网络工程专业职教师资
培养系列教材

中小型企业网络构建

赖会霞　主编

科学出版社

网络工程专业职教师资培养系列教材

中小型企业网络构建

赖会霞　主编

科学出版社

北京

内 容 简 介

本书以一个典型的中小型企业网络构建项目为驱动，介绍网络工程的一般流程，以及项目实施过程中涉及的主要技术和相关知识。书中所述配置命令、配置实例以及项目实施部分均基于 Cisco 的路由器和交换机，读者进行实验时可以在配备了 Cisco 网络设备的实验室进行，也可以使用相关模拟器进行实验，例如 Cisco Packet Tracer、GNS3 等。

本书分为 9 章，第 1 章项目介绍给出了贯穿全书的中小型企业网络构建项目，后续各章根据中小型企业网络构建的一般流程，将教材内容划分为 8 个任务。具体包括： IP 地址规划、路由器及交换机基本配置、VLAN 划分及配置、生成树协议及路由热备份的配置、网络路由的配置、配置网络地址转换、配置访问控制列表、配置虚拟专用网 VPN。

本书可以作为职业技术学校网络工程或相关专业的教材，也可以作为大中专院校相关专业的课程教材，也适用于网络技术爱好者和初学者自学或作为参考资料。

图书在版编目(CIP)数据

中小型企业网络构建/赖会霞主编. —北京：科学出版社，2016
网络工程专业职教师资培养系列教材
ISBN 978-7-03-048809-1

Ⅰ. ①中… Ⅱ. ①赖… Ⅲ. ①中小企业-计算机网络-师资培养-教材
Ⅳ. ①TP393.18

中国版本图书馆 CIP 数据核字(2016)第 132857 号

责任编辑：张丽花 于海云/ 责任校对：桂伟利
责任印制：张 伟 / 封面设计：迷底书装

科 学 出 版 社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

北京中石油彩色印刷有限责任公司 印刷

科学出版社发行 各地新华书店经销

*

2016 年 6 月第 一 版 开本：787×1092 1/16
2016 年 6 月第一次印刷 印张：12 1/4
字数：280 000

定价：43.00 元

(如有印装质量问题，我社负责调换)

前　言

随着计算机网络技术的飞速发展和普遍应用，当今社会已经进入信息经济和知识经济的时代。在这样的环境下，推进企业信息化建设、实现信息化管理已经成为提高企业核心竞争力的重要条件。日益增长的网络建设及网络维护的社会需求，要求培养更多的高素质的网络工程专业人才。而企业网络构建是一个网络工程人员必须具备的技能，本书的编写目的和意义就在于此。

企业网络构建课程实践性较强，在教学目标的设计上，应注重培养学生将所学理论知识与技能应用到工程实践中的能力。因此，本教材在编写上注重理论与实践相结合，实现理实一体化。充分考虑了该课程实践性较强的特点，在内容编排上打破传统教材的编写模式，采用项目驱动模式。以一个典型的中小型企业网络工程项目为主线贯穿全书，按照网络工程的实际流程，将该项目的实施分解为若干任务。每个任务解决中小型企业网络工程项目中的一个问题，达到全书学完后即可完成整个项目的目的。

本书在内容编排上的主要特点如下。

(1)项目驱动：本书在第 1 章给出一个完整的典型的中小型企业网络构建的项目，并将其分解为 8 个任务，以完成该项目为目的安排后续各章的内容。

(2)提出问题，明确任务：在后续各章中，首先提出需要解决的问题及解决问题需要的理论知识和相关技术；详细描述需要完成的任务需求，以完成任务为目标有针对性地进行学习。

(3)相关知识：在明确了任务需求和需要解决的问题后，介绍所需的理论知识和相关技术。

(4)技能训练：针对每一部分所学的理论知识和相关技术，精心设计了对应的实验案例，使读者通过动手实践，加深对理论知识的理解，提高技能水平，真正做到“在学中做，在做中学”。

(5)融会贯通：每章最后安排任务实施，将本章所学理论及技能应用于项目中，完成项目中对应本章的一个任务，全书学完，即可完成整个项目。因为全书以一个项目贯穿，能很好地使读者将全书所学知识和技能融会贯通，真正培养将所学知识和技能应用于工程实践中的能力，而不仅仅是掌握了一些零散的知识和技能。

