

华为系列丛书

HCNA

网络技术

◎ 蒋建峰 蒋建锋 马强 编著



中国工信出版集团



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>

华为系列丛书

HCNA 网络技术

蒋建峰 蒋建锋 马 强 编著

电子工业出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本书以 HCNA 职业认证内容为参考, 主要面向高校学生, 旨在为广大院校学生提供一个学习最新实用网络技术的窗口。在圆满完成本课程内容的学习后, 学生可以参加华为公司认证考试, 获取华为公司权威数通认证, 提升自身竞争力。本书主要内容包括: IP 网络层次结构、华为数通设备在电信级 IP 网络中的应用; IP 协议、ICMP/Ping/Tracert 原理、IPv6 基础知识; HDLC/PPP 协议基本原理与配置、Frame Relay 基本原理与配置; 以太网技术、交换机基本原理、VLAN 基本原理与配置、STP 基本原理与配置; 路由器工作原理、VRRP 特点与基本配置、静态路由协议原理与配置、RIP 协议基本原理与配置、OSPF 协议基本原理与配置、路由器基本故障处理方法; 防火墙类型和基本原理、ACL 和 NAT 在防火墙中的实现等。

本书既可作为高职高专院校计算机网络技术、通信、电子信息类专业及其他相关专业的网络基础课程教材, 也可作为对计算机网络技术感兴趣的相关专业技术人员的参考书, 还可作为准备参加华为公司认证考试人员的复习资料和相关企业员工的培训教材。

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

HCNA 网络技术/蒋建峰, 蒋建锋, 马强编著. —北京: 电子工业出版社, 2019.1
(华为系列丛书)
ISBN 978-7-121-35585-1

I. ①H… II. ①蒋… ②蒋… ③马… III. ①企业内联网—教材 IV. ①TP393.18

中国版本图书馆 CIP 数据核字(2018)第 265053 号

策划编辑: 宋 梅

责任编辑: 王 炜

印 刷: 三河市良远印务有限公司

装 订: 三河市良远印务有限公司

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: 787×980 1/16 印张: 14.25 字数: 320 千字

版 次: 2019 年 1 月第 1 版

印 次: 2019 年 1 月第 1 次印刷

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, 88258888。

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

本书咨询联系方式: mariams@phei.com.cn。

前 言

嘉环公司是华为公司在国内重点培育的华为客户培训分部、授权培训合作伙伴 (HALP)、华为教育合作伙伴 (HAEP)。苏州工业园区服务外包职业学院与嘉环公司合作成立嘉环 ICT 学院, 积极参与 ICT 专业的人才培养, 提供教育服务整体解决方案。

书本以 HCNA 为参考, 主要面向高校学生, 旨在为广大院校学生提供学习最新实用网络技术的窗口。编著者长期从事网络技术专业的教学工作, 同时也与业内知名企业合作紧密, 在技能型人才配型方面有着独到的经验, 本书旨在提供一本理实一体化教材, 充分体现技能的培养。

本书内容安排以基础性和实践性为重点, 力图在讲述路由与交换相关协议工作原理的基础上, 注重对学生实践技能的培养。本书的主要特色是教学内容设计做到了理论与技术应用的对接, 具有鲜明的专业教材特色, 在理论上把各个协议的原理讲述透彻, 在实验的设计方面以实际工程应用为基础, 体现与实际工程接轨。

全书分为 7 章。

第 1 章主要讲述 VRP 的基础知识, 以及华为 VRP 平台的基本操作。

第 2 章主要介绍以太网技术、虚拟局域网、生成树协议 STP 及以太网链路聚合技术。

第 3 章主要介绍路由原理与各类路由协议, 主要涉及静态路由、RIP 协议、OSPF 协议、IS-IS 协议和 BGP 协议。

第 4 章介绍网络安全相关技术, 包括 ACL、DHCP、NAT 和防火墙技术。

第 5 章介绍广域网互联技术, 包括 HDLC、PPP 和帧中继。

第 6 章介绍虚拟专网 VPN 技术, 包括 MPLS 和 BGP MPLS VPN 技术。

第 7 章以工程项目作为背景, 综合分析实践路由与交换技术。

本书的编写团队由蒋建峰老师、蒋建锋老师和嘉环公司项目经理马强联合组成, 全书由蒋建峰老师统稿。由于作者水平有限, 书中难免存在错误和疏漏之处, 敬请各位老师和同学指正, 可发送邮件至 alaneroson@126.com。

