



世纪高职高专规划教材
高等职业教育规划教材编委会专家审定

WANGLUO JIAOHUAN JI LUYOU JISHU
XIANGMU SHIXUN JIAOCHENG

网络交换及路由技术 项目实训教程

李 益 编著



北京邮电大学出版社
www.buptpress.com



21 世纪高职高专规划教材

高等职业教育规划教材编委会专家审定

网络交换及路由技术 项目实训教程

李 益 编著



北京邮电大学出版社
www.buptpress.com

内 容 简 介

在我国大力提倡“互联网+”的大背景下,互联网与社会各行各业深度融合,急需大批高素质的 IT 技术人员。本书以主要 H3C 网络设备为依托,针对网络架构概念,网络布线,以 VLAN、STP 和链路聚合等以太网交换技术,广域网,帧中继网络,DHCP 和 FTP 服务,IPv6,以 RIP 和 OSPF 为代表的路由技术,以 ACL、NAT、AAA、802.1x 为代表的网络安全技术,链路和路由备份技术等主流标准技术,采取项目驱动教学模式,由浅入深地设计编写了一系列相应的实训项目案例,帮助读者迅速、全面地提高网络组建与管理维护方面的综合技能。

本书既可作为计算机网络技术专业及其相关专业的教材,也可供需学习和了解网络的其他专业学生选读,还可作为专业技术人员对相关技术理论和实践细节进行探讨的参考用书。

图书在版编目(CIP)数据

网络交换及路由技术项目实训教程 / 李益编著. — 北京:北京邮电大学出版社,2016.9
ISBN 978-7-5635-4920-7

I. ①网… II. ①李… III. ①网络交换—高等学校—教材②路由选择—高等学校—教材 IV. ①TP393②TN913.1

中国版本图书馆 CIP 数据核字(2016)第 198925 号

书 名:网络交换及路由技术项目实训教程
著作责任者:李 益 编著
责任编辑:张珊珊
出版发行:北京邮电大学出版社
社 址:北京市海淀区西土城路 10 号(邮编:100876)
发 行 部:电话:010-62282185 传真:010-62283578
E-mail: publish@bupt.edu.cn
经 销:各地新华书店
印 刷:北京九州迅驰传媒文化有限公司
开 本:787 mm×1 092 mm 1/16
印 张:12.5
字 数:306 千字
版 次:2016 年 9 月第 1 版 2016 年 9 月第 1 次印刷

ISBN 978-7-5635-4920-7

定价:28.00 元

• 如有印装质量问题,请与北京邮电大学出版社发行部联系 •

前 言

随着互联网的出现,基于计算机技术、通信技术和信息技术的网络技术得到飞速发展。在今天,计算机网络技术已经普及应用到人们的生活、生产和商业活动中,对社会的各个领域产生了广泛而深远的影响。2015年3月,李克强总理提出制订“互联网+”行动计划,在此大背景下,社会急需大量的具备实践操作能力及解决实际问题的高素质网络技术应用人才。

作者根据自身多年丰富的教学经验,以及目前网络行业的主流认证标准要求,依托H3C网络设备为主的实训硬件背景,结合高职学生的学习特点和认知规律,因地制宜,采取项目驱动的教学模式,精心设计了一系列实训案例,编写了本实训教程,以期提高大学生尤其是高职学生网络组建与管理维护方面的综合素质,有助于学生迅速、全面地掌握相关的知识和技能。

本书编写过程中得到院系领导及网络教研室同事的大力支持,以及网络行业公司同行的热心帮助,在此表示深深的谢意。由于作者水平有限,时间仓促,本书内容如有不妥之处,敬请指正。

作 者

目 录

项目 1 配置管理网络设备	1
1.1 实训目标	1
1.2 项目背景	1
1.3 知识背景	1
1.4 实训环境	6
1.5 实训设备	6
1.6 命令列表	7
1.7 实训过程	7
实训任务一:通过 Console 登录	7
实训任务二:使用系统操作及文件操作的基本命令	11
实训任务三:通过 Telnet 登录	13
1.8 思考题	17
项目 2 简单调试网络设备	18
2.1 实训目标	18
2.2 项目背景	18
2.3 知识背景	18
2.4 实训环境	23
2.5 实训设备	24
2.6 命令列表	24
2.7 实训过程	24
实训任务一:搭建基本连接环境	24
实训任务二:检查连通性	27
实训任务三:检查数据包转发路径	27
实训任务四:练习使用察看调试信息	27
2.8 思考题	28
项目 3 制作 UTP 网线	29
3.1 实训目标	29
3.2 项目背景	29
3.3 知识背景	29