本书分为 9 部分，第 1 部分给出贯穿全书的中小型企业网络构建项目，后续各部分根据中小型企业网络构建的一般流程，将教材内容先划分为 8 个任务，内容涵盖了企业网络构建的主要技术和相关理论知识。具体任务包括：IP 地址规划、路由器及交换机基本配置、VLAN 划分及配置、生成树及路由热备份的配置、网络路由的配置、配置网络地址转换、配置访问控制列表、配置虚拟专用网 VPN。

在使用本教材时，可以在学习每章的相关知识并动手完成对应实验案例进行技能训练后，即进行任务实施，将项目的各任务分布在每章学习中完成；亦可先学习每章的相关知识、训练技能，将全书所有相关知识学完，并通过动手实验掌握技能，最后再完成项目各任务的实施。

本书可以作为职业技术学校网络工程或相关专业的教材，也可以作为大中专院校相关专业的课程教材。同时适用于网络技术爱好者和初学者自学或作为参考资料。

由于作者水平所限，书中难免存在不足和疏漏之处，恳请广大读者和同行不吝赐教，不胜感激。作者的电子邮箱：lhx@fjnu.edu.cn。

赖会霞

2015 年 12 月于福建师范大学

目　录

项目介绍　中小型企业网络构建

随着计算机网络技术的发展，信息化越来越成为一个企业核心竞争力的重要体现。为了实现高效的管理与沟通方法，增强市场竞争力，建设企业网络、实行信息自动化管理已经成为越来越多的企业的需求。本书将以某公司的网络建设为例，介绍中小型企业网络构建的基本流程和相关技术。

学习目标

- 明确项目需求；
- 根据项目需求构建中小型企业网络拓扑；
- 明确项目的任务分解。

项目需求描述

某公司在 A、B 两地分别设有公司总部和分公司。现需要为该公司建设企业园区网络，需要将公司总部和分公司互联，以实现企业内部安全、高效的数据通信及资源共享；同时，总公司和分公司都需要接入 Internet 网络。目前，公司只申请到有限数量的公网 IP 地址，企业网络内部需要使用私有 IP 地址，但需要全网接入 Internet。

网络需求描述如下：

(1) 公司总部包括财务部、开发部、销售部以及服务器区，分公司包括开发部和销售部。因提高数据传输效率、保证数据传输安全等因素，需要按照部门对公司内部网络进行广播域分割，公司所有服务器需要在一个独立的广播域内。

(2) 公司总部规模大，承担公司主要业务以及所有服务器的运行维护，对网络安全性和可靠性要求高，要求核心设备冗余备份；为了节约成本，规模较小的分公司不设核心设备冗余备份。

(3) 为了节省公网 IP 地址，内部均使用私有 IP 地址，但要能与 Internet 网络通信。

(4) 为了保证内部网络安全，以及内部网络各部门之间访问权限的限制，需要根据公司具体要求过滤内部网络与外部网络之间的数据包，以及内部网络各部门之间的数据包。

(5) 使用路由协议或者静态/默认路由，实现内部网络的连通以及对 Internet 网络的访问。

1.1　分层网络设计概述

在进行网络设计时，一般采用分层网络设计思想。一个大规模的网络系统往往被分为几个较小的部分，它们之间既相对独立又相互关联。这种化整为零的设计方法称为分层设计。

Cisco 提出的三层分层模型包括核心层 (Core Layer)、汇聚层 (Distribution Layer) 和接入层 (Access Layer)，如图 1-1 所示。

