思科系列丛书

广域网技术精要与实践

蒋建峰　杜梓平◎编著

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

思科系列丛书

广域网技术精要与实践

蒋建峰　杜梓平　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书针对高职高专教育的培养目标和要求，以广域网相关技术的原理与操作技能为主要内容，根据改版更新后的思科网络技术 CCNA RS 版本及 CCNA 认证考试要求，合理安排教学与实验内容，充分体现了理论实践一体化的理念，把实验操作与理论知识相结合，符合高职高专学生的学习、认知特点。全书共 8 章，第 1 章主要介绍广域网链路封装技术 HDLC 和 PPP 的基本操作技能；第 2 章介绍帧中继 FR 的概念和基本配置；第 3 章主要介绍网络访问控制技术 ACL 及相关配置；第 4 章介绍 DHCP 协议的工作原理和配置；第 5 章介绍网络地址转换协议 NAT 的特点、类型及配置；第 6 章详细介绍广域网安全主流技术 VPN 的工作原理和配置；第 7 章介绍网络管理、网络监管的技术与配置；第 8 章介绍下一代网络技术 IPv6 协议的特点和过渡技术及配置技能。

本书既可作为高职高专计算机网络专业的教材，也可作为对计算机网络技术感兴趣的相关专业技术人员和广大自学者的参考书。

图书在版编目（CIP）数据

广域网技术精要与实践 / 蒋建峰，杜梓平编著. —北京：电子工业出版社，2017.8
（思科系列丛书）
ISBN 978-7-121-32070-5

Ⅰ. ①广… Ⅱ. ①蒋… ②杜… Ⅲ. ①广域网－高等职业教育－教材 Ⅳ. ①TP393.2

中国版本图书馆 CIP 数据核字（2017）第 154030 号

策划编辑：宋 梅
责任编辑：王敬栋
印 刷：三河市双峰印刷装订有限公司
装 订：三河市双峰印刷装订有限公司
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：10.75 字数：248 千字
版 次：2017 年 8 月第 1 版
印 次：2017 年 8 月第 1 次印刷
定 价：39.00 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

CCNA RS 较之前的 CCNA 版本有了较大的改变，本书在思科网络技术 CCNA RS 改版及 CCNA 认证考证全面更新的基础上，针对性地安排最新的内容与实验。本书是“思科系列丛书”中的一册，与作者的上一部著作《路由与交换技术精要与实践》构成 CCNA RS6.0 的完整教学内容。编著者长期从事网络技术专业的教学工作，同时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论实践一体化、充分体现技能培养的校企合作规划教材。

本书内容安排以基础性和实践性为重点，力图在讲述广域网技术相关协议工作原理的基础上，注重对学生的实践技能培养。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，与实际工程接轨，以真实设备与仿真软件相结合。

全书内容分为 8 章。

第 1 章主要介绍广域网链路封装技术 HDLC 和 PPP 的基本操作技能。

第 2 章介绍帧中继 Frame Relay 的概念和基本配置。

第 3 章主要介绍网络访问控制技术 ACL 的分类、工作原理及相关配置。

第 4 章介绍 DHCP 协议的工作原理、安全措施和配置。

第 5 章介绍了网络地址转换协议 NAT 的特点、类型及配置。

第 6 章详细介绍广域网安全主流技术 VPN 的工作原理和配置。

第 7 章介绍网络管理、网络监管的技术与配置。

第 8 章介绍下一代网络技术 IPv6 协议的特点和过渡技术及配置技能。

本教材作为苏州工业园区服务外包学院江苏省示范教材建设项目成果，由江苏省青蓝工程项目资助，全书由蒋建峰老师撰稿、修改并定稿。参加本书编写的还有杜梓平、蒋建锋、刘源等老师。特别感谢思科公司华东区经理张冉和南京建策公司培训经理吉旭对编写工作的支持。

本教材配套有教学资源 PPT 课件，如有需要，请登录电子工业出版社华信教育资源网（www.hxedu.com.cn），注册后免费下载。

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

2017 年 6 月

目　录

第1章 >>>

广域网技术

本章要点

- 广域网 WAN 概述
- HDLC 简介
- PPP 简介
- 实训一：HDLC 基本配置
- 实训二：PPP 封装与认证配置
- 实训三：MLP 配置

广域网即 WAN（Wide Area Network），是覆盖较大地理范围的数据通信网络。WAN 可能会覆盖一座城市、一个国家/地区或全球，一般情况广域网使用 ISP（Internet Service Provider）提供的传输设施传输数据。