编著者

2018 年 12 月

目 录

第 1 章 VRP 基础及操作	1
1.1 VRP 基础	1
1.1.1 VRP 平台介绍	1
1.1.2 配置环境搭建	2
1.1.3 VRP 配置基础	6
1.2 实训 VRP 平台基本操作	10
1.3 总结与习题	21
第 2 章 以太网交换技术	22
2.1 以太网原理	22
2.1.1 以太网数据链路层	22
2.1.2 以太网的帧格式	23
2.1.3 共享式以太网	24
2.1.4 交换式以太网	25
2.2 虚拟局域网	29
2.2.1 VLAN 概述	29
2.2.2 VLAN 的划分方式	30
2.2.3 VLAN 技术原理	32
2.2.4 VLAN 端口类型	35
2.2.5 VLAN 的基本配置	36
2.3 生成树协议 STP	37
2.3.1 STP 的产生	37
2.3.2 STP 的基本原理	41
2.3.3 STP 端口状态	45
2.4 以太网端口技术	46
2.4.1 端口自协商技术	46
2.4.2 端口聚合技术	47
2.5 实训一 交换机 VLAN 配置	49
2.6 实训二 生成树协议 STP 配置	51
2.7 实训三 交换机链路聚合配置	59
2.8 总结与习题	61

第3章 路由的实现	62
3.1 路由基础	62
3.1.1 路由与路由器	62
3.1.2 路由原理	63
3.1.3 路由的来源	65
3.1.4 路由的优先级	68
3.1.5 路由的度量值	69
3.1.6 VLAN 间通信	72
3.2 动态路由协议基础	74
3.2.1 动态路由协议概述	74
3.2.2 动态路由协议分类	75
3.2.3 动态路由协议的性能指标	76
3.3 RIP 协议	76
3.3.1 RIP 协议概述	76
3.3.2 RIP 协议工作过程	77
3.3.3 RIP 协议的配置	78
3.4 OSPF 协议	78
3.4.1 OSPF 协议概述	78
3.4.2 OSPF 协议工作过程	79
3.4.3 OSPF 协议报文	82
3.4.4 OSPF 网络类型	83
3.4.5 OSPF 区域	85
3.4.6 路由引入	86
3.4.7 OSPF 配置	88
3.5 IS-IS 协议	88
3.5.1 IS-IS 协议概述	88
3.5.2 IS-IS 区域划分、路由器类型和邻接关系	90
3.5.3 IS-IS 协议工作过程	92
3.5.4 IS-IS 协议报文	94
3.5.5 路由引入	96
3.5.6 路由渗透	96
3.5.7 IS-IS 配置	97
3.6 BGP 协议	97
3.6.1 BGP 协议概述	97
3.6.2 BGP 协议工作过程	98

3.6.3 BGP 协议报文	99
3.6.4 BGP 路径属性	100
3.6.5 BGP 路径选择	103
3.7 虚拟路由冗余 VRRP 协议	103
3.7.1 VRRP 工作原理	103
3.7.2 VRRP 协议报文	105
3.7.3 VRRP 工作方式	106
3.7.4 VRRP 基本配置	107
3.8 实训一 静态路由配置	108
3.9 实训二 默认路由配置	110
3.10 实训三 RIPv2 配置	112
3.11 实训四 OSPF 单区域配置	115
3.12 实训五 OSPF 多区域配置	119
3.13 实训六 RIP、OSPF 路由引入	123
3.14 实训七 BGP 协议配置	130
3.15 总结与习题	137
第 4 章 网络安全技术	139
4.1 ACL 技术	139
4.1.1 ACL 概述	139
4.1.2 ACL 工作原理	140
4.1.3 通配符掩码	141
4.1.4 ACL 匹配顺序	142
4.2 DHCP 技术	143
4.2.1 DHCP 概述	143
4.2.2 DHCP 的组网方式	143
4.2.3 DHCP 协议报文	145
4.2.4 DHCP 工作过程	145
4.3 NAT 技术	147
4.3.1 NAT 概述	147
4.3.2 基本地址转换	148
4.3.3 端口地址转换	149
4.4 防火墙技术	150
4.4.1 防火墙概述	150
4.4.2 防火墙的安全区域	151