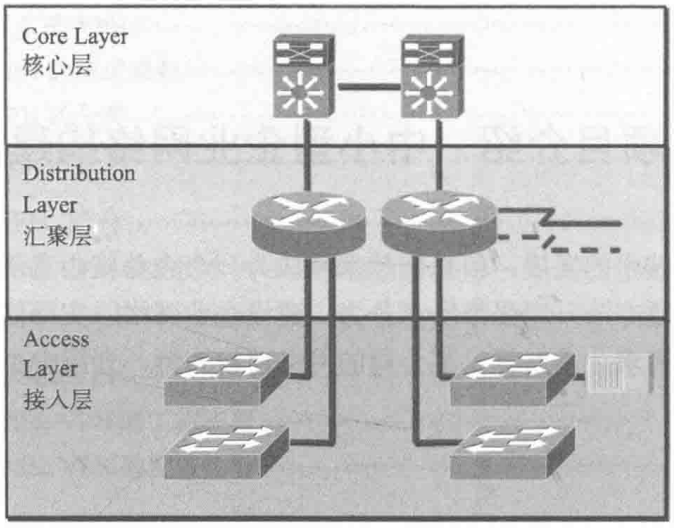

图 1-1　Cisco 的三层分层模型

其中每一层都有其特定的功能，下面对每一层的功能进行详细说明。

(1)核心层位于网络的最顶层，被视为主干网络，其主要功能是实现快速而可靠的数据传输。核心层所处的特殊位置，决定了核心层的性能和可靠性对整个网络的性能和可靠性是至关重要的。一旦核心层出现故障，将影响整个网络的数据传输。因此在设计核心层时，只将高可靠性、高速的传输作为其设计目标，而影响传输速度的数据处理则不放在核心层实现。核心层交换机需要具有较高的可靠性和性能。

(2)汇聚层位于核心层和接入层中间，负责连接接入层和核心层，将众多的接入层接入点汇集起来，屏蔽接入层对核心层的影响。汇聚层需要实现一些网络策略，包括提供路由、实现包过滤、网络安全、创建 VLAN 并实现 VLAN 间路由、分割广播域、WAN 接入等。汇聚层交换机仍需要较高性能和比较丰富的功能。

(3)接入层又称为桌面层，提供用户或工作站的网络接入，用户可以通过接入层访问网络设备。接入层交换机的数量较多，在设备选择上需要选择易于使用和维护、具有较高性价比和高端口密度的交换机。

分层设计的主要优点如下

(1)把复杂的网络问题进行层次分割，每层次执行特定的功能，使复杂的网络问题更易于解决。

(2)各层间相对独立，某一层的拓扑结构变化不会影响其他层。

(3)使用分层模型设计的网络更易于实现和维护，并具有更好的可扩展性。

1.2　核心层设计

核心层是互联网络的高速主干，核心层的性能和可靠性对于网络互联是至关重要的，因此核心层设计的主要目标如下：

- 提高网络的可靠性；
- 提供冗余；
- 提供故障隔离；

- 提供高速转发速率；
- 快速适应升级。

基于上述目标，核心层设计时需要遵循以下原则。

1)可达性

要保证网络中每个目的地的可达性，通常应该注意以下几个方面的要求：

(1)具有足够的路由信息来交换发往网络中节点的数据包；

(2)核心层的路由器不应该使用默认路由到达内部网络的目的地；

(3)通过聚合路径减少核心层路由表大小；

(4)默认路由用来与外部通信，如与 Internet 通信。

2)冗余性

冗余性设计的目的是保障核心网络的可靠性，通常可以通过增加冗余设备、冗余模块或者冗余链路的方式实现。

3)不在核心层执行网络策略

(1)任何形式的网络策略必须在核心层之外执行，如数据包的过滤和 QoS 等；

(2)禁止采用任何降低核心层处理能力或增加数据包交换延迟时间的方法；

(3)避免增加核心层设备配置的复杂度；

对于大型的园区网或重要部门的局域网，为了保证网络的可靠性，核心层一般采用设备冗余技术，即使用两台核心交换机互为备份，这样也可以实现负载均衡。当网络规模较小时，通常使用一台核心交换机，该核心交换机与汇聚层的所有交换机相连，此时可以使用链路冗余技术增强网络的可靠性。而当网络规模更小时，为了节约建网成本，可以合并核心层与汇聚层，核心层交换机可以直接与接入层交换机相连，以这种方式设计的网络易于配置和管理，但其可扩展性较差，容错能力也较差。

1.3　汇聚层设计

汇聚层是网络核心层与接入层之间的分界点。汇聚层将大量低速的连接(与接入层设备的连接)通过少量高速的连接接入核心层，以实现通信量的收敛，提高网络聚合点的效率，同时减少核心层设备路由项的数量。