1.1 广域网 WAN 概述

企业必须将局域网（LAN）连接到一起才能通信，而各个企业有总部、分部及远程办事处等，这些网络必须通过广域网连接到一起，企业则需要支付一定的费用来使用运营商提供的 WAN 网络服务。图 1-1 所示是一个广域网互连网络架构。

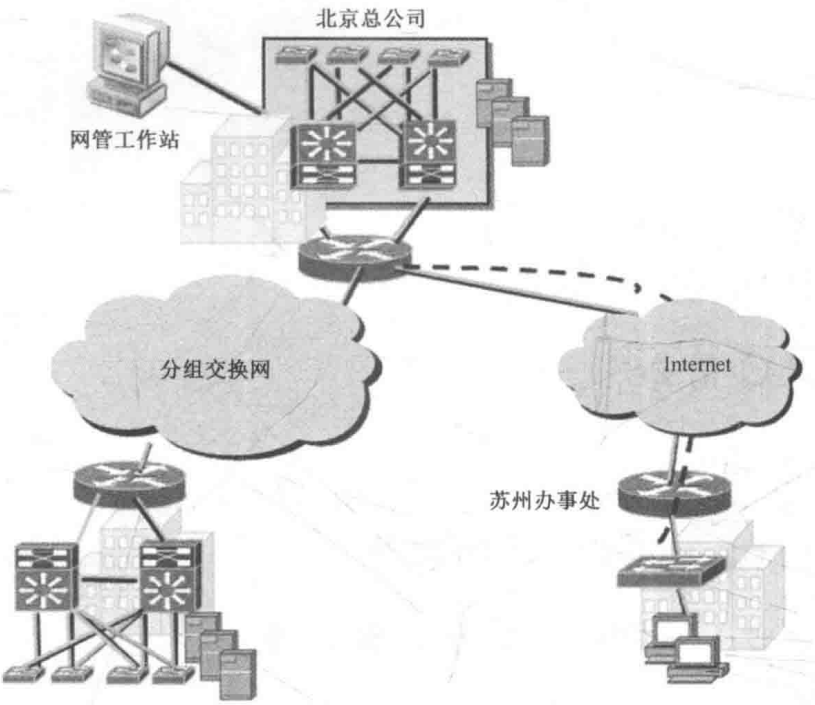

图 1-1 广域网互连架构

广域网技术中，最常见的两种数据交换技术是电路交换和分组交换。

1. 电路交换（Circuit Switching）

采用电路交换技术进行数据传输期间，在源和目的节点之间有一条利用中间节点构成的专用物理连接线路，直到数据传输结束，这条物理线路才被释放被其他通信所用。如果两个相邻节点之间的通信容量很大，那么这两个节点之间可以复用多条线路。用电路交换技术完成数据传输，需要经历电路建立、数据传输、电路拆除三个过程。

2. 分组交换（Packet Switching）

将一个报文分成若干个组，每个分组的长度有一个上限，典型长度是数千个 bit 位。有限长度的分组使每个节点所需要的存储能力降低，提高了交换速度，分组交换适用于交互式通信。

1.2　HDLC 简介

1.2.1　HDLC 协议

高级数据链路控制（HDLC，High-level Data Link Control）是一种面向比特的链路层协议，其最大特点是对任何一种比特流，均可以实现透明的传输。HDLC 协议具有以下优点。

- **透明传输**：HDLC 不依赖于任何一种字符编码集，数据报文可以实现透明传输。
- **可靠性高**：所有帧均采用 CRC 校验，对信息帧进行顺序编号，可防止漏收和重发。
- **传输效率高**：在 HDLC 中，额外的开销比特少，允许高效的差错控制和流量控制。
- **适应性强**：HDLC 规程能适应各种比特类型的工作站和链路。
- **结构灵活**：在 HDLC 中，传输控制功能和处理功能分离，层次清楚，应用非常灵活。

1.2.2　HDLC 帧格式

在 HDLC 中，数据和控制报文均以帧的标准格式传送，完整的 HDLC 的帧由标志字段（F）、地址字段（A）、控制字段（C）、信息字段（I）、帧校验字段（FCS）等组成，其格式如图 1-2 所示。

