

“十三五”

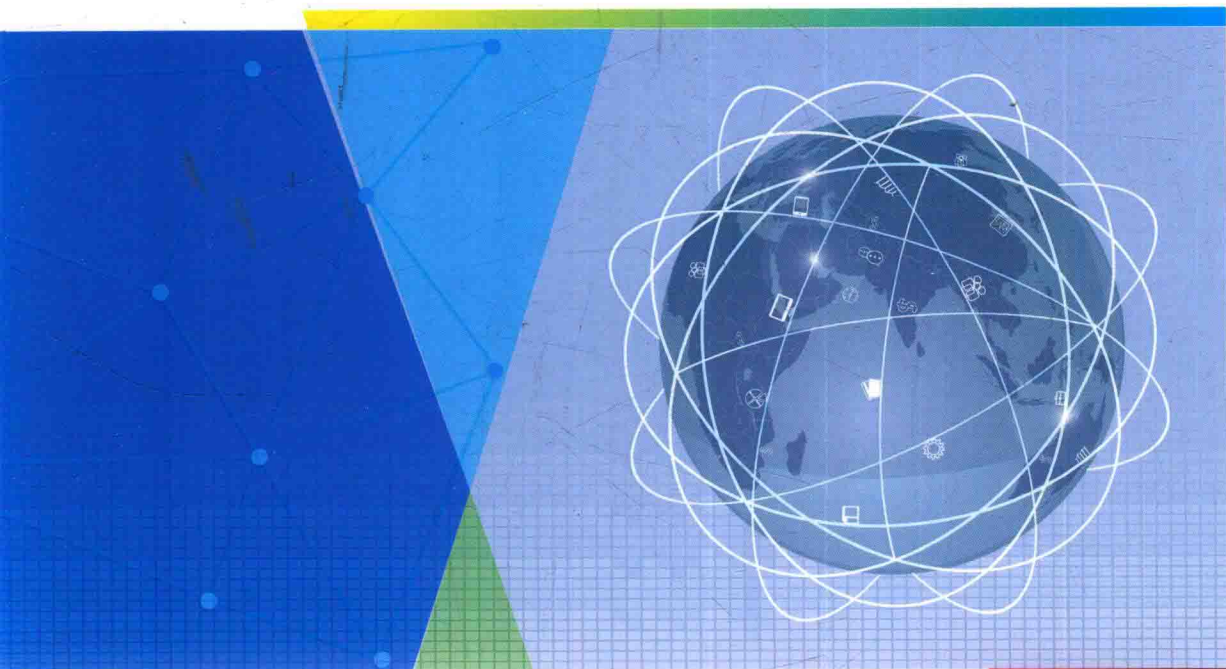
国家重点图书出版规划项目
ICT认证系列丛书



华为信息与网络技术学院指定教材

高级网络技术

田果 刘丹宁 余建威 / 著



LEADING NEW ICT



中国工信出版集团



人民邮电出版社
POSTS & TELECOM PRESS

★ ★ ★
★ “十三五” ★

国家重点图书出版规划项目
ICT认证系列丛书



华为信息与网络技术学院指定教材

高级网络技术

田果 刘丹宁 余建威 / 著

人民邮电出版社
北京

图书在版编目 (C I P) 数据

高级网络技术 / 田果, 刘丹宁, 余建威著. — 北京:
人民邮电出版社, 2017. 11
(ICT认证系列丛书)
ISBN 978-7-115-45649-6

I. ①高… II. ①田… ②刘… ③余… III. ①计算机
网络 IV. ①TP393

中国版本图书馆CIP数据核字(2017)第227419号

内 容 提 要

本书是华为 ICT 学院路由与交换技术官方教材, 旨在帮助读者理解和掌握在实际工作中常见技术的原理和操作方法。

第 1 章介绍了企业网的架构、设计与发展趋势。在后面各章中, 会分别介绍各类网络冗余技术、访问控制列表的使用、网络地址转换技术的配置、各类广域网技术的原理与配置、DHCP 的原理以及 DHCP 服务器和中继的配置、IPv6 原理与 IPv6 路由、重要的网络安全技术、无线技术的概述以及网络管理协议相关的知识。