汇聚层的主要任务是提供与流量控制、安全及路由相关的策略，具体内容如下：

- 定义广播域和组播域；
- 执行安全策略和网络策略，如 QoS、静态或动态路由、数据包过滤等；
- 实现 VLAN 之间的路由；
- 完成部门或工作组级的数据交换；

汇聚层的主要设计目标如下。

1. 隔离拓扑结构的变化

隔离核心层和接入层，因为网络拓扑变化多发生在接入层(如增加网段、重新分段等)，增加汇聚层可以将接入层的拓扑变化对核心层的影响降到最低。

2. 通过路由聚合控制路由表的大小

较小的路由表意味着占用较小的存储空间，花费较少的寻址时间，获得较快的数据转发速度。在汇聚层进行有效的路由聚合可以减小核心层的路由表，保证核心层的高速转发。

路由聚合的计算方法示例：如路由表中存储了如下 4 个网络。

172.16.12.0/24

172.16.13.0/24

172.16.14.0/24

172.16.15.0/24

要计算路由器的聚合路由，首先要判断这些地址的高位有多少位是相同的。计算汇总路由的步骤如下：

(1)将地址转换为二进制格式，并将它们对齐。

172.16.12.0/24 =10101100.00010000.00001100.00000000

172.16.13.0/24= 10101100.00010000.00001101.00000000

172.16.14.0/24= 10101100.00010000.000011 10.00000000

172.16.15.0/24= 10101100.00010000.000011 11.00000000

(2)确定所有地址中高位相同的位数，本例中 4 个 IP 地址高位相同的位数为 22 位。

(3)计算聚合后的网络号及掩码。聚合后的网络号就是 IP 地址高位相同的值，在本例中聚合后的 IP 地址是 172.16.12.0，掩码即高位相同的位数，本例中掩码为 22 位，所以 4 个网络 IP 地址 172.16.12.0～172.16.15.0 最佳的聚合路由为 172.16.12.0/22。

3. 收敛网络流量

汇聚层收集接入层的流量，转发到上连的核心层。

1.4　接入层设计

接入层的主要设计目标如下：

(1)接入层控制用户和工作组对互联网络的访问。大多数用户所需的网络资源在本地获取，汇聚层处理远程服务的访问流量。

(2)控制访问。由于接入层是用户接入网络的入口，所以也是黑客入侵的门户，所以必须进行访问控制。如防止直通的数据、对数据分组进行过滤等。

1.5　项 目 介 绍

根据项目需求，该中小型企业网络项目描述如下：

(1)总公司和分公司内部网络设计为两层结构，将核心层与汇聚层合并；核心层选择 Cisco Catalyst 3560 三层交换机，接入层选择 Cisco Catalyst 2960 二层交换机。