4.5	实训一 基本 ACL 配置	153
4.6	实训二 DHCP 的配置与实现	156
4.7	实训三 防火墙 NAT 的配置与实现	158
4.8	总结与习题	160
第 5 章	广域网互联技术	161
5.1	HDLC 协议	161
5.2	PPP 协议	162
5.2.1	PPP 协议概述	162
5.2.2	PPP 协议工作流程	163
5.2.3	PPP 协议的认证	164
5.2.4	PPPoE 协议	165
5.3	帧中继协议	166
5.3.1	帧中继协议概述	166
5.3.2	帧中继协议的帧结构	167
5.3.3	帧中继协议的带宽管理	168
5.3.4	帧中继协议的分配	169
5.3.5	帧中继协议的寻址	169
5.4	实训一 HDLC 互联配置	170
5.5	实训二 PPP 互联配置	171
5.6	实训三 帧中继协议的配置与实现	173
5.7	总结与习题	174
第 6 章	虚拟专网 VPN 技术	176
6.1	MPLS	176
6.1.1	MPLS 概述	176
6.1.2	MPLS 结构	177
6.1.3	MPLS 标签格式	178
6.1.4	MPLS 转发流程	179
6.2	BGP MPLS VPN	181
6.2.1	MPLS VPN 概述	181
6.2.2	BGP MPLS VPN 基本工作原理	183
6.2.3	BGP MPLS VPN 路由传递	184
6.2.4	BGP MPLS VPN 标签分配过程	188
6.2.5	BGP MPLS VPN 数据转发过程	188

6.3	实训 BGP MPLS VPN 配置	189
6.4	总结与习题	194
第 7 章	项目综合分析	195
7.1	项目需求	195
7.2	业务功能分析	196
7.3	任务分解	197
7.4	网络基础部分项目实施	197
7.4.1	网络地址规划	197
7.4.2	网络设备基本配置	200
7.5	局域网的组建部分项目实施	204
7.5.1	VLAN 的配置与实现	204
7.5.2	端口聚合的配置与实现	207
7.5.3	STP 的配置与实现	209
7.5.4	单臂路由的配置与实现	212
7.5.5	三层交换的配置与实现	214

第 1 章 VRP 基础及操作

本章导读

计算机网络诞生以来，伴随着信息技术的革新与发展，在经济、生活等各个方面扮演着越来越重要的角色。本章要求掌握 VRP 平台操作系统，掌握网络设备的基本操作，能对设备做简单的调试。

1.1 VRP 基础

1.1.1 VRP 平台介绍

VRP (Versatile Routing Platform) 通用路由平台是华为公司数据通信产品使用的网络操作系统。它是运行于一定设备上的、提供网络接入及互联服务的系统软件。

VRP 通用路由平台（简称 VRP 平台）作为华为公司从低端到核心的全系列路由器、以太网交换机、业务网关等产品的软件核心引擎，实现统一的用户界面和管理界面；实现控制平面功能，并定义转发平面端口规范，实现各产品转发平面与 VRP 控制平面之间的交互；屏蔽各产品数据链路层对于网络层的差异。

随着网络技术和应用的飞速发展，VRP 平台在处理机制、业务能力、产品支持等方面也在持续演进。VRP 版本主要有 VRP1.x、VRP3.0~3.x、VRP5.10、VRP5.30、VRP5.70、VRP5.90，分别具有不同的业务能力和产品支持能力。

