

凭八年执教思科，铸一剑心血融合；避外版错漏波折，开国人亲耕先河

CCNA

学习宝典

(考试号640-802)

◎ 张国清 编著 ◎

<http://www.phei.com.cn>

NETWORKS



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

CCNA 学习宝典

(考试号 640-802)

张国清 编著

电子工业出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 简 介

本书由资深 Cisco 技术讲师根据多年的教学心得编写, 针对 CCNA 课程中的重点、难点和认证考试内容, 进行了详细的讲解。主要内容包括: 网络基础知识; OSI 参考模型; TCP/IP 协议栈; 路由原理基础; 路由协议工作原理及配置方法 (RIP, RIPv2, IGRP, EIGRP 和 OSPF); Cisco 路由器的基本配置; 访问控制列表; 以太网和 WLAN; 以太网交换原理和交换机的配置; 广域网技术和广域网接入技术 (PPP、帧中继和 IPsec VPN 等)。

未经许可, 不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有, 侵权必究。

图书在版编目 (CIP) 数据

CCNA 学习宝典: 考试号 640-802/ 张国清编著. —北京: 电子工业出版社, 2008.6
ISBN 978 7-121-06434-0

I. C… II. 张… III. 计算机网络—工程技术人员—资格考核—自学参考资料 IV. TP393

中国版本图书馆 CIP 数据核字 (2008) 第 056391 号

责任编辑: 宋 梅

印 刷: 北京市通州大中印刷厂

装 订: 三河市鹏成印业有限公司

出版发行: 电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本: 787×1092 1/16 印张: 27.25 字数: 697 千字

印 次: 2008 年 6 月第 1 次印刷

印 数: 4 000 册 定价: 58.00 元

凡所购买电子工业出版社图书有缺损问题, 请向购买书店调换。若书店售缺, 请与本社发行部联系, 联系及邮购电话: (010) 88254888。

质量投诉请发邮件至 zlt@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线: (010) 88258888。

前 言

多年来, CCNA 在 IT 界非常知名, 该认证是世界著名的互联网设备及方案提供商——思科公司推出的系列职业认证之一。思科公司开发的通用职业认证系列包括 CCNA (Cisco Certified Network Associate), CCNP (Cisco Certified Network Professional) 和 CCIE (Cisco Certified Internetwork Expert)。除了通用职业认证之外, 还有若干专业技术认证。CCNA 是通用职业认证和专业技术认证的基础, 因此, 广泛受到从事网络技术的人员及大中专学生的青睐。

2007 年 8 月, 思科公司对 CCNA 要求的知识和技能进行了升级, 删去了相对过时的 ISDN 技术, 并增加了一些新技术——WLAN 技术、VPN 技术和 IPv6 技术。因此, 从整体上提升了获取 CCNA 认证的难度, 同时也增加了 CCNA 证书的含金量。本书对 CCNA 涉及的难点进行了深入剖析, 详细讲解了要点和重点知识, 在 CCNA 要求的知识层面上使读者对相关理论和技术有一个比较深刻而全面的理解, 并为读者进一步学习打下良好的基础。

本书弥补了原版教材中的不足。作者力求把理论和实践结合起来, 让读者不仅能掌握理论知识, 还能掌握如何配置设备, 实现相应功能, 提高读者的实际操作能力。

本书适合以下人员阅读:

- 自学 CCNA 者;
- 参加 CCNA 培训者;
- 准备获取 CCNA 认证证书者;
- 工程技术人员。

另外, 本书也非常适合作为以提高专业技术人员职业技能为目的的培训教材。

全书共 14 章。

第 1 章 网络通信基础知识: 介绍了计算机基础知识和网络基础知识。本章内容是学习网络技术的入门知识。

第 2 章 开放系统互连: 讲述了 OSI 参考模型理论。

第 3 章 TCP/IP 协议栈: 详细讲解了 IP 地址、子网划分、VLSM、ARP 和 ICMP 协议等。

第 4 章 初识路由器: 讲述路由器的软 / 硬件构成和命令行操作界面。

第 5 章 路由原理基础: 介绍了路由原理, 以及距离矢量型路由协议和链路状态型路由协议的工作原理和特性。

第 6 章 配置静态和动态路由: 介绍了如何在路由器上配置 RIPv1、RIPv2 和 IGRP 协议及静态路由。

第 7 章 访问控制列表: 介绍了在路由器上实现数据和网络安全的技术——ACL。

第 8 章 OSPF 路由协议: 介绍了 OSPF 路由协议原理及配置。

第 9 章 EIGRP 原理及配置: 介绍了 EIGRP 协议的原理及配置。

第 10 章 以太网技术: 介绍了以太网原理及 WLAN 技术。

第 11 章 以太网交换技术: 介绍了以太网交换原理和以太网交换机的配置方法。

第 12 章 管理交换机: 介绍 Catalyst 系列交换机及配置交换机的命令和步骤。

第 13 章 广域网及其接入技术: 介绍广域网的概念和广域网接入技术。

第14章 IPv6 概述：介绍 IPv6 地址、ICMPv6、实现 IPv6 的方案和 IPv6 路由协议等。

本书覆盖了 CCNA (640-802) 考试的全部内容，建议读者按照顺序阅读。但每一章又具有相对的独立性，因此，读者也可以根据自己的实际情况有针对性地阅读特定章节。

电子工业出版社的宋梅女士为本书的出版做了大量工作，在此表示感谢！作者在编著本书时得到了好友栗君的大力帮助，在此表示感谢！

鉴于作者水平有限，书中难免出现错误和纰漏之处，欢迎读者批评指正，作者不胜感激 (tsing@btamail.net.cn)。

编者

2007年12月于北京

目 录

第 1 章 网络通信基础知识	(1)
1.1 网络中的数学——数制	(1)
1.1.1 十进制	(1)
1.1.2 二进制	(2)
1.1.3 十六进制	(2)
1.2 组网基础	(2)
1.2.1 常用术语	(2)
1.2.2 带宽	(4)
1.3 本章小结	(5)
附录 A 思考与练习	(6)
第 2 章 开放系统互连	(7)
2.1 ISO 与 OSI	(7)
2.2 OSI 参考模型	(8)
2.2.1 物理层	(9)
2.2.2 数据链路层	(10)
2.2.3 网络层	(12)
2.2.4 OSI 的其他层	(12)
2.3 数据封装与 OSI 参考模型	(13)
2.4 对等层通信原则	(14)
2.5 本章小结	(15)
附录 A 思考与练习	(16)
第 3 章 TCP/IP 协议栈	(17)
3.1 TCP/IP 的诞生	(17)
3.2 TCP/IP 的分层结构	(17)
3.2.1 网络接口层	(18)
3.2.2 互联网层	(18)
3.2.3 传输层	(19)
3.2.4 应用层	(19)
3.3 互联网协议——IP	(19)
3.3.1 IP 数据包格式	(19)
3.3.2 IPv4 地址	(21)
3.3.3 子网划分	(23)
3.3.4 变长子网掩码技术	(27)

3.4	地址解析协议	(29)
3.4.1	子网内的 ARP	(29)
3.4.2	子网外的 ARP	(31)
3.5	ICMP 协议	(32)
3.6	传输层协议	(33)
3.6.1	TCP 协议	(34)
3.6.2	UDP 协议	(37)
3.7	应用层协议	(37)
3.8	本章小结	(38)
附录 A	思考与练习	(40)
第 4 章	初识路由器	(42)
4.1	路由器的主要硬件	(42)
4.2	路由器的操作系统	(44)
4.3	路由器基本操作	(44)
4.3.1	启动过程	(45)
4.3.2	配置模式	(47)
4.3.3	路由器的基本维护指令	(48)
4.3.4	寄存器与加载 IOS	(66)
4.4	本章小结	(68)
附录 A	思考与练习	(69)
附录 B	实验 1: 设置超级终端	(70)
附录 C	实验 2: 练习常用命令	(75)
附录 D	实验 3: 设置 Telnet	(82)
附录 E	实验 4: 备份 IOS	(84)
附录 F	实验 5: 密码恢复	(86)
第 5 章	路由原理基础	(88)
5.1	路由概念	(88)
5.1.1	静态路由	(90)
5.1.2	动态路由	(90)
5.1.3	自治系统	(91)
5.1.4	路由协议	(92)
5.1.5	路由协议分类	(92)
5.1.6	路由度量	(93)
5.1.7	管理距离	(96)
5.2	路由算法	(96)
5.2.1	距离矢量型路由协议算法	(96)