(2)为了提高总公司网络的安全性和高可靠性，使用生成树协议和路由热备份协议，实现冗余备份和负载均衡。

(3)在总公司和分公司内部网络中，均使用 VLAN 技术，按照部门对内部网络进行 VLAN 划分。

(4)因公司内部均使用私有 IP 地址，且需要与 Internet 网络通信，因此在网关路由器上使用 NAT 技术实现 IP 地址转换。

(5)为了保证内部网络的安全，以及实现内部网络各部门之间的访问权限控制，采用 ACL 技术。

(6)使用 OSPF 协议实现内部网络的互连，在网关路由器和内部网络三层交换机上使用默认路由，实现内部网络与 Internet 网络的通信。

(7)为了节约成本，同时保证公司内部通信的安全性，总公司和分公司之间的互联选择 IPSec VPN 技术。

企业网络拓扑图如图 1-2 所示。

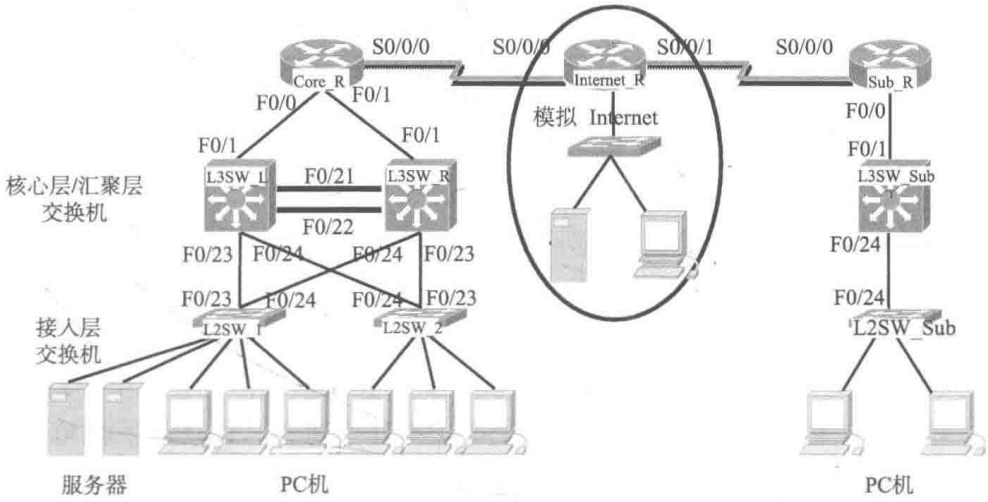

图 1-2　企业网络拓扑图

在该项目中，将核心层与汇聚层合并。使用一台路由器、一台服务器、一台 PC 机模拟 Internet 网络，便于测试企业网络与 Internet 网络的通信。在学习过程中，可以根据实际教学环境对 PC 机的数量进行增减。

在拓扑图中，标注了设备的主机名，以及设备之间连接所使用的接口。在构建拓扑时，可以按照拓扑图中标注的接口连接各设备，在后续课程中分解任务的实施方案均按照拓扑图中标注的连接情况进行设计及配置。读者也可以自行确定设备连接所需接口，但需要注意在进行后续任务的配置时按照自己设计的设备间接口连接情况进行配置。

1.6　任 务 分 解

在本书后续章节，我们将围绕该项目的具体实施展开介绍。根据该项目建设的需求，我们将该项目分解为如下几个任务。

任务 1：IP 地址规划。

任务 2：路由器及交换机基本配置。

任务 3：VLAN 划分及配置。

任务 4：生成树协议及路由热备份的配置。
任务 5：网络路由的配置。
任务 6：配置网络地址转换。
任务 7：配置访问控制列表。
任务 8：配置虚拟专用网 VPN。

任务 1　IP 地址规划

合理的 IP 地址规划对于企业网络设计尤其是大中型企业网络设计是至关重要的一个环节。合理、统一的 IP 地址规划将直接影响网络的性能、网络的可扩展性、可管理性以及网络的可用性。

学习目标

- 理解 IP 地址的概念和分类；
- 理解子网掩码的概念，掌握子网划分的方法；
- 理解 IP 地址规划原则；
- 根据需求进行企业网络 IP 地址规划。

任务需求

在这一单元中，我们需要解决的问题是为中小型企业网络构建项目规划 IP 地址。

根据项目需求描述，该公司由总公司和分公司组成，构建企业网络要求总公司及分公司均有自己的内部网络，且还要将总公司和分公司的内部网络互联起来。因此，在构建网络之前，需要对总公司和分公司的网络进行统一的 IP 地址规划。

在进行 IP 地址规划时，应遵守 IP 地址规划的相关原则和指导意见。

公司根据国家相关法律规定，已经申请到有限数量的公有 IP 地址，以满足企业网络内部一些对外提供服务的服务器的需要。

由于公有 IP 地址数量所限，企业网内部普通用户以及不需要对外提供服务的服务器使用私有 IP 地址。在进行 IP 地址规划时，企业内部网络需要使用私有 IP 地址。

2.1　IP　地　址

IP 地址由 32 位二进制位组成，在使用中用点分十进制(Dotted Decimal)表示。

2.1.1　IP 地址的概念

我们把整个 Internet 看成一个单一的、抽象的网络，IP 地址就是给每个连接在 Internet 上的主机(或路由器)分配一个在全世界范围内唯一的 32 位的标识符。

