

VPN

网络组建案例实录

技术要点:

- ✿ 基本VPN服务器的组建
- ✿ 企事业单位VPN网络的组建
- ✿ 具有多出口的校园VPN网络的组建
- ✿ 使用智能卡组建VPN网络
- ✿ 某市政府VPN网络解决方案
- ✿ 证书服务
- ✿ 路由和远程访问服务
- ✿ ISA Server 2006代理服务器与防火墙
- ✿ 常见问题的解决方法
- ✿ 实验环境的搭建

集作者多年网络工程经验,提供实施VPN网络的完整解决方案

5个大型VPN网络案例,全部来自一线工程实践,极具实用价值



TP393.01/15

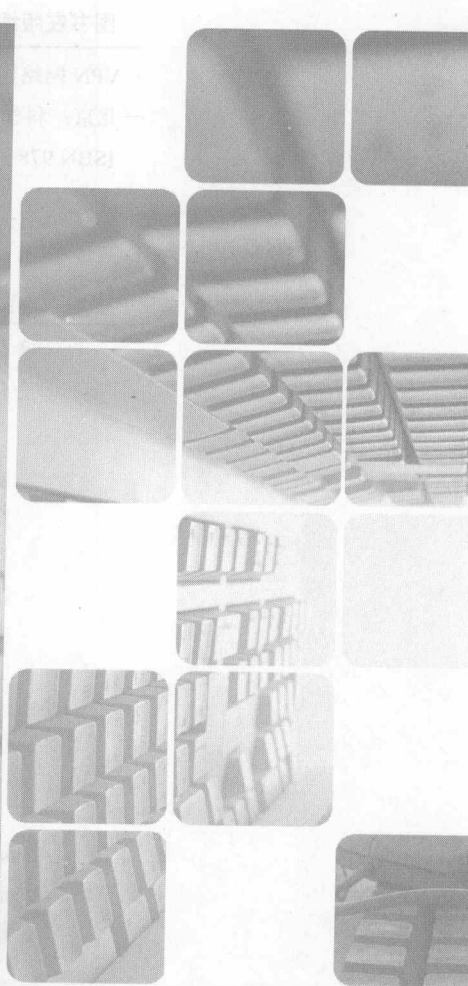
2008

VPN

网络组建案例实录

王春海 张晓莉 田浩 编著

 科学出版社



内 容 简 介

本书通过实际工程案例,介绍了使用 Windows Server 2003、ISA Server 2006 组建“软件”VPN 服务器与 VPN 网络的解决方案。

全书技术先进,所介绍的案例都是实际 VPN 网络的完整方案,并且都经过实际工作环境的检验,具有较高的实用价值。全书主要分三部分,第一部分(第1章~第6章)是实际 VPN 案例的真实记录,旨在让读者快速掌握 VPN 网络的组建,提高动手能力,增加 VPN 组网经验;第二部分(第7章~第9章)主要介绍 VPN 网络的理论知识,包括证书服务、Windows Server 2003 路由和远程访问服务及 ISA Server 2006 代理服务器和防火墙;第三部分(第10章及附录)主要介绍 VPN 网络中常见问题的解决方法及本书试验环境的搭建。

本书适合网络工程技术人员、网络技术爱好者、网络管理员和维护人员阅读,也很适合作为网络技术培训机构的教学用书。

图书在版编目(CIP)数据

VPN 网络组建案例实录/王春海, 张晓莉, 田浩编著.

—北京: 科学出版社, 2008

ISBN 978-7-03-021793-6

I. V… II. ①王… ②张… ③田… III. 虚拟网络—基本知识

IV. TP393.01

中国版本图书馆 CIP 数据核字(2008)第 060455 号

责任编辑: 何立兵 / 责任校对: 李玉茹

责任印刷: 科海 / 封面设计: 王嵩

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>

北京市鑫山源印刷有限公司

科学出版社发行 各地新华书店经销

*

2008 年 7 月 第 一 版

开本: 16 开

2008 年 7 月第一次印刷

印张: 23.25

印数: 000 1-4 000

字数: 565 千字

定价: 45.00 元

(如有印装质量问题, 我社负责调换)