除华为 ICT 学院的学生之外, 本书同样适合正在备考 HCNA 认证或者正在参加 HCNA 技术培训的人士进行阅读和参考。其他有志从事 ICT 行业的初级人员和网络技术爱好者也可以通过阅读本书, 加深对网络技术的理解。

-
- ◆ 著 田 果 刘丹宁 余建威
责任编辑 李 静
责任印制 彭志环
 - ◆ 人民邮电出版社出版发行 北京市丰台区成寿寺路 11 号
邮编 100164 电子邮件 c_315@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
北京圣夫亚美印刷有限公司印刷
 - ◆ 开本: 787×1092 1/16
印张: 26.75 2017 年 11 月第 1 版
字数: 553 千字 2017 年 11 月北京第 1 次印刷

定价: 69.00 元

读者服务热线: (010)81055488 印装质量热线: (010)81055316
反盗版热线: (010)81055315

序

物联网、云计算、大数据、人工智能等新技术的兴起，推动着社会的数字化演进。全球正在从“人人互联”发展至“万物互联”。未来二三十年，人类社会将演变成以“万物感知、万物互联、万物智能”为特征的智能社会。

新兴技术快速渗透并推动企业加速向数字化转型，企业业务应用系统趋于横向贯通，数据趋于融合互联，ICT正在成为企业新一代公共基础设施和创新引擎，成为企业的核心生产力。华为 GIV（全球 ICT 产业愿景）预测，到 2025 年，全球的连接数将达到 1 000 亿，85% 的企业应用云计算技术，100% 的企业会联接云服务，工业智能的普及率将超过 20%。数字化发展为各行业带来的纵深影响远超出想象。

ICT 人才作为企业数字化转型中的关键赋能者，将站在更新的高度，以更为全局的视角审视整个行业，并依靠新思想、新技术驱动行业发展。因此，企业对于融合型 ICT 人才需求也更为迫切。未来 5 年，华为领导的全球 ICT 产业生态系统对人才的需求将超过 80 万。华为积累了 20 余年的 ICT 人才培养经验，对 ICT 行业发展现状及趋势有着深刻的理解。面对数字化转型背景下企业 ICT 人才短缺的情况，华为致力于构建良性 ICT 人才生态链。2013 年，华为开始与高校合作，共同制订 ICT 人才培养计划，设立华为信息与网络技术学院（简称华为 ICT 学院），依据企业对 ICT 人才的新需求，将物联网、云计算、大数据等新技术和最佳实践经验融入到课程与教学中。华为希望通过校企合作，让大学生在校园内就能掌握新技术，并积累实践经验，促使他们快速成长为有应用能力、会复合创新、能动态成长的融合型人才。

教材是知识传递、人才培养的重要载体，华为聚合技术专家、高校教师倾心打造 ICT 学院系列精品教材，希望能帮助大学生快速完成知识积累，奠定坚实的理论基础，助力同学们更好地开启 ICT 职业道路，奔向更美好的未来。

亲爱的同学们，面对新时代对 ICT 人才的呼唤，请抓住历史机遇，拥抱精彩的 ICT 时代，书写未来职业的光荣与梦想吧！华为，将始终与你同行！

前 言

华为 ICT 学院路由与交换技术官方教材分为 3 册，是华为技术有限公司、YESLAB 培训中心和高校专家，针对华为 ICT 学院的学生推出的诚意之作。教材的大纲结构到文字描述由业内专家执笔，内容更由多方顶级专家反复论证推敲。

本书定位的人群为学习过《网络基础》《路由与交换技术》，参加过华为 HCNA 或同等课程的学习，或掌握了一定程度的网络技术知识及华为 VRP 系统的操作使用方法，希望能够在在此基础上继续学习并掌握关于 IPv6、无线、冗余、安全等技术的读者。特别值得一提的是，由于本书的内容主要针对企业网络中的常用技术，因此本书不仅适合有志成为网络工程师的人员，同样适合希望成为系统工程师的人员参阅。