5.2.2	路由环路的形成	(99)
5.2.3	避免环路的技术	(100)
5.2.4	链路状态型路由协议算法	(103)
5.3	本章小结	(105)
附录 A	思考与练习	(107)
第 6 章	配置静态和动态路由	(108)
6.1	静态路由	(108)
6.1.1	配置静态路由	(108)
6.1.2	配置默认路由	(109)
6.2	RIPv1 协议	(110)
6.2.1	配置 RIPv1 协议	(110)
6.2.2	检查协议运行状态	(111)
6.2.3	选择性通告路由	(117)
6.3	IGRP 协议	(119)
6.3.1	度量值的计算公式	(119)
6.3.2	配置 IGRP 路由协议	(120)
6.3.3	检查 IGRP 的运行	(121)
6.4	有类和无类路由协议	(124)
6.4.1	有类路由协议	(124)
6.4.2	无类路由协议	(126)
6.5	RIPv2	(127)
6.5.1	配置 RIPv2	(127)
6.5.2	RIPv2 的路由归纳	(129)
6.5.3	RIPv2 的验证	(130)
6.6	本章小结	(132)
附录 A	思考与练习	(133)
附录 B	实验 1: 配置静态路由	(135)
附录 C	实验 2: 配置 RIPv1	(138)
附录 D	实验 3: 配置 IGRP 协议	(142)
附录 E	实验 4: 配置 RIPv2	(145)
附录 F	实验 5: 验证 ip classless 功能	(149)
第 7 章	访问控制列表	(151)
7.1	ACL 概述	(151)
7.2	执行 ACL 的过程	(152)
7.3	ACL 类型和通配符掩码	(153)
7.3.1	ACL 的类型	(153)

7.3.2	通配符掩码	(154)
7.4	配置 ACL	(156)
7.4.1	配置标准 ACL	(156)
7.4.2	配置扩展 ACL	(159)
7.4.3	命名的 ACL	(163)
7.4.4	控制 Telnet	(164)
7.4.5	基于时间的 ACL	(165)
7.4.6	动态 ACL	(165)
7.4.7	反射 ACL	(166)
7.5	ACL 的使用规则	(170)
7.6	管理 ACL 的命令	(172)
7.7	本章小结	(172)
附录 A	思考与练习	(174)
附录 B	实验 1: 配置标准访问列表	(176)
附录 C	实验 2: 配置扩展访问列表	(179)
附录 D	实验 3: 控制单向 Ping 测试	(181)
附录 E	实验 4: 禁止远程控制路由器	(183)
附录 F	实验 5: 禁止通过虚拟终端控制路由器	(185)
第 8 章	OSPF 路由协议	(187)
8.1	OSPF 概述	(187)
8.2	OSPF 术语	(187)
8.3	OSPF 与广播型链路	(190)
8.3.1	Hello 包	(190)
8.3.2	选举 DR 和 BDR	(192)
8.3.3	路由发现过程	(193)
8.3.4	再次同步拓扑库	(194)
8.4	OSPF 与点到点链路	(196)
8.5	在以太网上启用 OSPF	(196)
8.5.1	启动 OSPF 进程	(196)
8.5.2	常用管理命令	(197)
8.5.3	使用自定义参数	(212)
8.5.4	默认路由	(214)
8.5.5	OSPF 的认证	(216)
8.6	在点到点链路上启用 OSPF	(219)
8.7	本章小结	(221)
附录 A	思考与练习	(222)
附录 B	实验 1: 配置 OSPF 协议	(224)