3.4	实训环境	31
3.5	实训设备	31
3.6	实训过程	32
	实训任务一:制作 UTP 线	32
	实训任务二:双绞线测试	33
3.7	思考题	34
项目 4	组建简单以太网	35
4.1	实训目标	35
4.2	项目背景	35
4.3	知识背景	35
4.4	实训环境	36
4.5	实训设备	36
4.6	命令列表	37
4.7	实训过程	37
	实训任务:配置以太网双工与速率	37
4.8	思考题	39
项目 5	组建简单的广域网	40
5.1	实训目标	40
5.2	项目背景	40
5.3	知识背景	40
5.4	实训环境	41
5.5	实训设备	41
5.6	命令列表	42
5.7	实训过程	42
	实训任务:广域网接口线缆	42
5.8	思考题	45
项目 6	组建点对点网络	46
6.1	实训目标	46
6.2	项目背景	46
6.3	知识背景	46
6.4	实训环境	48
6.5	实训设备	48
6.6	命令列表	49
6.7	实训过程	49
	实训任务一:PPP 协议基本配置	49
	实训任务二:PPP PAP 认证配置	50

实训任务三:PPP CHAP 认证配置	51
实训任务四:PPP MP 配置	53
6.8 思考题	54
项目 7 组建帧中继网络	55
7.1 实训目标	55
7.2 项目背景	55
7.3 知识背景	55
7.4 实训环境	58
7.5 实训设备	58
7.6 命令列表	58
7.7 实训过程	59
实训任务:帧中继物理接口静态映射互通配置	59
7.8 思考题	61
项目 8 划分子网	62
8.1 实训目标	62
8.2 项目背景	62
8.3 知识背景	62
8.4 实训环境	65
8.5 实训设备	65
8.6 命令列表	66
8.7 实训过程	66
实训任务:基本的 IP 网段内通信	66
8.8 思考题	68
项目 9 构建 ARP 代理	69
9.1 实训目标	69
9.2 项目背景	69
9.3 知识背景	69
9.4 实训环境	72
9.5 实训设备	73
9.6 命令列表	73
9.7 实训过程	73
实训任务一:ARP 表项观察	73
实训任务二:ARP 代理配置	75
9.8 思考题	77

项目 10 搭建 DHCP 服务器	78
10.1 实训目标	78
10.2 项目背景	78
10.3 知识背景	78
10.4 实训环境	81
10.5 实训设备	81
10.6 命令列表	81
10.7 实训过程	82
实训任务一:PCA 直接通过 RTA 获得 IP 地址	82
实训任务二:PCA 通过 DHCP 中继方式获得 IP 地址	84
10.8 思考题	85
项目 11 搭建 FTP/TFTP 服务器	86
11.1 实训目标	86
11.2 项目背景	86
11.3 知识背景	86
11.4 实训环境	89
11.5 实训设备	89
11.6 命令列表	90
11.7 实训过程	90
实训任务一:FTP 操作与分析	90
实训任务二:TFTP 操作与分析	93
11.8 思考题	95
项目 12 配置 IPv6 网络	96
12.1 实训目标	96
12.2 项目背景	96
12.3 知识背景	96
12.4 实训环境	98
12.5 实训设备	99
12.6 命令列表	99
12.7 实训过程	99
实训任务:IPv6 地址配置及查看	100
12.8 思考题	101
项目 13 配置 VLAN	102
13.1 实训目标	102
13.2 项目背景	102

13.3	知识背景	102
13.4	实训环境	105
13.5	实训设备	105
13.6	命令列表	105
13.7	实训过程	106
	实训任务一:配置 Access 链路端口	106
	实训任务二:配置 Trunk 链路端口	107
	实训任务三:配置 Hybrid 链路端口	108
13.8	思考题	110
项目 14	配置 STP	111
14.1	实训目标	111
14.2	项目背景	111
14.3	知识背景	111
14.4	实训环境	113
14.5	实训设备	113
14.6	命令列表	114
14.7	实训过程	114
	实训任务:STP 基本配置	114
14.8	思考题	116
项目 15	配置链路聚合	117
15.1	实训目标	117
15.2	项目背景	117
15.3	知识背景	117
15.4	实训环境	118
15.5	实训设备	119
15.6	命令列表	119
15.7	实训过程	119
	实训任务:交换机静态链路聚合配置	119
15.8	思考题	121
项目 16	配置静态路由	122
16.1	实训目标	122
16.2	项目背景	122
16.3	知识背景	122
16.4	实训环境	123
16.5	实训设备	124
16.6	命令列表	124