前言

全书通过5个实际工程案例，详尽地讲解了使用Windows Server 2003与ISA Server 2006组建安全VPN网络的具体方法，所提供的案例都是来自笔者亲自参与的实际工程，并经过实际工作环境的检验，具有较高的实用价值，读者完全可以将这些案例应用于自己的组网工程中。

与传统的硬件VPN组网方案相比，随着PC服务器硬件性能的不提高与成本的不断下降，软件VPN服务器在成本、性能、可靠性、安全性、可扩展性等方面已体现出无可比拟的优势。因此软件VPN服务器成为了VPN网络解决方案的首选。本书只介绍软件VPN组网方案。

本书内容

本书共分3部分，各部分内容安排如下：

第一部分（第1章~第6章）：实际工程案例的真实记录，包括：组建基本的VPN服务器、企事业单位VPN网络的组建、具有多出口的校园VPN网络的组建、使用智能卡验证的VPN网络的组建、某市政府VPN网络解决方案。

第二部分（第7章~第9章）：介绍VPN网络的理论知识，包括：证书服务、Windows Server 2003路由和远程访问服务、ISA Server 2006代理服务器与防火墙。

第三部分（第10章、附录A、附录B）：介绍Windows Server 2003 VPN网络中常见问题的解决方法、VMware Workstation 6.0的使用以及本书中试验环境的搭建。

本书案例

本书主要介绍了适合以下三种应用环境的VPN案例。

- 中小企业单VPN服务器解决方案：基本VPN服务器的组建，适合预算较小、维护与使用经费有限的中小企业或者中小学，使用一台Windows Server 2003服务器，通过Internet

为不超过1000个用户、最大并发300~500个用户的网络提供VPN接入服务。

- 大中专院校、中型企业VPN解决方案：单台或者两台服务器（一台低配置的证书服务器、一台VPN服务器），适合对安全性要求比较高、有一定经费的企业，通过Internet为出差用户、家庭办公用户、远程分公司或办事处，提供到公司总部指定网络的、安全的VPN接入服务。在访问时，使用“证书”进行身份验证与数据加密。
- 政府、机关与事业单位、大学VPN解决方案：多台服务器（一台证书服务器、一台Active Directory服务器、至少一台使用ISA Server标准版或企业版的VPN服务器），为单位内部、分公司、各下级部门提供到单位内网、政府内网（或其他网络，例如教育网）的访问。在访问时，使用硬件的“智能卡”进行身份验证与数据加密，智能卡具有唯一性，并且每隔一段时间需要进行认证。

本书约定

- 一般情况下，本书采用的VPN服务器，只要配置Pentium 4 2.0 GHz CPU、1GB内存、双网卡、10GB剩余硬盘空间的计算机、具有Internet环境，都可以满足其硬件要求。
- 本书所采用的操作系统是Windows Server 2003 R2（带SP2），ISA Server 2006简体中文标准版、客户端操作系统支持Windows 98及其以上的Windows操作系统。但当使用“智能卡”进行身份验证时，需要Windows XP及其以上的Windows操作系统。

读者对象

- 网络工程技术人员
- 网络技术爱好者
- 网络管理员和网络维护人员
- 网络技术培训机构

本书由王春海、张晓莉、田浩编著，樊玉芳、任文霞、马卫华、乔龙、龚威、白凤涛、陈永川、王冠雄、李海川、潘宁、李荣秀、李琳、王利峰、张新彦、盖伟东、彭静、赵艳也参与了编写工作。另外，感谢王金柱的大力支持与协助。

由于编者水平有限，并且本书涉及的系统与知识点很多，尽管笔者力求完善，但难免有不妥和错误之处，诚恳地期望广大读者和各位专家不吝指教。有关本书的意见反馈和更新消息以及在学习中遇到的问题，您都可以通过下列方式与作者联系。