本书第 1 章概述了企业网络的分层设计原则。此后各章则分别介绍了冗余性技术、不同类型的访问控制列表、网络地址转换技术、广域网连接技术、DHCP 协议的原理与（其在 VRP 系统中的）配置方法、IPv6 协议原理与 IPv6 路由技术、AAA 与 IPSec、无线局域网技术和网络管理技术。第 1 章介绍的内容涵盖了目前在企业网络中部署最为广泛的网络技术，学习并掌握这些技术的原理和实施方法是成为网络技术人员的基本条件。

本书自第 2 章开始的各章，除第 7 章（IPv6 基础）和第 8 章（IPv6 路由）之间存在逻辑上的先后关系之外，其余章节均相互独立，不存在先后顺序关系。因此，读者和教师完全可以根据自己的工作、学习和教学需求自由组织顺序。

本书主要内容

本书共分为 11 章，其中第 1 章从总体上介绍企业网络的分层设计模型，其余各章则分别从不同的角度介绍当下企业网络中常用的技术。

第 1 章：企业网概述

本章首先对比传统的办公方式，介绍部署企业网络给企业带来的各种利好。接下来在介绍企业网设计方案时，本章从平面设计方式不利于大规模企业网络通信的角度切入，由此引入企业网的分层设计模型，并且在接下来的内容中详细介绍分层模型中各层的功能，以及适合在各层部署的技术。最后，本章对企业网的未来发展进行简单的展望。

第 2 章：网络可靠性

本章首先对 BFD 的原理进行介绍，这项技术主要着眼于检测通信是否正常。之后

本章介绍两种通过冗余提高网络可靠性的技术：VRRP 和链路聚合。前者旨在为企业网中的终端提供网关的冗余；后者则规避了生成树协议阻塞冗余端口的做法，通过捆绑平行链路的方式让冗余端口参与数据转发，让交换机之间能够通过多条平行链路转发数据。

第 3 章：访问控制列表

本章对访问控制列表技术进行详细介绍。首先对访问控制列表的用途进行介绍，并且由此进一步对路由器通过访问控制列表过滤/匹配流量的逻辑方式，以及访问控制列表的应用方向等概念进行解释说明。之后，本章演示如何在 VRP 系统中创建和应用基本 ACL 与高级 ACL 两类访问控制列表。

第 4 章：网络地址转换

本章会围绕网络地址转换（NAT）技术进行介绍。首先对 NAT 的必要性、路由器执行网络地址转发的操作方法和 NAT 的分类进行一一说明。接下来，本章对几类 NAT 在华为路由设备上的配置方法分别进行演示。

第 5 章：广域网

本章介绍了几种常见的广域网连接技术。首先概述了广域网技术，并且对 HDLC 这个简单连接协议的原理，及其在华为设备上的实施方法进行简单说明。接下来，本章对 PPP 协议的原理、PPP 协议提供的两种认证方式的原理分别进行详细的介绍，并且演示如何在华为路由设备上配置 PPP 协议连接及认证。最后，本章会在 PPP 协议的基础上，对 PPPoE 的原理进行阐述，并且演示 PPPoE 的配置方法。

第 6 章：DHCP 协议

本章对《网络基础》中曾经进行简单介绍的 DHCP 进行详细全面的介绍。首先，我们会从一台（未配置 IP 地址的）终端连接到一个包含 DHCP 服务器的局域网中开始，按照 DHCP 定义的消息类型逐步介绍这套设备如何通过 DHCP 获取、续租 IP 地址及其他相关参数。接下来，我们对 DHCP 服务器不在局域网本地时，由其他设备代理转发 DHCP 消息的工作方式进行介绍。最后，我们分别演示如何将一台华为设备配置为 DHCP 服务器和 DHCP 中继。