16.7 实训过程	125
实训任务一:直连路由与路由表查看	125
实训任务二:静态路由配置	126
16.8 思考题	127
项目 17 配置 RIP 网络	128
17.1 实训目标	128
17.2 项目背景	128
17.3 知识背景	128
17.4 实训环境	130
17.5 实训设备	130
17.6 命令列表	131
17.7 实训过程	131
实训任务一:配置 RIPv1	131
实训任务二:配置 RIPv2	134
17.8 思考题	136
项目 18 配置 OSPF 网络	137
18.1 实训目标	137
18.2 项目背景	137
18.3 知识背景	137
18.4 实训环境	141
18.5 实训设备	142
18.6 命令列表	142
18.7 实训过程	142
实训任务一:单区域 OSPF 基本配置	142
实训任务二:单区域 OSPF 增强配置	144
实训任务三:多区域 OSPF 基本配置	145
18.8 思考题	147
项目 19 配置包过滤防火墙	148
19.1 实训目标	148
19.2 项目背景	148
19.3 知识背景	148
19.4 实训环境	150
19.5 实训设备	151
19.6 命令列表	151
19.7 实训过程	152
实训任务一:配置基本 ACL	152

实训任务二:配置高级 ACL	153
19.8 思考题.....	155
项目 20 配置 NAT	156
20.1 实训目标.....	156
20.2 项目背景.....	156
20.3 知识背景.....	156
20.4 实训环境.....	157
20.5 实训设备.....	158
20.6 命令列表.....	158
20.7 实训过程.....	159
实训任务一:配置 Basic NAT	159
实训任务二:NAPT 配置	160
实训任务三:Easy IP 配置	161
实训任务四:NAT Server 配置	162
20.8 思考题.....	163
项目 21 配置 AAA	164
21.1 实训目标.....	164
21.2 项目背景.....	164
21.3 知识背景.....	164
21.4 实训环境.....	166
21.5 实训设备.....	166
21.6 命令列表.....	166
21.7 实训过程.....	167
实训任务:Telnet 用户本地认证、授权、计费配置	167
21.8 思考题.....	168
项目 22 实现交换机端口安全	169
22.1 实训目标.....	169
22.2 项目背景.....	169
22.3 知识背景.....	169
22.4 实训环境.....	171
22.5 实训设备.....	171
22.6 命令列表.....	171
22.7 实训过程.....	172
实训任务一:配置 802.1x	172
实训任务二:配置端口隔离	173
实训任务三:配置端口绑定	174

22.8 思考题.....	175
项目 23 配置链路备份和路由备份	176
23.1 实训目标.....	176
23.2 项目背景.....	176
23.3 知识背景.....	176
23.4 实训环境.....	178
23.5 实训设备.....	179
23.6 命令列表.....	179
23.7 实训过程.....	179
实训任务一:配置链路备份	179
实训任务二:配置路由备份	181
23.8 思考题.....	183
附录.....	184
参考文献.....	185

项目 1 配置管理网络设备

1.1 实训目标

- 学会使用 Console 线缆登录设备
- 掌握使用 Telnet 终端登录设备
- 掌握基本系统操作命令的使用
- 掌握基本文件操作命令的使用

1.2 项目背景

某公司新任网络管理员需对本公司相关网络设备(路由器、交换机)的配置数据进行熟悉和备份,并开启相关设备的 Telnet 服务以便远程管理。

1.3 知识背景

1. 网络设备

基本的网络设备有:计算机、集线器、交换机、网桥、路由器、网关、网络接口卡、无线接入点、打印机和调制解调器、光纤收发器、光缆等。虽然网络设备种类繁多,且与日俱增,但现如今,路由器和交换机依然是网络互联最主要和最关键的设备。

(1) 交换机

交换机(Switch)从网桥发展而来,属于 OSI 第二层即数据链路层设备,故也称二层设备。它可以为接入交换机的任意两个网络节点提供独享的信号通路。交换机有多个端口(如图 1-1 所示),每个端口都具有桥接功能,可以连接一个局域网或一台高性能服务器或工作站。实际上,交换机有时被称为多端口网桥。



图 1-1 交换机(H3C S3610)

从广义上来看,网络交换机分为两种:广域网交换机和局域网交换机。广域网交换机主要应用于电信领域,提供通信的基础平台。而局域网交换机则应用于局域网络,用于连接终端设备,如 PC 及网络打印机等。本书所介绍的交换机多指局域网交换机。