根据 TCP/IP 规定，IP 地址由 32 位二进制位组成，在使用中用点分十进制表示。通常将 32 位的二进制 IP 地址平均分成 4 组，每组 8 位，组与组之间用点号隔开，表示为 x.x.x.x 的格式，例如，192.168.1.1，每个 x 的取值范围为 0～255。Internet 管理委员会将 IP 地址分为 A、B、C、D 和 E 类 5 大类。其中 A、B、C 三类是主要的 IP 地址类型，用于网络组建，而 D 类是提供给组播使用的组播地址，E 类是保留的 IP 地址。IP 地址的分类如图 2-1 所示。

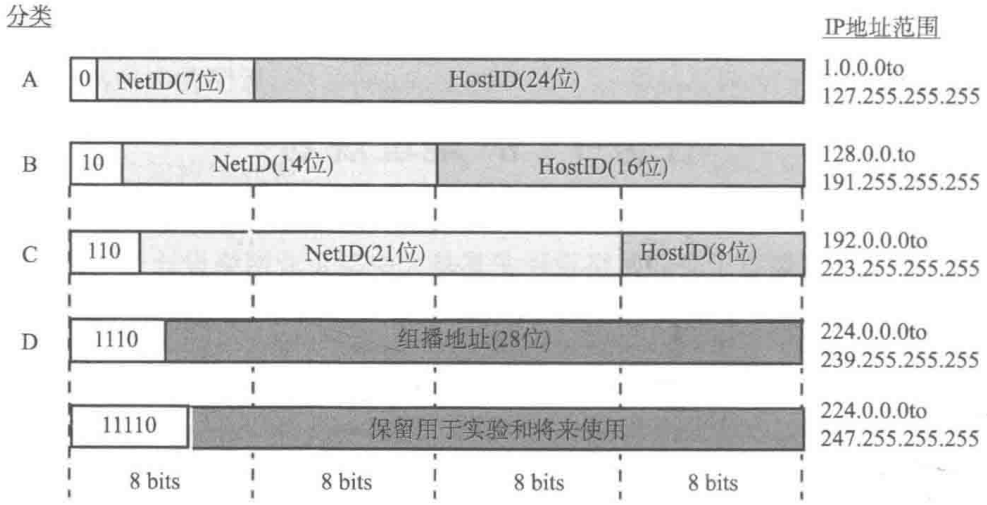

图 2-1　IP 地址分类

如图 2-1 所示，每一类地址都由两个固定长度的字段组成。其中一个字段是网络号 NetID，它标志主机(或路由器)所连接到的网络；而另一个字段则是主机号 HostID，它标志该主机(或路由器)。两级的 IP 地址可以记为：**IP 地址 ::= { <网络号>, <主机号>}**，其中：：表示“定义为”。

不同分类的 IP 地址是使用前几位的不同取值进行区分的。如 A 类地址的第一位取值为“0”。

1. A 类地址

- A 类地址的第一位取值为“0”；
- A 类地址网络号 NetID 的长度为 7 位，主机号 HostID 的长度为 24 位；
- A 类地址的范围是 1.0.0.0～127.255.255.255；
- 网络号 NetID 的长度为 7 位，所以允许有 126 个不同的 A 类网络(共 2^7=128 个 A 类地址，其中网络地址的 0 和 127 保留，用于特殊用途)；
- 主机号 HostID 的长度为 24 位，所以每个 A 类网络包含的 IP 地址数多达 2^{24} 约 16 000 000 个；
- A 类 IP 地址结构适用于有大量主机的大型网络。

2. B 类地址

- B 类地址最高两位取值为“10”；
- B 类地址网络号 NetID 的长度为 14 位，主机号 HostID 的长度为 16 位；
- B 类 IP 地址的范围是 128.0.0.0～191.255.255.255；
- 网络号 NetID 的长度为 14 位，所以允许有 2^{14}=16 384 个不同的 B 类网络；
- 主机号 HostID 的长度为 16 位，所以每个 B 类网络包含的 IP 地址数多达 2^{16}=65 536 个；
- B 类 IP 地址适用于一些国际性大公司与政府机构等。

3. C 类地址

- C 类地址最高 3 位取值为“110”；