第 9 章 EIGRP 原理及配置	(230)
9.1 EIGRP 特性概述	(230)
9.2 EIGRP 和 IGRP 的关系	(230)
9.3 EIGRP 的数据包	(231)
9.4 EIGRP 运行原理	(231)
9.5 EIGRP 的路由算法	(232)
9.5.1 术语	(232)
9.5.2 DUAL 的运行步骤	(233)
9.6 配置 EIGRP	(237)
9.7 管理 EIGRP	(238)
9.8 路由归纳	(244)
9.8.1 自动归纳	(244)
9.8.2 手工归纳	(247)
9.8.3 注意事项	(247)
9.9 负载均衡	(250)
9.10 本章小结	(251)
附录 A 思考与练习	(252)
附录 B 实验 1: 配置 EIGRP 协议	(254)
第 10 章 以太网技术	(258)
10.1 以太网规范	(258)
10.1.1 DIX 规范	(258)
10.1.2 IEEE 802.3 规范	(259)
10.1.3 二者与 OSI	(259)
10.2 工作原理	(260)
10.2.1 工作机制	(260)
10.2.2 碰撞检测	(263)
10.2.3 碰撞域	(264)
10.2.4 迟冲突	(265)
10.3 以太网数据帧	(266)
10.3.1 以太帧结构	(266)
10.3.2 最小帧的定义	(268)
10.4 千兆位以太网	(269)
10.4.1 载波扩展帧	(269)
10.4.2 千兆位家族成员	(270)
10.5 集线器	(271)
10.6 自动协商	(272)

10.7	WLAN 技术	(273)
10.7.1	WLAN 标准	(274)
10.7.2	WLAN 工作模式	(274)
10.7.3	WLAN 的安全性	(276)
10.7.4	Cisco 无线安全套件	(278)
10.7.5	AP 基本配置	(279)
10.8	本章小结	(282)
附录 A	思考与练习	(283)
第 11 章	以太网交换技术	(284)
11.1	交换技术的提出	(284)
11.2	构建 MAC 地址表	(286)
11.3	生成树协议	(287)
11.3.1	桥接环路	(287)
11.3.2	广播风暴的形成	(288)
11.3.3	MAC 地址表不稳定	(289)
11.3.4	IEEE 802.1D 生成树	(289)
11.3.5	IEEE 802.1W 生成树	(293)
11.3.6	生成树运行方式	(297)
11.4	虚拟局域网技术	(297)
11.4.1	VLAN 概述	(298)
11.4.2	VLAN 类型	(298)
11.4.3	VLAN 标签	(298)
11.5	VTP	(300)
11.5.1	交换机的 VTP 身份	(300)
11.5.2	VTP 运行原理	(301)
11.6	跨 VLAN 的通信方法	(301)
11.6.1	外接路由器方法	(302)
11.6.2	使用 3 层交换机	(302)
11.7	本章小结	(303)
附录 A	思考与练习	(304)
第 12 章	管理交换机	(306)
12.1	思科 Catalyst 系列交换机简介	(306)
12.1.1	Catalyst 6500 系列	(306)
12.1.2	Catalyst 4500 系列	(306)
12.1.3	Catalyst 4900 系列	(307)
12.1.4	Catalyst 3750/3750E 系列	(307)