作者个人网站：<http://www.wangchunhai.cn>

51cto专家博客：<http://wangchunhai.blog.51cto.com>

电子邮件：wangchunhai@heuet.edu.cn

作者

2008年5月

目 录

第1章 VPN网络概述	1
1.1 VPN网络的概念.....	1
1.2 VPN的连接方式.....	3
1.2.1 远程访问VPN连接.....	4
1.2.2 路由器到路由器的VPN连接.....	4
1.3 基于Internet或Intranet的VPN连接.....	4
1.3.1 基于Internet的VPN连接.....	4
1.3.2 基于Intranet的VPN连接.....	5
1.4 VPN的连接属性.....	5
1.4.1 封装.....	5
1.4.2 身份验证.....	5
1.4.3 数据加密.....	6
1.5 本书的VPN方案.....	6
1.6 商用VPN服务器系统需求与网络架构（小于1000个连接）.....	8
1.6.1 为客户端提供PPTP连接的VPN网络拓扑.....	8
1.6.2 为客户端提供L2TP连接的VPN网络拓扑.....	9
1.6.3 为客户端提供智能卡验证的VPN网络拓扑.....	10
1.7 高档商用VPN服务器网络架构（客户端超过1000个连接）.....	11
1.8 VPN服务的硬件与软件构成.....	12
1.9 注意事项.....	13
1.10 本章小结.....	13
第2章 组建基本的VPN服务器	14
2.1 VPN服务器的规划.....	14
2.1.1 单网卡VPN服务器.....	15

2.1.2	双网卡VPN服务器.....	16
2.1.3	用VPN服务器同时代替路由器与防火墙.....	17
2.1.4	有关VPN客户端地址问题.....	18
2.2	单网卡VPN服务器的配置.....	19
2.2.1	单网卡VPN服务器的基本配置.....	19
2.2.2	使用自定义方式启用VPN服务.....	20
2.2.3	为VPN服务器分配客户端IP地址.....	21
2.3	双网卡VPN服务器的配置.....	22
2.3.1	双网卡VPN服务器的基本配置.....	22
2.3.2	启用VPN服务器.....	24
2.4	用VPN服务器做代理服务器.....	26
2.5	VPN用户管理.....	29
2.6	在客户端使用PPTP拨号.....	31
2.6.1	创建VPN拨号连接.....	32
2.6.2	使用VPN客户端连接到VPN服务器.....	34
2.7	本章小结.....	35
第3章	企事业单位VPN网络的组建.....	36
3.1	企事业单位VPN网络拓扑.....	37
3.2	企事业单位VPN服务器的安装与基本配置.....	39
3.2.1	服务器基本配置.....	39
3.2.2	安装ISA Server 2006.....	41
3.2.3	在ISA Server中启用VPN服务.....	43
3.2.4	检查与配置VPN服务器.....	45
3.2.5	创建策略.....	46
3.2.6	用户管理与设置.....	51
3.2.7	使用PPTP拨叫VPN服务器.....	52
3.3	为VPN服务器配置L2TP接入.....	55
3.3.1	配置证书服务器.....	56
3.3.2	允许VPN服务器访问根证书服务器.....	57
3.3.3	在ISA Server中发布证书服务器到Internet.....	60
3.3.4	在VPN服务器上启用L2TP连接支持.....	63
3.3.5	为VPN服务器安装证书.....	64
3.3.6	VPN客户端的设置.....	68
3.3.7	使用L2TP拨叫VPN服务器时出现的问题.....	70
3.4	本章小结.....	71
第4章	具有多出口的校园VPN网络的组建.....	72

4.1	校园VPN网络拓扑	72
4.2	校园VPN服务器的配置	75
4.2.1	关于单网卡问题的解决方案	75
4.2.2	安装ISA Server 2006	78
4.3	在ISA Server中启用VPN服务	78
4.3.1	启用VPN服务	79
4.3.2	创建策略	80
4.3.3	其他配置	81
4.4	使用Windows连接管理器定制VPN客户端	82
4.4.1	在Windows Server 2003中使用连接管理器定制客户端	82
4.4.2	在Windows XP客户端使用打包后的配置文件	90
4.5	本章小结	91
第5章	使用智能卡验证的VPN网络的组建	92
5.1	使用智能卡验证的VPN网络拓扑结构	93
5.2	准备Windows Server 2003的Active Directory服务器	95
5.3	准备企业证书服务器	97
5.4	准备VPN服务器	99
5.4.1	VPN服务器基本准备	99
5.4.2	将计算机加入到Active Directory	99
5.4.3	安装ISA Server	101
5.4.4	申请证书	102
5.5	启用VPN服务	106
5.5.1	为VPN客户端创建访问规则	106
5.5.2	为使用智能卡验证启用VPN服务器	107
5.5.3	在路由和远程访问服务中选择证书服务器	109
5.6	为智能卡用户颁发证书	110
5.6.1	安装智能卡驱动程序	111
5.6.2	初始化智能卡	112
5.6.3	在企业证书服务器上注册服务	113
5.6.4	创建用户并为智能卡颁发证书	116
5.7	使用智能卡登录到VPN服务器	119
5.8	本章小结	122
第6章	某市政府VPN网络解决方案	123
6.1	用户网络现状	123
6.2	用户需求与网络改造总体方案	125
6.3	网络改造具体方案	126