第 7 章：IPv6 基础

本章的重点在于 IPv6 协议自身的规范，包括 IPv6 协议提出的背景、IPv6 协议定义的数据包封装格式、IPv6 协议定义的编址方式，以及 IPv6 地址的分类。除了 IPv6 协议之外，本章也对 IPv6 环境中用来完成地址解析和无状态地址自动配置的 NDP 进行了介绍。

第 8 章：IPv6 路由

本章延续第 7 章的内容，继续对 IPv6 的网络环境进行介绍，但本章将重点转移到 IPv6 路由的相关内容。在本章中，IPv6 静态路由、默认路由和汇总路由在 VRP 系统中的配置方式一一都会得到演示。此外，本章还会对 RIPng 和 OSPFv3 两种 IPv6 路由协议的原理和配置方法进行简单说明。

第9章：网络安全技术

本章重点介绍了 AAA 和 IPSec 两种与网络安全相关的技术。AAA 是认证、授权和审计的总称，本章的重点在于介绍被管理设备与 AAA 服务器之间通信时应用的 RADIUS 协议，以及如何通过 VRP 系统配置 AAA 中的认证与授权。IPSec 是一个比较复杂的协议框架，本章会对这个协议框架涉及的内容进行相对深入的理论演绎，并提供 IPSec VPN 的配置案例。最后，本章对用于保障网络安全性的技术进行相对概括的说明。

第10章：WLAN 技术

本章的重点是无线局域网相关技术的说明。本章首先对无线通信的由来、原理与标准进行了简单的介绍说明；接下来将重点转移到了无线局域网当中，并且逐一介绍 WLAN 中的数据帧封装结构，设备通信的过程、安全隐患，以及安全防护措施进行了简单的介绍；最后通过一个（相对复杂的）瘦 AP 无线案例，介绍了无线局域网的实施方法。

第11章：网络管理

本章对网络管理相关的知识进行了说明。我们首先对简单网络管理协议（SNMP）的原理及其各个版本之间的异同进行了介绍，并且对 SNMP 的配置进行了演示；接下来对用于维护网络设备时间准确性的 NTP 进行了原理阐述和实验演示；最后对图形化网络管理平台 e-Sight 的优势进行了简要的说明。

本书配套资源

从理论到实战为高校提供贴合实际应用的定制化教学学习资源。

- 实验手册：教材配套实验材料，助力读者动手能力的提升，以实验促进读者对理论知识的理解。
- 视频讲解：教材配套重点知识讲解小视频，帮助读者更好地理解书中的重点、难点，相关视频可到华为 ICT 学院官方网站进行观看。
- 授课 PPT：教材配套授课材料，方便高校授课，提升教师备课效率。
- 综合实验：教材配套综合练习课程，注重知识间的关联性，提升读者综合运用知识的能力。
- 综合实训：教材配套实训课程，还原真实项目，提升读者应对实际项目的能力。

关于本书读者

本书的定位是华为 ICT 学院路由与交换技术官方教材。本书适合于以下几类读者。

- 华为 ICT 学院的学生。
- 各大高校学生。
- 正在学习 HCNA 课程的学员和正在备考 HCNA 认证的考生。

- 有志于从事 ICT 行业的初学者。
- 网络技术爱好者。

本书阅读说明

读者在阅读本书的过程中，尤其是教师在使用本书作为教材的过程中，需要注意以下事项。

1. 本书多处把路由器或计算机上的网络适配器接口称为“接口”，把交换机上的网口称为“端口”，这种差异仅仅是称谓习惯上的差异。在平时的交流中，“接口”一词与“端口”一词完全可以混用。

2. 在华为公司的作品中，串行链路常用虚线表示，以太网链路而以实线表示。本书中所有链路一概用实线表示，虚线在各图中做特殊表意使用，如数据包前进路线、区域范围等。

3. 本书学习目标中要求读者了解的内容，读者只需了解对应的概念及其表意；本书学习目标中要求读者理解的内容，读者应把握其工作原理，做到既知其然，也知其所以然；本书学习目标中要求读者掌握的内容，读者还应在理解的基础上有能力对其灵活运用。