为了使单一软件平台能运行于各类路由器和交换机之上，VRP 软件模块采用了组件结构，各种协议和模块之间采用了开放的标准端口。VRP 由 GCP、SCP、DFP、SMP、SSP 五个平面组成，VRP 平台结构如图 1-1 所示。

通用控制平面 (GCP)：支持网络协议簇，其中包括 IPv4 和 IPv6。它所支持的协议和功能包括 SOCKET、TCP/IP 协议、路由管理、各类路由协议、VPN、端口管理、链路层、MPLS、安全性能，以及对 IPv4 和 IPv6 的 QoS 支持。

业务控制平面 (SCP)：基于 GCP 支持增值服务，包括连接管理、用户认证计费、用户策略管理、VPN、组播业务管理和维护与业务控制相关的 FIB。

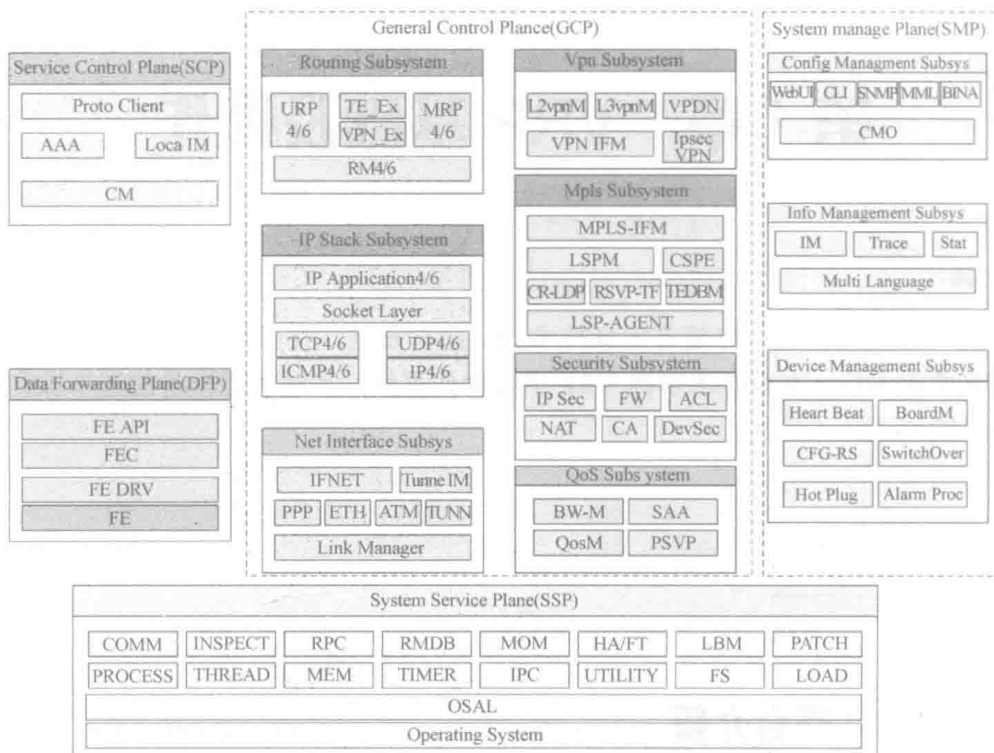


图 1-1 VRP 平台结构

数据转发平面 (DFP): 为系统提供转发服务, 由转发引擎和 FIB 维护组成。转发引擎可依照不同产品的转发模式通过软件或硬件实现, 数据转发支持高速交换、安全转发和 QoS, 并可通过开放端口支持转发模块的扩展。

系统管理平面 (SMP): 具有系统管理功能, 其外部与设备交互端口, 对外控制输入、协议配置输入进行处理。在平台的配置和管理方面, VRP 可灵活引入一些网络管理机制, 如命令行、NMP 和 Web 等。