字段名称	标志F	地址A	控制C	信息I	帧校验序列 FCS	标志F
大小	1个字节 01111110	1个字节	1个字节	N个字节	2个或4个字节	1个字节 01111110

图 1-2　HDLC 帧格式

- **标志字段（F）**：标志字段为 01111110 的比特模式，用以标志帧的起始和前一帧的结束。

- **地址字段（A）**：地址字段表示链路上站的地址。在许多系统中规定，地址字段为“11111111”时，定义为全站地址，即通知所有的接收站接收有关的命令帧并按其动作；全“0”比特为无站地址，用于测试数据链路的状态。
- **控制字段（C）**：控制字段用来表示帧类型、帧编号，以及命令、响应等。HDLC 帧分为三种类型，即信息帧、监控帧、无编号帧，分别简称 I 帧（Information）、S 帧（Supervisory）、U 帧（Unnumbered）。
- **信息字段（I）**：信息字段内包含了用户的数据信息和来自上层的各种控制信息，其长度未作严格限制，目前用的比较多的是 1000～2000 bit。Cisco 设备封装的 HDLC 帧中，此字段包含了一个用于识别封装网络协议的字段 Protocol，用于支持多协议的问题。
- **帧校验序列字段（FCS）**：帧校验序列用于对帧进行循环冗余校验，其校验范围从地址字段的第 1 比特到信息字段的最后一比特的序列，并且规定为了透明传输而插入的“0”不在校验范围内。

1.3 PPP 简介

点对点（PPP，Point to Point）协议是用于在两个节点之间传送帧的协议。PPP 标准有 IETF 的 RFC 定义。PPP 是一种用于广域网的数据链路层协议，可在多种串行 WAN 中实施，可用于各种物理介质，包括双绞线、光缆、卫星传输及虚拟连接。PPP 可用于承载多种三层协议，如 IPv4、IPv6 和 IPX。

1.3.1 PPP 协议

PPP 主要包括以下协议。

- **链路控制协议（LCP，Link Control Protocol）**：用来建立、拆除和监控数据链路。
- **网络控制协议（NCP，Network Control Protocol）**：用来协商在数据链路上所传输的网络层报文的一些属性和类型。