6.3.1	三层交换机的设置	127
6.3.2	路由器与防火墙代理服务器的调试	131
6.4	VPN服务器的组建	131
6.4.1	服务器的总体设置	131
6.4.2	Active Directory服务器与证书服务器的安装与配置	132
6.5	准备VPN服务器	135
6.5.1	VPN服务器基本准备	135
6.5.2	将计算机加入到Active Directory	136
6.5.3	安装ISA Server	137
6.5.4	申请证书	139
6.6	启用VPN服务	141
6.6.1	改变ISA Server网络结构	141
6.6.2	为VPN客户端创建访问规则	144
6.6.3	启用VPN服务器	145
6.6.4	检查路由和远程访问服务是否启用	146
6.7	VPN服务器的分组功能——高级设置	147
6.7.1	提升域功能级别	148
6.7.2	为VPN用户分配静态IP地址	148
6.7.3	在ISA Server上创建不同的访问策略	149
6.7.4	用户不能通过自己设定IP地址的方式访问VPN服务器	152
6.8	使用脚本安装驱动并配置证书、创建VPN连接	153
6.9	VPN客户端使用问题总结	154
6.9.1	解锁被锁定的智能卡	155
6.9.2	吊销丢失的智能卡	156
6.9.3	续订到期证书	157
6.9.4	Windows 2000操作系统的问题	158
6.9.5	用户名或密码无效——691号错误	158
6.9.6	VPN服务器不能到达——800号错误	159
6.9.7	未知错误——802号错误	159
6.9.8	提示PIN码不对——0x8010002A错误	160
6.9.9	身份验证方法错误	160
6.9.10	修改服务器的地址	161
6.9.11	修改PIN码的方法	161
6.10	本章小结	162
第7章 证书（CA）服务		163
7.1	证书（CA）服务概述	163
7.1.1	计算机证书与现实生活中证书的对比	163

7.1.2	证书服务基础知识	164
7.2	企业证书服务器的安装	165
7.3	企业证书服务器的使用	166
7.3.1	通过Web界面申请与安装证书	166
7.3.2	导出与导入证书	169
7.3.3	使用“证书申请向导”申请证书	172
7.3.4	配置证书自动注册策略	174
7.4	企业证书服务器的备份与还原	175
7.4.1	证书的备份	176
7.4.2	证书的还原	177
7.5	企业证书服务的管理	178
7.5.1	发放证书	178
7.5.2	宣告证书无效	178
7.5.3	解除吊销的证书	179
7.5.4	发布证书撤销清单	179
7.6	安装标准证书服务器	180
7.6.1	安装证书服务器	180
7.6.2	标准证书服务的三种角色	183
7.6.3	证书的类型	183
7.7	服务器身份验证证书	184
7.7.1	为Web服务器申请证书	184
7.7.2	在标准CA上颁发证书	187
7.7.3	下载颁发的证书	187
7.7.4	导出证书	188
7.7.5	下载证书颁发机构证书	192
7.7.6	信任标准CA服务器	193
7.8	将申请的计算机证书用于安全Web通信	194
7.8.1	导入证书	194
7.8.2	将证书应用于Web服务器	195
7.8.3	在工作站上使用SSL方式访问Web服务器进行验证	197
7.9	使用证书提高电子邮件的安全性	199
7.9.1	为安全电子邮件申请证书	199
7.9.2	在Foxmail中使用证书(B用户)	203
7.10	本章小结	207
第8章 路由和远程访问服务		208
8.1	路由和远程访问服务简介	208
8.2	Windows Server 2003路由服务	209