交换机能基于目标 MAC 地址转发信息,而不是以广播方式传输,在交换机中存储并且维护着所连计算机网卡地址和交换机端口的对应表,它对接收到的所有帧进行检查,读取帧的源 MAC 地址字段后,根据所传递的数据包的目的地,按照对应表中的内容进行转发,每一个独立的数据包都可以从源端口送到目的端口,以避免和其他端口发生冲突,对应表中如果没有对应的目的地,则转发给所有端口。由此可以看出,交换机的基本功能包括地址学习、帧的转发和过滤、环路避免,实现以太网间的透明桥接和交换。

交换机的基本功能概括如下。

- 像集线器一样,提供了大量可供线缆连接的端口,这样可以采用星形拓扑布线。
- 像中继器、集线器和网桥那样,当它转发帧时,交换机会重新产生一个不失真的电信号。
- 像网桥那样,交换机在每个端口上都使用相同的转发或过滤逻辑。
- 像网桥那样,交换机将局域网分为多个冲突域,每个冲突域都是有独立的带宽,因此可大大提高局域网的带宽。
- 还提供了更先进的功能,如虚拟局域网(VLAN)和更高的性能。

(2) 路由器

路由器(Router)工作在网络层(如图 1-2 所示),是互联网络的枢纽,可以在多个网络上



图 1-2 路由器(H3C MSR 20-40)

交换和路由数据包,路由器通过在相对独立的网络中交换具体协议的信息来实现这个目标。比起网桥,路由器不但能过滤和分割网络信息流、连接网络分支,还能访问数据包中更多的信息,并且可以提高数据包的传输效率。

路由表包含网络地址、连接信息、路径信息和发送代价等。路由器比网桥慢,主要用于广域网或广域网与局域网的互联。

目前的潮流是路由器和交换机在功能上逐渐走向融合。路由主要体现在第三层(IP)互联的功能,而交换特指以太网数据链路层的交换。现在,越来越多的路由器开始提供二层以太网交换模块与功能;交换机也不仅提供二层交换的基本功能,而增加了路由等三层功能。交换和路由的融合扩展了这两种设备的应用范围,增加了设备使用的灵活性。

2. 访问网络设备命令行接口的方法

通过 Console 口本地访问、使用 Telnet 终端访问、通过 AUX 口远程访问、使用 SSH 终端访问等多种方式均可访问网络设备命令行接口,其中 Console 本地访问和 Telnet 远程访问是较为常用的方式。

(1) 通过 Console 口本地访问

通过网络设备的 Console 口进行本地登录(如图 1-3 所示)是登录网络设备的最基本的方式,也是通过其他方式登录网络设备的前提基础,如:用户通过 Console 口登录到网络设备上后,继而可以对 AUX 用户进行相关的配置。



图 1-3 通过 Console 口本地访问

如表 1-1 所示,其中各项参数的含义如下。

- Console——翻译为“控制板”的意思,Console 控制接口是网络设备用来与计算机或终端设备进行连接的常用接口。
- 波特率——模拟线路信号的速率,也称调制速率,以波形每秒的振荡数来衡量。它是所传送代码的最短码元占有时间的倒数。例如一个代码的最短时间码元宽度为 50 ms,则其波特率就是 20 Bd/s。50 ms=0.05 s,波特率 $1/0.05=20$ Bd。
- 数据位——利用调制解调器在线路上传输数据时,每传送一组数据,都要含有相应的控制数据,包括开始发送数据、结束数据,而这组数据中最重要的是数据位。不同的通信环境下,一般规定不同的数据位和结束位数量。它的个数可以是 4、5、6、7、8 等,构成一个字符。通常采用 ASCII 码。从最低位开始传送,靠时钟定位。
- 校验方式——校验是一个冗余校验。在启动过程中的一台电脑,这使得确保计算机的数据是完整的。最简单的检错方法是“奇偶校验”,即在传送字符的各位之外,再传送 1 位奇/偶校验位。可采用奇校验或偶校验。
- 停止位——它是一个字符数据的结束标志。可以是 1 位、1.5 位、2 位的高电平。
- 流控方式(也叫数据流控制)——是用于通信设备之间管理数据流的异步通信协议。流控的信令可以用硬件(带外信令)或软件(带内信令)实现。

表 1-1 Console 口缺省配置

Console 端口属性	缺省值	Console 端口属性	缺省值
波特率(每秒位数)	9 600 bit/s	停止位	1
数据位	8	流控方式(数据流控制)	不进行流控
校验方式(奇偶校验)	无校验位		

(2) 通过 Telnet 终端访问

如图 1-4 所示,网络设备作为 Telnet 服务器,用户在主机上通过 Telnet 客户端远程登录该网络设备。由于该访问方式可通过网络远程实现,为网络管理员的远程维护提供了可能。但需注意,使用 Telnet 方式有以下几个先决条件。