PPP 协议的分层体系架构如图 1-3 所示。

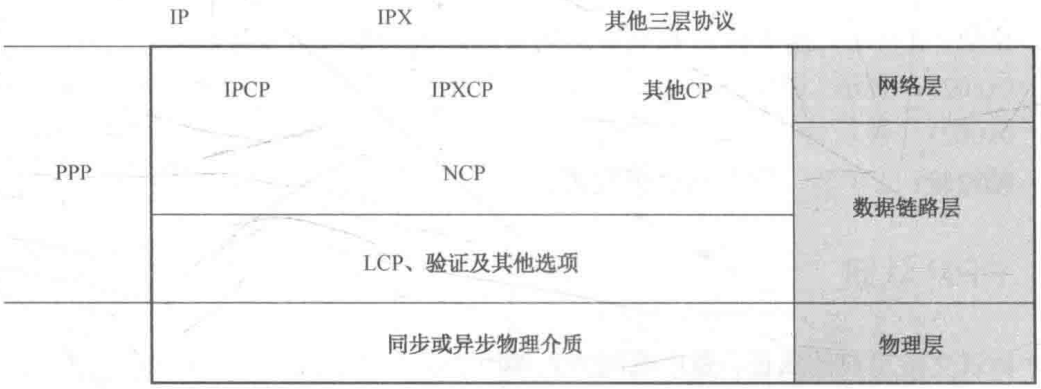

图 1-3　PPP 分层体系架构

PPP 链路的建立共有 5 个阶段，如图 1-4 所示。

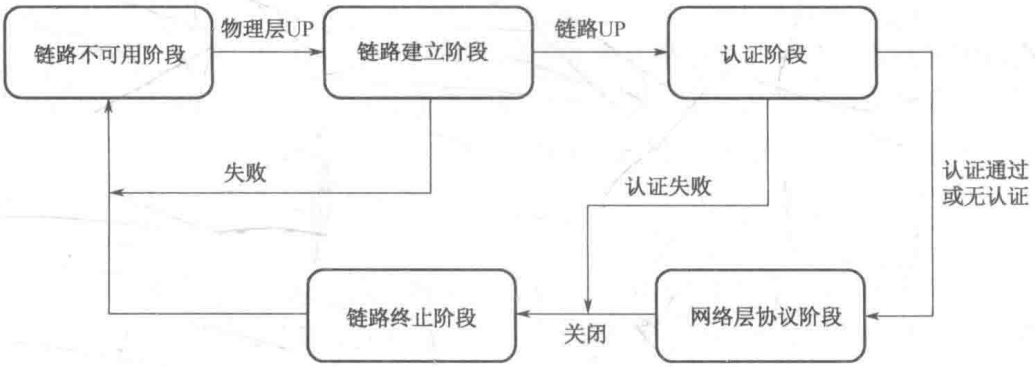

图 1-4　PPP 链路建立过程

1.3.2　PPP 帧格式

PPP 帧的格式如图 1-5 所示。

图 1-5　PPP 帧格式

- **标志**：1 字节，填充 0x7E，用来标示 PPP 帧的开始和结束。
- **地址**：1 字节，对方的数据链路层地址，因为 PPP 协议是点对点的链路层协议，所以此字节无意义，用 0xFF 填充。
- **控制**：1 字节，填充 0x03。

- 协议：2 字节，用于标志 PPP 数据帧中信息域所承载的数据报文的内容，常见取值如 0xc021，表示 LCP；0xc023，表示 PAP；0xc223，表示 CHAP；0x8021，表示 NCP；0x0021，表示 IP 协议数据报文。
- 帧校验：2 字节，用于 PPP 帧检查。

1.3.3 PPP 认证

PPP 协议支持用户的认证，是广域网接入使用的最广泛协议，目前 PPP 用的最多的两种认证是口令认证协议（PAP，Password Authentication Protocol）和质询握手认证协议（CHAP，Challenge Handshake Authentication Protocol）认证。

1. PAP 认证

PAP 为两次握手协议，它通过用户名和密码来对用户进行认证。PAP 在网络上以明文的方式传递用户名和密码，如果认证报文在传输过程中被截获，便有可能对网络安全造成威胁。因此，它适用于对网络安全要求相对较低的环境。

2. CHAP 认证

CHAP 为三次握手协议，CHAP 认证过程分为两种方式：认证方配置了用户名、认证方没有配置用户名。推荐使用认证方配置用户名的方式，这样被认证方可以对认证方的身份进行确认。CHAP 只在网络上传输用户名，并不传输用户密码（准确地讲，它不直接传输用户密码，传输的是用 MD5 算法将用户密码与一个随机报文 ID 一起计算的结果），因此它的安全性要比 PAP 高，其工作过程如图 1-6 所示。

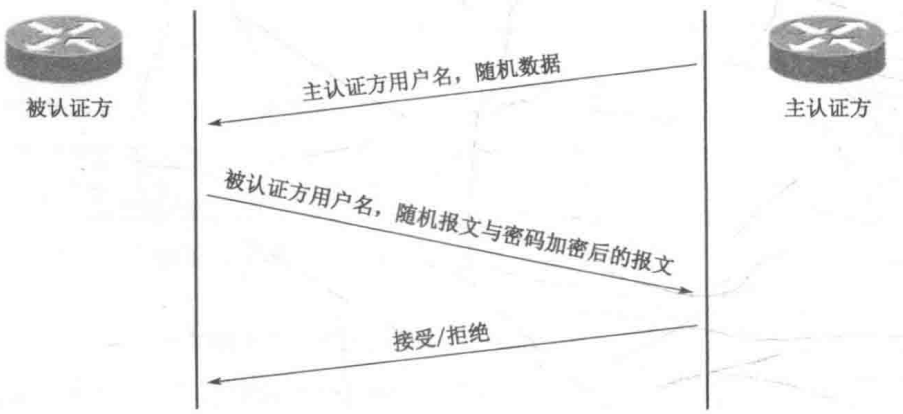

图 1-6 CHAP 认证过程

1.3.4　MLP

MLP（MultiLink PPP）可以将多条 PPP 链路捆绑起来。对于 MLP 链路两端的设备，就好像只有一条 PPP 连接，只需配置一个 IP 地址。MLP 具有以下优点。