8.2.1	Windows Server 2003路由器基本应用	210
8.2.2	路由表	212
8.2.3	路由协议	213
8.2.4	其他特性	214
8.3	Windows Server 2003远程访问服务	216
8.3.1	Windows Server 2003远程访问服务的新特性	216
8.3.2	远程访问服务的类型	218
8.3.3	远程访问服务的物理连接	219
8.3.4	远程访问协议	223
8.3.5	远程访问服务的验证与计费	225
8.4	路由和远程访问服务中的“路由器”功能	227
8.4.1	为每块网卡设置名称并设置IP地址	228
8.4.2	启用路由器功能	228
8.5	远程访问服务的启用和配置	230
8.5.1	远程访问服务器的准备工作	230
8.5.2	配置远程访问服务	233
8.5.3	配置远程访问服务客户端	239
8.6	远程访问策略	247
8.6.1	访问策略	247
8.6.2	远程访问策略的评估流程	249
8.6.3	默认策略	251
8.6.4	多策略	252
8.6.5	访问策略设置	253
8.7	本章小结	255
第9章 ISA Server 2006代理服务器与防火墙		256
9.1	ISA Server功能概述	256
9.1.1	代理服务器功能——提供安全性非常高的共享Internet服务	257
9.1.2	加快Web访问速度——业界最好的缓存服务器	257
9.1.3	虚拟专用网络（VPN）支持——代理服务器、防火墙服务器与VPN服务器共存	257
9.1.4	安全发布服务器——将内部网络中的多台服务器发布到Internet对外提供服务	258
9.2	防火墙与代理服务器的基础知识	259
9.2.1	网络服务与端口的关系	259
9.2.2	TCP/IP地址的意义	261
9.2.3	代理与转换	261
9.2.4	端口映射与端口转发	262
9.2.5	理解ISA Server 2006中的网络	262
9.2.6	理解ISA Server 2006的规则	263

9.2.7	理解ISA Server2006的客户端.....	263
9.3	ISA Server的部署与应用.....	265
9.3.1	Internet边缘防火墙.....	265
9.3.2	部门或主干网络防火墙.....	265
9.3.3	分支办公室防火墙.....	266
9.3.4	安全服务器发布.....	266
9.4	ISA Server 2006部署与使用注意事项.....	267
9.4.1	安装ISA Server 2006的软件与硬件需求.....	267
9.4.2	多VLAN网络中三层交换机的配置.....	267
9.4.3	在计算机上添加到其他网段的静态路由.....	269
9.4.4	ISA Server 2006的安装.....	269
9.5	安全连接Internet——将ISA Server 2006用作代理服务器.....	272
9.5.1	允许内网访问Internet.....	272
9.5.2	允许内网ping通网关.....	277
9.5.3	允许本地主机访问外网.....	278
9.5.4	有关使用QQ等聊天软件和联众游戏的设置.....	280
9.5.5	在ISA Server 2006中屏蔽垃圾网站、黄色网站和恶意网站.....	287
9.5.6	禁止使用代理服务器访问被禁止访问的网站和禁止使用的服务.....	290
9.5.7	禁止用户QQ、MSN等聊天软件和BT等P2P下载软件.....	291
9.5.8	利用ISA Server 2006阻止某些文件.....	293
9.6	发布服务器.....	294
9.6.1	发布Web站点.....	295
9.6.2	发布邮件服务器.....	299
9.6.3	发布Exchange Web客户端访问.....	300
9.6.4	发布SharePoint站点.....	302
9.6.5	发布其他服务器.....	303
9.6.6	发布安全Web服务器.....	305
9.6.7	为Internet用户提供代理服务.....	306
9.7	本章小结.....	308
第10章	Windows Server 2003服务器关键问题的解决.....	309
10.1	VPN服务器在第一次登录到域时出现错误.....	309
10.2	怎样添加授权数量.....	312
10.3	启用Windows Server 2003的硬件加速.....	316
10.4	禁用IE增强的安全配置.....	317
10.5	修改关机菜单.....	319
10.6	修改盘符.....	320
10.7	本章小结.....	321