本书常用图标



本书作者

著：田果、刘丹宁、余建威

编委人员：田果、刘丹宁、余建威、江永红、刘军、韩士良、苏函、刘洋、闫建刚、刘耀林、谢金伟

技术审校：江永红、刘军、谢金伟、韩士良

目 录

第 1 章 企业网概述	0
1.1 分层网络概述	3
1.1.1 企业网与数字办公	3
1.1.2 分层模型概述	5
1.2 企业网体系结构	9
1.2.1 接入层	10
1.2.2 汇聚层	12
1.2.3 核心层	14
1.3 企业网发展趋势	15
1.4 本章总结	19
1.5 练习题	19
第 2 章 网络可靠性	22
2.1 BFD	24
2.1.1 BFD 概述	25
2.1.2 BFD 的工作机制	25
2.1.3 BFD 的报文格式	27
2.2 第一跳冗余协议	30
2.2.1 VRRP 概述	31
2.2.2 VRRP 工作原理	33
2.2.3 VRRP 的配置	38
2.3 链路聚合	49
2.3.1 链路聚合介绍	49
2.3.2 链路聚合的模式	51
2.3.3 链路聚合的配置	54
2.4 本章总结	63
2.5 练习题	63
第 3 章 访问控制列表	66
3.1 IPACL 概述	69

3.2 IPACL 工作原理	70
3.2.1 通配符掩码	71
3.2.2 IPACL 中的匹配顺序	76
3.2.3 入向 IPACL	77
3.2.4 出向 IPACL	79
3.3 基本 IPACL	81
3.3.1 创建基本 IPACL	82
3.3.2 应用基本 IPACL	85
3.4 高级 IPACL	90
3.4.1 创建高级 IPACL	92
3.4.2 应用高级 IPACL	93
3.5 本章总结	97
3.6 练习题	97
第 4 章 网络地址转换	100
4.1 NAT 原理	103
4.1.1 NAT 的作用	103
4.1.2 NAT 的工作原理	105
4.1.3 NAT 的类型	108
4.2 配置 NAT	111
4.2.1 配置基本 NAT	111
4.2.2 配置 NAPT	114
4.2.3 配置 Easy IP	119
4.2.4 配置 NAT 服务器	124
4.3 本章总结	130
4.4 练习题	131
第 5 章 广域网	134
5.1 广域网概述	137
5.2 HDLC 概述	139
5.2.1 HDLC 的封装与消息类型	139
5.2.2 HDLC 的配置演示	141
5.3 PPP	146
5.3.1 PPP 原理	147
5.3.2 PPP 认证	151
5.3.3 PPP 的配置	155
5.4 PPPoE 概述	160