- 增加带宽。
- 负载分担。
- 降低时延。

1.4　实训一：HDLC 基本配置

【实验目的】

- 掌握串行链路上的封装概念。
- 掌握 HDLC 封装。
- 验证配置。

【实验拓扑】

实验拓扑如图 1-7 所示。

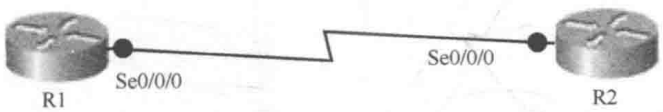

图 1-7　实验拓扑

设备参数如表 1-1 所示。

表 1-1　设备参数表

设　备	接　口	IP 地址	子网掩码	默认网关
R1	S0/0/0	192.168.12.1	255.255.255.0	N/A
R2	S0/0/0	192.168.12.2	255.255.255.0	N/A

【实验内容】

1. 配置接口封装

（1）R1 的基本配置

```
R1(config)#interface Serial0/0/0
R1(config-if)#ip address 192.168.12.1 255.255.255.0
R1(config-if)#encapsulation hdlc
//配置 HDLC 封装，思科路由器的串行接口默认是 HDLC 协议封装的
R1(config-if)#no shutdown
```

（2）R2 的基本配置

```
R2(config)#interface Serial0/0/0
R2(config-if)#ip address 192.168.12.2 255.255.255.0
R2(config-if)#encapsulation hdlc
R2(config-if)#no shutdown
```

2. 查看接口信息

```
R1#show interfaces Serial0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 192.168.12.2/24
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
//接口封装的协议是 HDLC
  Keepalive set (10 sec)
  Last input 00:00:07, output 00:00:06, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
```

```
5 minute output rate 0 bits/sec, 0 packets/sec
    15 packets input, 1584 bytes, 0 no buffer
    Received 15 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    13 packets output, 906 bytes, 0 underruns
    0 output errors, 0 collisions, 7 interface resets
    0 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out
    1 carrier transitions
    DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

1.5　实训二：PPP 封装与认证配置

1.5.1　PAP 单向认证

【实验目的】

- 掌握 PAP 单向验证配置。
- 掌握 PAP 单向验证调试。

【实验拓扑】

实验拓扑如图 1-8 所示。

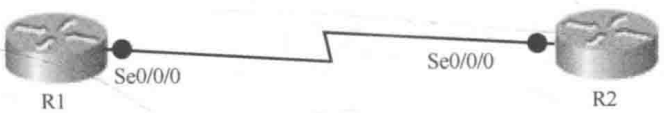

图 1-8　实验拓扑

设备参数如表 1-2 所示。

表 1-2　设备参数表

设　备	接　口	IP 地址	子网掩码	默认网关
R1	S0/0/0	192.168.12.1	255.255.255.0	N/A
R2	S0/0/0	192.168.12.2	255.255.255.0	N/A

【实验内容】

本实验配置路由器 R1（远程路由器，被验证方）被路由器 R2（中心路由器，验证方）验证。

1. 配置 PAP 单向认证

（1）R1 的基本配置

```
R1(config)#interface Serial0/0/0
R1(config-if)#ip address 192.168.12.1 255.255.255.0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp pap sent-username R1 password cisco
//配置客户端发送给中心路由器验证的用户名和密码
R1(config-if)#no shutdown
```

（2）R2 的基本配置

```
R2(config)#username R1 password cisco
//建立本地验证数据库
R2(config)#interface Serial0/0/0
R2(config-if)#clock rate 128000
R2(config-if)#ip address 192.168.12.2 255.255.255.0
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication pap
//配置 PAP 验证的主认证方
R2(config-if)#no shutdown
```

2. 实验调试

（1）查看 PPP 验证过程

```
R2#debug ppp authentication
*May 11 07:16:11.959: Se0/0/0 PPP: Authorization required
*May 11 07:16:11.963: Se0/0/0 PAP: I AUTH-REQ id 16 len 13 from "R1"
//收到用户名 R1 发送的 id 为 16、长度为 13 的验证请求
*May 11 07:16:11.963: Se0/0/0 PAP: Authenticating peer R1
//开始验证对端
*May 11 07:16:11.967: Se0/0/0 PPP: Sent PAP LOGIN Request
//发送 PAP 登录请求
```