附录A VMware Workstation 6.0 基本操作	322
A.1 创建虚拟机的方法	322
A.1.1 创建“典型”的虚拟机	322
A.1.2 创建“自定义”的虚拟机	324
A.2 修改虚拟机配置	327
A.3 打造虚拟机模板（在虚拟机中安装操作系统）	328
A.3.1 定制Windows XP Professional虚拟机模板	329
A.3.2 安装Windows XP	330
A.3.3 安装VMware Tools	334
A.3.4 使用共享文件夹	335
A.4 在虚拟机中使用U盘和其他USB设备	338
A.5 使用快照与使用克隆虚拟机	339
A.5.1 使用快照	339
A.5.2 使用克隆虚拟机	340
A.6 虚拟网络设备及虚拟机中的Team功能描述	342
附录B 本书中实验环境的搭建	344
B.1 第2章实验环境的搭建	344
B.1.1 实验前准备	344
B.1.2 创建克隆虚拟机	344
B.1.3 新建Team并进行设置	345
B.2 第3章实验环境的搭建	348
B.3 第4章实验环境的搭建	355
B.4 第5章实验环境的搭建	356
B.5 第6章实验环境的搭建	357



1

CHAPTER

VPN 网络概述

本章首先简要介绍虚拟专用网络（Virtual Private Network, VPN）的概念，然后介绍VPN网络的连接方式、连接属性以及商用VPN服务器的系统需求和网络架构。

技术要点：

- (1) VPN网络的概念。
- (2) VPN网络的拓扑结构。
- (3) VPN网络的基础理论知识。
- (4) 软、硬件VPN网络各自的特点与优缺点。

学习目标：

- (1) 理解网络的“物理连接”、“逻辑连接”。
- (2) 掌握VPN网络的网络拓扑、组成与架构。

1.1 VPN网络的概念

使用通信介质将网络设备与计算机设备连接之后，网络在“物理”上已经连通，但必须让“计算机设备”通过“通信介质”与“网络设备”进行“逻辑连通”，才可能进行网络的应用。

所谓“逻辑连通”，是指在网络应用范围内的网络中，两个想要通信的“计算机设备”（假设这两个计算机设备之间没有网络防火墙或者防火墙未生效，而防火墙问题暂时不考虑）是可以互相ping通的。在TCP/IP网络中，两个设备（或多个设备）可以互相ping通，包括以下几种情况（物理网络已经连通）。

▼ 两个设备在同一个子网之中，即子网掩码相同，网络号相同，只有主机号不同。例

如，IP 地址分别为 192.168.1.1 和 192.168.1.23，子网掩码都是 255.255.255.0。

- 两个设备不在同一个子网之中，但这两个设备之间有路由器或网关，由路由器或网关转发数据，使这两个设备之间可以通信。

所以，只要交换机或路由器中的路由参数（路由表）正确，计算机设置正确（正确设置IP地址、子网掩码、网关地址），网络物理连通，就可以互相访问、ping通（不考虑防火墙屏蔽网络之间互访信息）。

网络物理连通、网络逻辑连通之后，网络设备就可以通信了。当然，如果在网络中处于“关键位置”的设备上设置了规则“阻止”某些设备通信，则网络也可能无法通信。图 1-1 中的“三层交换机”、“防火墙”和“路由器”都处于关键位置。