系统服务平面 (SSP): 支持公共系统服务, 如内存管理、计时器、IPC、装载、转换、任务/进程管理和组件管理。

VRP 平台还具有支持产品许可证文件 (License) 的功能, 可在不破坏原有服务的前提下根据需要调整各种特性和性能的范围。

1.1.2 配置环境搭建

系统支持的一般配置方式有以下三种:

- 通过 Console 口进行本地配置;
- 通过 Telnet 或 SSH 进行本地或远程配置;
- 通过 AUX 口进行本地或远程配置。

1. 通过 Console 口配置

以下两种情况只能通过 Console 口搭建配置环境：

- ① 路由器第一次上电；
- ② 无法通过 Telnet 或 AUX 口搭建配置环境。

通过 Console 口配置路由器的操作步骤如下。

(1) 连接配置电缆

- ① 取出路由器随机配置的电缆。
- ② RJ45 端口一端接在路由器的 Console 口上。
- ③ 9 针（或 25 针）RS-232 端口一端接在计算机的串行口（COM）上，如图 1-2 所示。

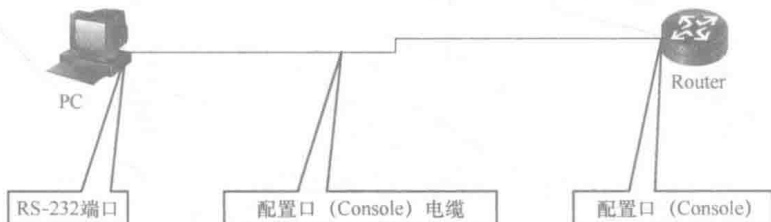


图 1-2 通过 Console 口配置

(2) 创建超级终端

- ① 在计算机上运行终端仿真程序（Windows XP 的“超级终端”等）。
- ② 单击“开始”→“程序”→“附件”→“通信”→“超级终端”。
- ③ 单击“超级终端”目录后，出现“新建连接”选项卡，输入任意字符作为名字，选择使用相应的 COM 连接，单击“确定”按钮，出现图 1-3 所示的界面，在该界面中设置如下：9600bps、8 位数据位、无奇偶校验、1 位停止位和无流量控制，然后单击“OK”按钮，即可登录设备进行操作。



图 1-3 超级终端环境配置

通过 Console 口配置是网络设备的基本配置方法，也是在网络构建、设备调试过程中最常用到的方式。

2. 通过 Telnet 配置

如果路由器非第一次上电, 而且用户已经正确配置了路由器各端口的 IP 地址, 并配置了正确的登录验证方式和呼入/呼出受限规则。在配置终端与路由器通信正常的情况下, 可以用 Telnet 通过局域网或广域网登录到路由器, 对路由器进行配置, 如图 1-4 所示。

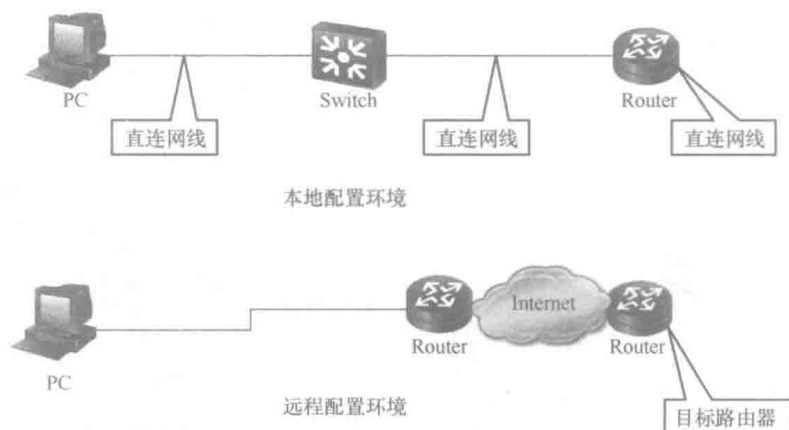


图 1-4 Telnet 配置环境

如果路由器和配置终端处于同一个局域网, 可以采用如下两种方式分别进行配置:

- 使用标准直通网线, 将 PC 等配置终端通过 Hub 或二层交换机与路由器相连;
- 使用交叉网线, 将 PC 等配置终端与路由器直接相连。

采用本地配置方式时, PC 等配置终端的 IP 地址需要与路由器以太网口的 IP 地址处于同一网段。

如果路由器和配置终端之间跨越了广域网, 则首先要保证配置终端与目标路由器之间存在可达路由且通信正常, 然后才可以通过 Telnet 登录路由器, 如图 1-5 所示。

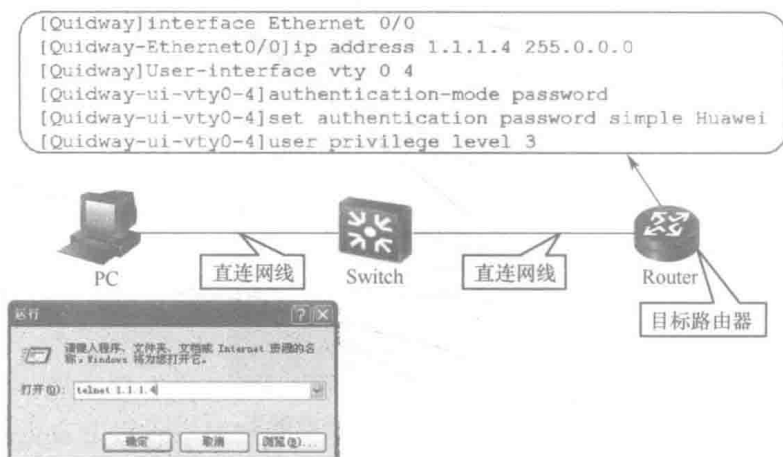


图 1-5 Telnet 配置举例

通过 Telnet 方式配置路由器之前，必须要在路由器上进行如下配置并保证配置终端和路由器维护网口之间通信正常，即从配置终端能够 ping 通路由器维护网口 IP 地址，另外还需要设置用户登录时使用的参数，包括对登录用户的验证方式。对登录用户的验证方式有以下三种：

- ① Password 验证：登录用户需要输入正确的口令；
- ② AAA 本地验证：登录用户需要输入正确的用户名和口令；
- ③ 不验证：登录用户不需要输入用户名或口令。但需要配置登录用户的权限。

详细设置与说明如下：

- 配置路由器的 IP 地址和 PC 的 IP 地址

#进入路由器接口视图

```
[Quidway]interface Ethernet 0/0
```

#为接口配置 IP 地址

```
[Quidway-Ethernet0/0]ip address 1.1.1.4 255.0.0.0
```

配置完路由器的 IP 地址，还需要配置 PC 的 IP 地址（如 1.1.1.2/8），完成配置后可以在 PC 上 ping 1.1.1.4，检查 PC 和路由器之间通信是否正常。

- 配置 Telnet 方式登录时的密码

#进入 vty 用户视图，0 4 表示允许最多 5 个用户同时登录

```
[Quidway] User-interface vty 0 4
```

#选择验证模式为 password

```
[Quidway-ui-vty0-4] authentication-mode password
```

#配置验证时需要的密码为 Huawei

```
[Quidway-ui-vty0-4] set authentication password simple Huawei
```

#设置用户级别为管理级别

```
[Quidway-ui-vty0-4] user privilege level 3
```

完成上述配置后，即可以在 PC 上运行 telnet 1.1.1.4 登录路由器

3. 通过 AUX 口配置

通过 AUX 口配置路由器如图 1-6 所示，在配置终端的串口和路由器的 AUX 口分别连接 Modem，Modem 通过 PSTN 网络连接。

在路由器上需要进行以下配置：

#进入 aux 用户视图

```
[Quidway] User-interface aux 0
```

#选择验证模式为 password

```
[Quidway-ui-aux0] authentication-mode password
```

#配置验证时需要的密码为 Huawei

```
[Quidway-ui-aux0] set authentication password simple Huawei
```