12.1.5	Catalyst 3560/3560E 系列	(308)
12.1.6	Catalyst 3550 系列	(308)
12.1.7	Catalyst 2960 系列	(309)
12.1.8	Catalyst 2950 系列	(309)
12.1.9	Catalyst 2940 系列	(310)
12.1.10	Catalyst 2900XL 系列	(310)
12.1.11	Catalyst 3500XL 系列	(311)
12.2	管理交换机的基本命令	(311)
12.3	管理生成树的基本命令	(315)
12.3.1	Catalyst 2900XL/3500XL 使用的命令	(316)
12.3.2	Catalyst 2950/2960/3550 使用的命令	(317)
12.4	管理 VLAN 的基本命令	(322)
12.4.1	添加普通区域 VLAN	(322)
12.4.2	添加扩展区域 VLAN	(323)
12.4.3	为 VLAN 分配端口	(324)
12.4.4	管理 Trunk	(324)
12.5	管理 VTP	(326)
12.5.1	设置 VTP 参数	(326)
12.5.2	交换机加入 VTP 域	(327)
12.6	跨 VLAN 通信	(328)
12.6.1	外接路由器方式	(329)
12.6.2	3 层交换机方式	(330)
12.7	本章小结	(331)
附录 A	思考与练习	(332)
附录 B	实验 1: IEEE 802.1D STP	(334)
附录 C	实验 2: MST	(339)
附录 D	实验 3: VLAN 及 VTP	(344)
附录 E	实验 4: 跨 VLAN 通信	(349)
第 13 章	广域网及其接入技术	(351)
13.1	广域网技术概述	(351)
13.1.1	线路类型	(351)
13.1.2	广域网接入技术	(352)
13.1.3	Internet 模型及术语	(353)
13.2	点到点链路	(354)
13.2.1	DTE/DEC	(354)
13.2.2	HDLC	(355)
13.3	PPP	(356)

13.3.1	PPP 的分层结构	(356)
13.3.2	PPP 的帧格式	(357)
13.3.3	PPP 建立链路的过程	(358)
13.3.4	PPP 认证	(358)
13.4	帧中继	(365)
13.4.1	运行原理	(365)
13.4.2	术语	(366)
13.4.3	帧中继的地址映射	(366)
13.4.4	子接口	(367)
13.4.5	帧中继的配置	(369)
13.5	DHCP	(374)
13.5.1	DHCP 工作过程	(375)
13.5.2	DHCP 中继	(376)
13.5.3	配置 DHCP	(377)
13.6	地址翻译技术	(378)
13.6.1	NAT 术语定义	(378)
13.6.2	配置 NAT	(379)
13.6.3	DHCP/NAT 案例	(383)
13.7	VPN 技术概览	(385)
13.7.1	VPN 类型	(385)
13.7.2	隧道	(386)
13.8	密码学基础	(388)
13.9	IPsec VPN	(390)
13.9.1	IPsec 主要部件	(390)
13.9.2	IPsec 的模式	(390)
13.9.3	安全联盟	(392)
13.9.4	Internet 密钥交换	(392)
13.9.5	配置 IPsec VPN	(393)
13.9.6	IPsec VPN 示例	(394)
13.10	SSL VPN	(397)
13.11	本章小结	(398)
	附录 A 思考与练习	(400)
	附录 B 实验 1: NAT	(401)
第 14 章	IPv6 概述	(403)
14.1	IPv6 地址	(403)
14.2	IPv6 地址前缀	(404)
14.3	IPv6 地址类型	(404)

14.4 IPv6 包头	(409)
14.5 ICMPv6	(410)
14.6 邻居发现协议.....	(411)
14.7 移动 IPv6 地址	(413)
14.7.1 移动 IPv6 的构成部件	(413)
14.7.2 移动 IPv6 的工作过程	(413)
14.8 实现 IPv6 的方案	(414)
14.9 IPv6 路由协议	(415)
14.10 本章小结	(416)
附录 A 思考与练习	(418)
思考与练习答案	(419)
参考文献	(421)