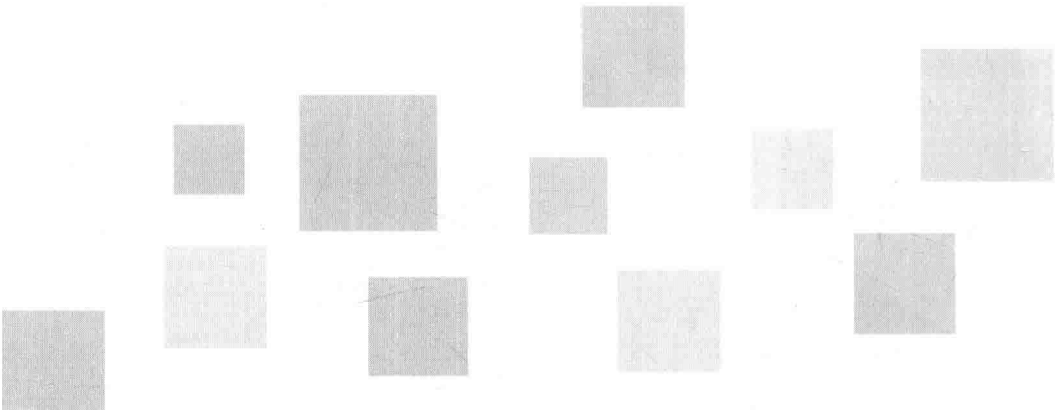
5.4.1 PPPoE 原理概述	160
5.4.2 PPPoE 的配置	164
5.5 本章总结	169
5.6 练习题	169
第 6 章 DHCP 协议	172
6.1 DHCP 原理	175
6.1.1 DHCP 概述	175
6.1.2 DHCP 的工作方式	176
6.1.3 DHCP 的封装格式	186
*6.1.4 DHCP 欺骗攻击概述	188
6.2 DHCP 配置	190
6.2.1 DHCP 服务器的配置	190
6.2.2 DHCP 中继的配置	197
6.3 本章总结	201
6.4 练习题	202
第 7 章 IPv6 基础	204
7.1 IPv6 协议	207
7.1.1 IPv4 的缺陷与 IPv6 的提出	207
7.1.2 IPv6 的数据包封装	209
7.1.3 IPv6 地址的表示方式	212
7.2 IPv6 地址分类	214
7.2.1 IPv6 单播地址	214
7.2.2 IPv6 任意播地址	220
7.2.3 IPv6 组播地址	221
7.3 IPv6 通信建立	223
7.3.1 NDP 协议概述	224
7.3.2 地址解析	227
7.3.3 无状态地址自动配置	230
7.4 本章总结	232
7.5 练习题	233
第 8 章 IPv6 路由	234
8.1 IPv6 静态路由的配置	237
8.1.1 IPv6 静态路由的配置	237
8.1.2 IPv6 默认路由的配置	247

8.1.3 IPv6 汇总路由的配置	250
8.2 RIPng 的配置	251
8.2.1 RIPng 与 RIPv2 的比较	252
8.2.2 RIPng 的配置	254
8.3 OSPFv3 的配置	258
8.3.1 OSPFv3 与 OSPFv2 的比较	258
8.3.2 OSPFv3 的配置	261
8.4 本章总结	269
8.5 练习题	269
第 9 章 网络安全技术	272
9.1 AAA 工作原理	275
9.1.1 AAA 简介	276
9.1.2 RADIUS 协议简介	277
9.1.3 AAA 的配置	281
9.2 IPSec VPN、GRE 原理和配置	291
9.2.1 IPSec 简介	291
9.2.2 IKE 介绍	293
*9.2.3 DH 算法数学背景概述	299
9.2.4 IPSec 的操作方式	300
9.2.5 GRE 概述	308
9.2.6 IPSec VPN 的配置	312
9.3 如何利用网络安全技术保证网络安全性	324
9.3.1 网络安全三要素	324
9.3.2 常见的网络安全问题与解决方法	326
9.4 本章总结	330
9.5 练习题	331
第 10 章 WLAN 技术	332
10.1 无线概念	335
10.1.1 无线射频	335
10.1.2 频段与信道	337
10.1.3 标准化组织介绍	339
10.2 WLAN 运行	340
10.2.1 802.11 标准的帧结构	340
10.2.2 无线局域网工作原理	344
10.3 无线 LAN 的安全性	353

10.3.1 无线 LAN 的隐患	354
10.3.2 保护无线 LAN 通信	355
10.4 无线 LAN 的配置	359
10.5 本章总结	367
10.6 练习题	368
第 11 章 网络管理	370
11.1 SNMP 协议	373
11.1.1 SNMP 协议概述	373
11.1.2 SNMP 版本对比	378
11.1.3 SNMP 的配置	381
11.2 NTP 协议	387
11.2.1 NTP 协议的原理	387
11.2.2 NTP 协议的配置	390
11.3 eSight 的基础知识	395
11.4 本章总结	399
11.5 练习题	400
术语表	402

The top half of the page features a decorative pattern of grey squares of varying sizes arranged in a grid-like fashion. Below this, a large, light grey geometric shape, resembling a stylized roof or a large 'V' shape, dominates the middle section. The text is positioned within this shape.