#设置用户的权限

```
[Quidway-ui-aux0] user privilege level 3
```

#配置允许 Modem 呼入/呼出

```
[Quidway-ui-aux0] modem both
```

完成上述配置后, 在 PC 上打开超级终端选择通过 Modem 连接登录路由器

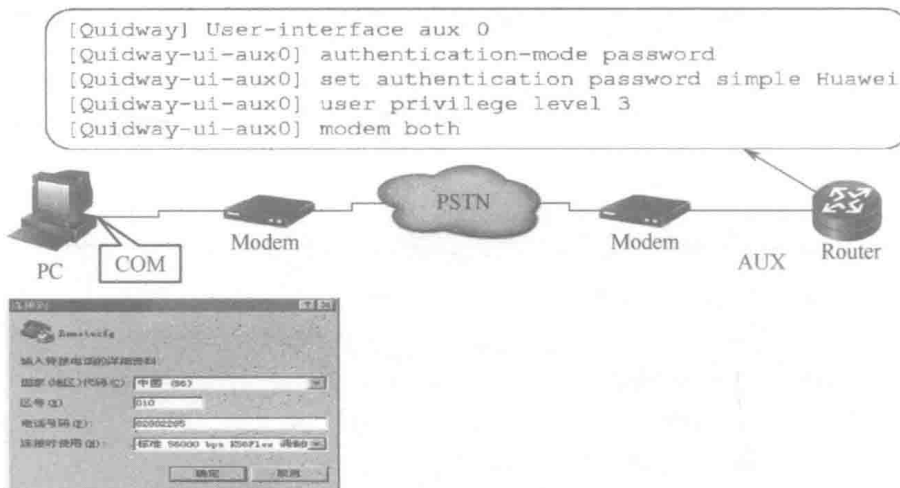


图 1-6 通过 AUX 口配置路由器

1.1.3 VRP 配置基础

登录路由器进入用户视图。在用户视图中用<>表示, 如<Quidway>这个视图就是用户视图, 如图 1-7 所示。在用户视图中只能执行文件管理、查看、调试等命令, 不能够执行设备维护、配置修改等工作。如果需要对网络设备进行配置, 必须在相应的视图模式下才可以进行。比如, 需要对端口创建 IP 地址, 那么就必须在端口视图下, 用户只有首先进入到系统视图后, 才能进入其他的子视图。