第1章 网络通信基础知识

今天的互联网（Internet）是一种很有价值的资源，对各行业来说，接入互联网都是非常重要的。可以从以下3个层面上理解什么是接入互联网。

物理接入：指通过计算机上的网卡及其他网络设备把计算机连接到互联网上。这条物理的通路用来传输本地计算机和远端计算机通信的信号。

逻辑接入：指本地计算机使用某种协议，通过互联网与远端的计算机进行通信。协议是一套标准的规则和约定，用来控制网络上的设备如何进行通信。虽然许多协议都可以把计算机接入互联网，但TCP/IP协议是今天主要使用的协议。

应用接入：指应用程序与协议一起工作，通过互联网收发数据。应用程序可以翻译和显示计算机间传送的数据，使用户能够读懂传送的内容。例如，Web浏览器可以翻译和显示用超文本标记语言（HTML）制作的网页。Web浏览器也使用特殊的插件（Plug-in）程序显示特殊类型的数据，如电影或Flash动画。

无论从哪个层面上理解，其目的是要把计算机接入到互联网中，与远端的计算机进行通信。所以计算机是构成互联网的最基本的元素。

1.1 网络中的数学——数制

数制由一组符号及使用这些符号的规则构成，使用这些符号及规则可以表达数。在日常生活中人们最熟悉的数制是十进制（Decimal）。在计算机和网络通信技术中，常用的数制是二进制（Binary）和十六进制（Hexadecimal）。

1.1.1 十进制

十进制是人们最熟悉的数制。在十进制计数系统中，使用0, 1, 2, 3, 4, 5, 6, 7, 8, 9十个符号来表达数，计数的规则是逢十进一。使用这10个符号的组合可以表达任意数。

十进制数是基于10的 n 次方计算数值的，也就是说，任何一个十进制数都可以用这10个符号乘以 10^n 来表达。这里的10称为基数， n 称为指数， n 的取值取决于符号在数中的位置，个位数取0，即 10^0 ；十位数取1，即 10^1 ；百位数取2，即 10^2 ；依次类推。

例如，可以把数字8376表达为： $8 \times 10^3 + 3 \times 10^2 + 7 \times 10^1 + 6 \times 10^0$

可以看出，数字中从右到左中的第一位取0作为指数；第二位取1作为指数；第三位取2作为指数；第四位取3作为指数。根据这个规律，如果数字非常大，只需要数一下数字有多少位就知道应该如何取指数了。

1.1.2 二进制

计算机及其他通信设备是由电子电路构成的, 电路的状态只有两种, 即开和关。计算机也只能识别和使用电路的这两种状态计算和存储数据。用符号 1 表示电路的开状态; 用符号 0 表示电路的关状态, 这对计算机来说是很自然的事情。

用 0 和 1 两个符号来表达数的计数系统称为二进制, 其计数规则是逢二进一。

二进制的基数是 2, 把二进制数转换成十进制数的方法是: 把处于不同位置上的二进制数符乘以 2^n , 然后把它们相加。 n 的取值取决于符号在数中的位置。

例如, 把二进制数 10110 (1101_2) 转换成十进制数:

$$1101_2 = 1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 = 13$$

1.1.3 十六进制

在十六进制计数系统中, 使用 16 个符号来表达数, 这 16 个符号是: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, 计数的规则是逢十六进一。

十六进制的基数是 16, 把十六进制数转换成十进制数的方法是: 把处于不同位置上的十六进制数符乘以 16^n , 然后把它们相加。 n 的取值取决于符号所处的位置。

例如, 把十六进制数 1A39 转换为十进制数:

$$1A39 = 1 \times 16^3 + 10 \times 16^2 + 3 \times 16^1 + 9 \times 16^0 = 6713$$

与二进制相比, 十六进制的表达形式更容易书写和阅读, 因此, 人们更喜欢用十六进制数表示二进制数。把二进制数转换为十六进制数的工作相当简单, 因为 4 位二进制数刚好等于 1 位十六进制数, 所以, 只需要把二进制数从最右端开始, 每 4 位转变成 1 位十六进制数即可, 不足 4 位的, 在最左边补 0。

例如, 把二进制数 10101011110101110 转换为十六进制数, 步骤如下:

第一步, 从右至左, 每 4 位分成一组, 最后不足 4 位的补 0

0001 1010 0111 1010 1110

第二步, 把每组二进制数转换成十六进制数

1 A 7 A E

如果把十六进制数转换为二进制数, 只需要把每位十六进制数直接转换成 4 位二进制数即可。

例如, 把 0x2A87 转换为二进制数 (0x 表示是十六进制数):

$$0x2A87 = 0010 \ 1010 \ 1000 \ 0111 = 10 \ 1010 \ 1000 \ 0111$$

1.2 组网基础

1.2.1 常用术语

(1) 局域网 (Local Area Network, LAN)

LAN 指覆盖地域面积较小, 负责网络内计算机通信的网络。例如, 一个公司或工厂的网

络。常用的 LAN 技术规范有以太网 (Ethernet)、令牌环 (Token Ring) 和光纤分布式数据接口 (FDDI)。

(2) 广域网 (Wide Area Network, WAN)

WAN 指覆盖地域面积大, 例如, 覆盖全球, 用于连接局域网并保证局域网之间通信的网络。广域网能够为不同地理位置上的用户提供实时通信的能力; 提供不间断访问远程资源的能力; 提供 E-mail 服务、WWW 服务和文件传送等其他服务。常用的广域网技术有 ISDN, DSL, Frame Relay, T1, E1, T3, E3, SONET 和 SDH 等。

(3) 城域网 (Metropolitan Area Network, MAN)

MAN 指覆盖一个城市及其郊区地域范围的网络。城域网通常由一两个局域网通过专线互连构成, 例如, 银行各网点之间互连。

(4) 存储区域网络 (Storage Area Network, SAN)

SAN 是一种专用的、高性能的网络体系, 负责在服务器和资源存储区之间快速传递数据。这种网络的特点是读写数据快、数据高度可靠和易于扩展网络。

(5) 虚拟私有网络 (Virtual Private Network, VPN)

VPN 是在公众互联网上, 如在 Internet 上, 利用某种技术为客户建立起来的专供客户使用的逻辑的专用链路, 把用户位于不同地理位置上的局域网连接起来, 为用户提供高度可靠和安全的通信。VPN 类似于跨越广域网的局域网。构建 VPN 的技术有隧道技术 (如 IPsec) 和标签技术 (MPLS)。

(6) 客户机 / 服务器计算模式

这是一种计算模式, 该计算模式把处理能力分布在多台计算机上进行, 客户机和服务器共同承担处理数据的责任 (如图 1-1 所示)。

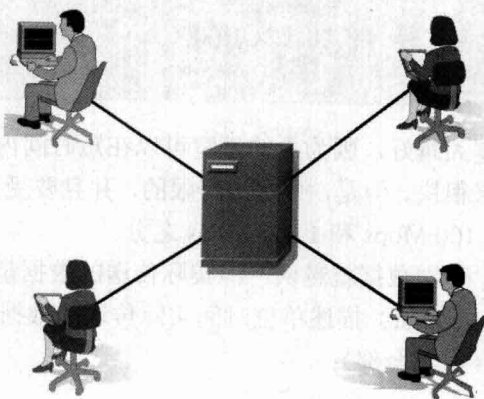


图 1-1 客户机 / 服务器模式

互联网就是一个分布式处理的客户机 / 服务器计算模式。客户机 (前端) 处理用户的表达工作, 如屏幕的显示格式、输入格式和数据编辑等; 而服务器 (后端) 执行数据的计算和查询等工作。浏览网页就是这种分布计算模型。用户的计算机就是客户机身份, 在用户的计算机上安装有 Web 浏览器, 用来向 Web 服务器发送请求, 当服务器收到请求后就会把客户机请求的数据发送过来, Web 浏览器收到来自服务器的响应后, 把收到的 HTTP 数据显示在屏幕上。服务器承担了大量的处理工作, 而客户机则承担了很小一部分处理工作。其他客户