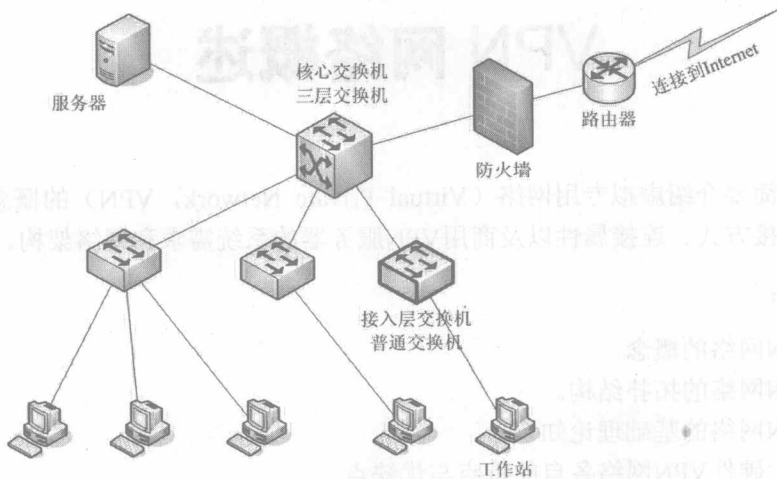


图 1-1 一个有防火墙、交换机、路由器、服务器和工作站的网络拓扑

根据网络“物理连通”的规模，网络可以分为局域网、城域网和广域网。许多的广域网与局域网互联后组成了Internet。

局域网，是指物理位置相近的、一个单位内的所有计算机组成的网络，或者个人的几台计算机组成的网络。局域网可以大到覆盖整个单位的所有楼层，小到只包含两台计算机。局域网主要使用交换机进行设备之间的互联，局域网如果要访问Internet，一般通过中心机房的“出口”连接到Internet。局域网是高速互联的，网络中的每台计算机都可以高速访问其他计算机或者服务器，通常情况下，局域网中的计算机可以用100Mbit/s的速度连接到交换机，局域网中的服务器通常以1Gbit/s甚至10Gbit/s的速度连接到中心交换机。

城域网，是指在局域网的基础上，将分布在同一个城区或一定范围内的一些局域网、单机连接在一起组成的网络。城域网的物理范围要大于局域网，它通常是多个单位或者一个单位的不同部门（物理上分散）通过无线或者租用网通或电信线路组建的网络。例如，某个城市的市政府、法院、医院、农业局等单位组建的政府内网就是城域网的典型示例。一般来说，城域网互联的接口速度要远远低于局域网的速度，一般为几Mbit/s到几十Mbit/s。