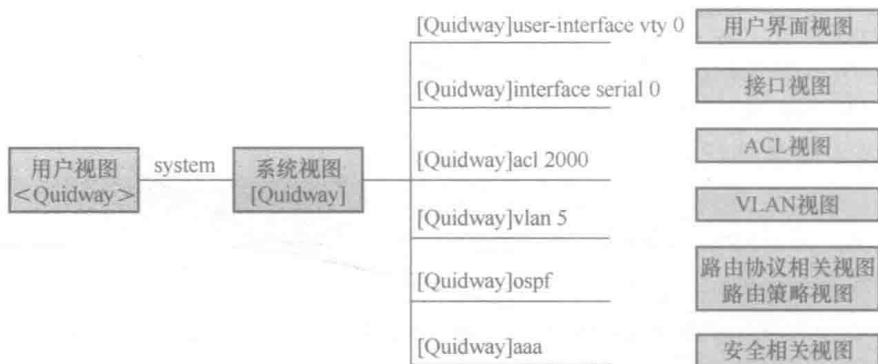


图 1-7 VRP 命令视图

从用户视图使用 System-view 命令可以切换到系统视图, 从系统视图使用 Quit 命令可

以切换到用户视图。

从系统视图使用相关的业务命令可以进入其他业务视图，不同的视图下可以使用的命令也不同。系统命令采用分级方式，如图 1-8 所示。

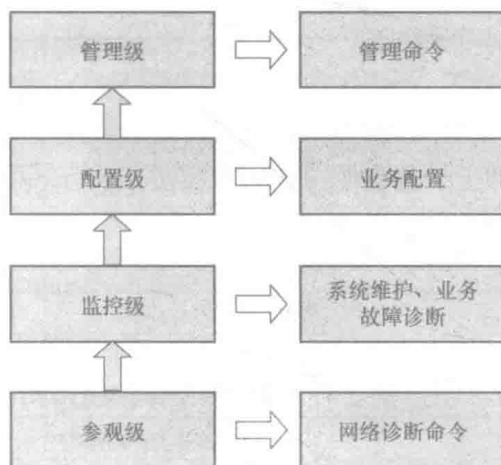


图 1-8 VRP 命令级别

系统命令从低到高划分为 4 个级别：

参观级：网络诊断工具命令（ping、tracert）、从本设备出发访问外部设备的命令（Telnet 客户端、SSH、Rlogin）等。

监控级：用于系统维护、业务故障诊断，包括 display、debugging 等命令。

配置级：业务配置命令，包括路由、各个网络层次的命令，向用户提供直接网络服务。

管理级：用于系统基本运行的命令，对业务提供支撑作用，包括文件系统、FTP、TFTP、Xmodem 下载、配置文件切换命令、备板控制命令、用户管理命令、命令级别设置命令、系统内部参数设置命令等。

系统对登录用户也划分为 4 级，分别与命令级别对应，即不同级别的用户登录后，只能使用等于或低于自己级别的命令。当用户从低级别用户切换到高级别用户时，需要使用命令：super password [level user-level] { simple | cipher } password 切换。

1. 进入和退出系统视图

(1) 从用户视图进入系统视图

```
<Quidway>system-view
Enter system view, return user view with Ctrl+Z
```

(2) 从系统视图进入端口视图

```
[Quidway]interface Serial 0/0/0
[Quidway-Serial0/0/0]
```

(3) 从端口视图退回到系统视图

```
[Quidway-Serial0/0/0]quit
```

```
[Quidway]
```

(4) 从系统视图退回到用户视图

```
[Quidway]quit
```

```
<Quidway>
```

命令 quit 的功能是返回上一层视图，在用户视图下执行 quit 命令就会退出系统。

命令 return 可以使用户从任意非用户视图退回到用户视图。return 命令的功能也可以用组合键【Ctrl+Z】完成。

2. 命令行在线帮助

命令行端口提供如图 1-9 所示的 2 种 VRP 命令行在线帮助：完全帮助和部分帮助。

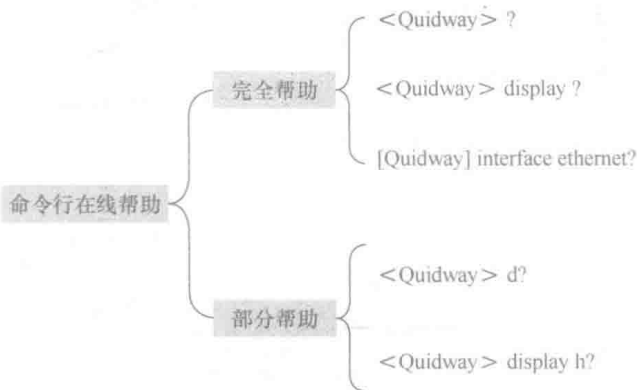


图 1-9 VRP 命令行在线帮助

<Quidway>?: 在任一命令视图下，输入“?”获取该命令视图下所有的命令及其简单描述。

<Quidway>display ?: 输入一命令后，接以空格分隔的“?”，如果该位置为参数，则列出有关的参数描述。

[Quidway]interface ethernet?: 输入一字符串，其后紧接“?”，列出以该字符串开头的命令：

```
<3-3> Slot number
```

<Quidway>d?: 输入一命令，后接一字符串紧接“?”，列出命令以该字符串开头的所有关键字：

```
Debugging delete dir display
```

<Quidway>display h?: 输入命令的某个关键字的前几个字母，按【tab】键，可以显示出完整的关键字：history-command。