　明
S4	S4	技术部二层交换机
S5	S5	市场部二层交换机
S6	S6	合作伙伴接入交换机
HUB1	—	财务部集线器
R1	R1	公司总部路由器
R2	R2	公司出口路由器
R3	R3	分部路由器
R4	R4	公网路由器
R5	R5	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	S1 与 S2 上的 G0/0/5～G0/0/10
VLAN 20	Finance	财务部	S1 与 S2 上的 G0/0/11～G0/0/13
VLAN 30	HR	人力资源部	S1 与 S2 上的 G0/0/14～G0/0/16
VLAN 40	CEO	总经理及董事会办公室	S1 与 S2 上的 G0/0/17～G0/0/19
VLAN 50	IT	信息技术部	S1 与 S2 上的 G0/0/20～G0/0/22
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 地址规划如表 0-5 所示,IP 地址配置如表 0-6 所示。

表 0-5　IP 地址规划

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	—

表 0-6 IP 地址配置

设 备	接 口	IP 地 址	默认网关
R1	G0/0/0	172.16.0.2/30	不适用
	G0/0/1	172.16.1.1/30	不适用
	VLAN 10(E0/0/0)	172.16.10.1/30	不适用
R2	G0/0/0	172.16.1.2/30	202.0.0.6
	G0/0/1	172.16.2.1/30	
	S1/0/0	202.0.0.1/28	
R3	G0/0/1	172.16.2.2/30	172.16.2.1
	E0/0/0	10.0.1.30/27	
R4	S1/0/0	202.0.0.6/28	不适用
	S1/0/1	202.0.1.1/29	不适用
R5	G0/0/0	10.0.2.30/27	202.0.1.1
	S1/0/1	202.0.1.2/29	
S1	VLAN 1	192.168.100.1/29	不适用
S2	VLAN 1	192.168.100.2/29	不适用
S3	VLAN 1	192.168.100.3/29	不适用
	VLAN 2(G0/0/3)	172.16.0.1/30	不适用
	VLAN 10(G0/0/5～G0/0/10)	10.0.0.126/25	不适用
	VLAN 20(G0/0/11～G0/0/13)	10.0.0.190/26	不适用
	VLAN 30(G0/0/14～G0/0/16)	10.0.0.222/27	不适用
	VLAN 40(G0/0/17～G0/0/19)	10.0.0.238/28	不适用
	VLAN 50(G0/0/20～G0/0/22)	10.0.0.254/28	不适用
S4	VLAN 1	10.0.0.241/28	不适用
S5	VLAN 1	10.0.0.1/25	不适用
PC1	E0/0/1	10.0.0.242/28	10.0.0.254
PC2	E0/0/1	10.0.0.2/25	10.0.0.126
PC3	E0/0/1	10.0.0.129/26	10.0.0.190
PC4	E0/0/1	10.0.0.225/28	10.0.0.238
PC5	E0/0/1	10.0.1.1/27	10.0.1.30
PC6	E0/0/1	10.0.2.2/27	10.0.2.30
Server1	E0/0/0	172.16.10.2/30	172.16.10.1
Client1	E0/0/0	10.0.2.3/27	10.0.2.30
AC1	VLAN 1	10.0.2.10/27	10.0.2.30
	VLAN 10(G0/0/2～G0/0/3)	192.168.10.100/24	

(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。R2 与 R4 使用广域网串口线连接,使用 PPP 的 CHAP 验证,为

R4 和 R5 之间添加 PPP 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 R1 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 R3 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 R2 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 用于总部访问外网与 202.0.0.6/29～202.0.0.8/29 用于分部访问外网,并在 R2 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 Server1 发布到 Internet,允许公网用户访问;在合作伙伴路由器 R5 上配置 PAT,以使用其申请到的唯一公网地址(202.0.1.2) 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 R1 上及分部路由器 R3 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(SSH)功能以及本地密码,按照表 0-7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 SSH 访问设备。

表 0-7　网络设备的密码

设备名称(主机名)	账号	远程登录密码	本地密码
R1	root	111111	123456
R2	root	111111	123456
R3	root	111111	123456
R5	root	111111	123456
S3	root	111111	123456
S2	root	111111	123456
S1	root	111111	123456

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,敷设缆线工作量巨大,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 HZHB。

② 无线路由器设置 WPA-PSK 密钥验证,密钥为 12345678。

0.2 教学项目分析

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。

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，因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，为方便学习，将本企业网搭建项目设计成以下 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

这 11 个独立项目是教学项目的主体，作为本书第二篇。在完成第二篇的基础上，读者有了初步的项目实践经验，可以进行第三篇的学习。第三篇是一个综合的教学项目，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，从而积累一定的项目经验。