广域网，是指在局域网的基础上，将一个单位的不同分公司、分部门的局域网，通过租用网络服务提供商（ISP）的线路连接起来组成的网络。像公安、税务、银行、电力等部

门，一般都组成省、市、县、镇四级的网络结构，如图1-2所示。

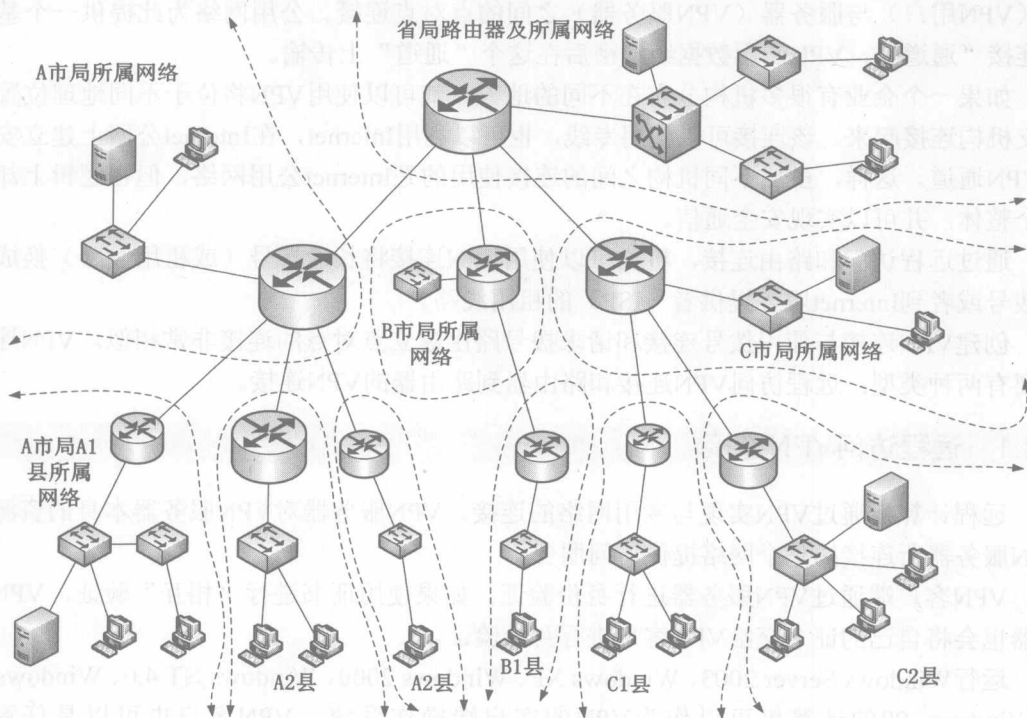


图 1-2 省、市、县、镇四级广域网结构拓扑图

在图1-2的网络拓扑中，省局到市局速度最快，市局到县局其次，县局到乡镇速度最慢。每个节点可以通过其上级节点与相邻节点互通。

在城域网与广域网中，都需要租用ISP的线路，通常情况下需要按月或者按年向ISP交纳专线租用费，而且费用比较高。

VPN网络是在“城域网”与“广域网”基础上，利用ISP提供的Internet接入线路，在公网（指Internet）上组建自己私有网络的一种技术与方法。通过Internet组建VPN网络，可以极大地节省组建成本与使用费用（与组建广域网相比）。

1.2 VPN的连接方式

通过VPN能以模拟点对点专用链路的方式，通过共享或公用网络在两台计算机之间交换数据。虚拟专用网是创建和配置虚拟专用网的行为。

要模拟点对点链路，应压缩或包装数据，并加上一个提供路由信息的报头，该报头使数据能够通过共享或公用网络到达其终点。为保密起见，如果要模拟专用链路，则应加密数据。一旦加密，若不知道密钥，即使从共享或者公用网络截取到数据包，也是很难解密的。封装和加密专用数据之外的连接是VPN连接。

在家里或者旅途中工作的用户可以使用VPN连接建立到企业内网的服务器的远程访问

连接，方法是使用公用网络提供的基础结构。从用户的角度来讲，VPN连接是一种在计算机（VPN用户）与服务器（VPN服务器）之间的点对点连接。公用网络为此提供一个基础的连接“通道”，VPN专用数据经加密后在这个“通道”上传输。

如果一个企业有很多机构分布在不同的地方，就可以使用VPN将位于不同地理位置的分支机构连接起来。该连接可以使用专线，也可以利用Internet，在Internet公网上建立安全的VPN通道。这样，虽然不同机构之间的连接使用的是Internet公用网络，但在逻辑上却是一个整体，并可以实现安全通信。

通过远程访问和路由连接，机构可以使用VPN连接将长途拨号（或租用线路）换成本地拨号或者到Internet服务提供者（ISP）的租用线路。

创建VPN连接与使用拨号连接和请求拨号路由建立点对点的连接非常相似。VPN连接主要有两种类型：远程访问VPN连接和路由器到路由器的VPN连接。

1.2.1 远程访问VPN连接

远程计算机通过VPN实现与专用网络的连接。VPN服务器对VPN服务器本身的资源及VPN服务器所连接的整个网络提供访问服务。

VPN客户端通过VPN服务器进行身份验证，如果使用证书进行“相互”验证，VPN服务器也会将自己的证书交给VPN客户进行身份验证。

运行Windows Server 2003、Windows XP、Windows 2000、Windows NT 4.0、Windows 95和Windows 98的计算机可以作为VPN的客户端操作系统，VPN客户也可以是任意非Microsoft点对点隧道协议（PPTP）的客户端，或是有IPSec的第二层隧道协议（L2TP）客户端。

1.2.2 路由器到路由器的VPN连接

路由器可以通过建立路由器到路由器的VPN连接将专用网络的两个部分连接起来。VPN服务器可以提供与网络的路由连接，以使此网络与VPN服务器连接。在路由器到路由器的VPN连接上，当两个路由器之间建立VPN连接时，路由器只负责数据包的发送和接收，但在发送之后和接收之前都要通过VPN进行数据包的处理。

1.3 基于Internet或Intranet的VPN连接

在需要安全的点对点连接来连接用户或网络时，可以使用VPN连接。典型的VPN连接可分为基于Internet的VPN连接和基于Intranet的VPN连接两种类型。

1.3.1 基于Internet的VPN连接

使用基于Internet的VPN连接，可以充分利用覆盖全球的Internet，费用较低。它一般也有以下两种方式。

- Internet 上的远程访问。远程访问客户通过 Internet 来初始化 VPN，连接到专用网