第1章 企业网概述



随着时代的发展，数字办公已经不再是一种时尚的办公方式，而日渐成为各行各业办公的标配。为了提升办公效率，改善办公环境，优化人际合作，降低通信成本，自 20 世纪 90 年代开始，各类企业纷纷搭建起了自己的办公网络，并且将它们接入了互联网。

当然，企业网并不是一种网络技术的代称，这个概念也没有十分严格的界定。实际上，任何企事业单位搭建起来用以共享内部信息资源的计算机网络都可以粗略地划分到企业网的范畴。所以，在这一章中，我们主要谈论的并不是网络的技术层面，而更侧重于介绍网络架构。

在 1.1 节中，我们会首先带领读者思考企业网给办公带来的效率提升都体现在了哪些方面，因为了解企业网相比于传统办公环境的优势有助于读者在现实工作中进一步对接用户的实际使用需求。

1.2 节是本章的重点，在 1.2 节中，我们会对在设计当中最为常见的三层企业网模型逐层进行介绍。我们不仅会解释按照分层模型规划企业网的好处，同时也会介绍各层在企业网中应该承担的作用，以及工程师应该在各层中部署哪些网络技术。

1.3 节会浅谈一些正在企业网中迅猛发展的新兴技术和趋势。在本书的读者走向企业之时，这些新兴技术应该已经发展得十分成熟。本书抛砖引玉，意在提醒读者在校期间不妨留意这些技术的发展动态。本书是华为 ICT 学院路由交换技术系列教材的最后一册，我们也推荐读者在完成这部分的学习之后，能够继续通过各种渠道深入学习这些新兴技术。这既可以帮助那些希望毕业后立刻进入职场的读者在择业和就业时占据更加有利的位置，又可以帮助那些渴望继续深造的读者提前了解自己在攻读更高一级学位时，对研究哪些课题更感兴趣，研究哪些课题更有可能获得更加宽广的发展空间。

学习目标

- 了解企业网的三层模型；
- 理解应该按照三层模型规划企业网的原因；
- 掌握企业网三层模型中各层的作用；
- 了解在部署企业网时，应该将哪些技术部署在企业网的哪一层中；
- 了解企业网的新兴需求及发展趋势。

1.1 分层网络概述

实际上，企业网络的设计并不能一概而论，先不说企业的规模，就是不同行业中的企业，也有各自不同的需求，比如：金融行业可能更多注重网络的可靠性和安全性；医疗行业可能需要满足多种医疗设备的联网需求；交通行业可能需要应对旺季突发的巨大流量和由此带来的服务器负载；石油和天然气行业由于地理环境复杂可能更需要结合多种通信方式（铺设海缆、架设微波系统等）；电力系统可能会更多关注冗余性的考量；零售行业可能更需要实现对所有门店及库存信息的统一管理和调度；酒店行业可能会更多地面临宾客自带设备的病毒传播问题。

虽然各行各业不同规模的企业对于自己的网络会提出各种各样的需求，但网络架构仍有共同之处。本节将会介绍企业网设计中最基本的指导原则，管理员只有掌握了这种原则，才能根据自己企业的特点和需求进行合理规划。

1.1.1 企业网与数字办公

时下，各行各业、不同规模的企业都已经在不同程度上实现了办公网络化，完全不借助网络进行办公的企业已经少之又少。然而，这一切的发生似乎并没有经历太长的过渡阶段。很多当前仍然在职的50后、60后、70后一代都曾经历过依靠纸、笔、算盘/计算器办公的时代，并且有幸见证了企业办公信息化、网络化的过程。在羡慕前辈们丰富经历的同时，我们建议本书的读者虚心向他们请教一个问题：企业网络化到底给企业和办公方式带来了哪些变化？因为企业办公网络化的驱动力，势必与企业网对服务提出的需求相关，而企业网的需求又会进一步与网络的解决方案和新兴的技术发展趋势相关，最终与每一位读者在未来工作中将要面临的问题相关。

我们在这里不奢望对企业网带来的变化进行全面总结，仅抛砖引玉，提出网络化办公与传统方式相比的几点优势。

- **信息交互方面：**从电子邮件被应用到办公环境中开始，网络技术就已经给企业