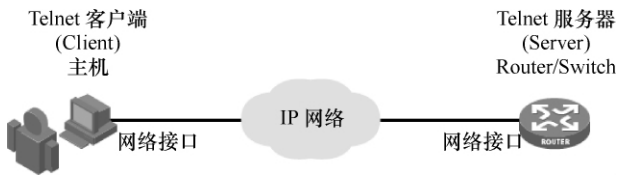


图 1-4 通过 Telnet 终端远程访问

a) 客户端与作为服务器的网络设备之间必须具备 IP 可达性,这意味着网络设备和客户端必须配置了 IP 地址,并且其中间网络必须具备正确的路由。

b) 出于安全性考虑,网络设备必须配置一定的 Telnet 验证信息,包括用户名、口令等。

c) 中间网络还必须允许 TCP 和 Telnet 协议报文通过,而不能禁止之。

当然,网络设备也可以作为 Telnet 客户端登录到其他网络设备上。

(3) 通过 AUX 口远程访问

若需调试的网络设备所在网络无法通达,还可考虑通过 AUX 口远程登录调试该设备(如图 1-5 所示),而不必让网络管理人员亲自到现场通过 Console 口登录设备进行故障排除。企业级的网络设备一般都有一个 AUX 口,其功能与 Console 口相同,但是 Console 口只能本地连接,而 AUX 口可以远程拨号连接。AUX 口一般通过电话线连接到一个外置的 Modem,维护人员利用 PSTN 网络拨号到该设备上,来实现远程维护工作。

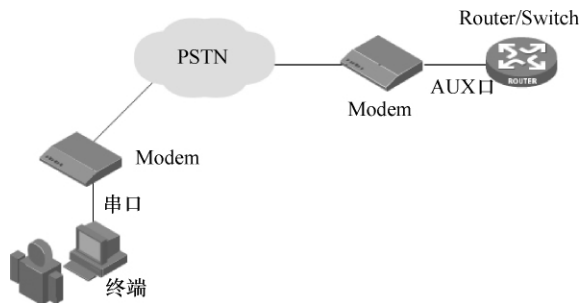


图 1-5 通过 AUX 口远程访问

(4) 使用 SSH 终端访问

使用 Telnet 远程配置网络设备时,所有的信息都是以明文的方式在网络上传输的。为了提高交互数据的安全性,可以使用 SSH(Secure Shell,安全外壳)终端进行配置(如图 1-6 所示)。用户通过一个不能保证安全的网络环境远程登录到设备时,SSH 特性可以提供安全保障和强大的验证功能,以保护设备不受诸如 IP 地址欺诈、明文密码截取等攻击。



图 1-6 使用 SSH 终端访问

SSH 是建立在应用层和传输层基础上的安全协议,由传输协议、验证协议、连接协议三部分组成。

- 传输层协议 [SSH-TRANS]

提供了服务器认证、保密性及完整性。此外它有时还提供压缩功能。SSH-TRANS 通常运行在 TCP/IP 连接上,也可能用于其他可靠数据流上。SSH-TRANS 提供了强有力的加密技术、密码主机认证及完整性保护。该协议中的认证基于主机,并且该协议不执行用户认证。更高层的用户认证协议可以设计为在此协议之上。

- 用户认证协议 [SSH-USERAUTH]

用于向服务器提供客户端用户鉴别功能。它运行在传输层协议 SSH-TRANS 上面。当 SSH-USERAUTH 开始后,它从低层协议那里接收会话标识符(从第一次密钥交换中的交换哈希 H)。会话标识符唯一标识此会话并且适用于标记以证明私钥的所有权。SSH-USERAUTH 也需要知道低层协议是否提供保密性保护。

- 连接协议 [SSH-CONNECT]

将多个加密隧道分成逻辑通道。它运行在用户认证协议上。它提供了交互式登录话路、远程命令执行、转发 TCP/IP 连接和转发 X11 连接。

SSH 使用 TCP 端口 22,提供两种验证方式。

- Password 验证

用户只要知道自己账号和口令,就可以登录到远程主机。所有传输的数据都会被加密,但是不能保证用户正在连接的服务器就是用户想连接的服务器。可能会有别的服务器在冒充真正的服务器,也就是受到“中间人”这种方式的攻击。

- Publickey 验证

该验证需要依靠密钥,先为用户创建一对密钥,并把公钥放在需要访问的服务器上;客户端软件会向服务器发出请求,请求用用户的密钥进行安全验证;服务器收到请求之后,在该服务器目录下寻找公钥,然后把它和用户发送过来的公钥进行比较。若两密钥一致,服务器就使用公钥加密“质询”(challenge)并把它发送给客户端软件;客户端软件收到“质询”之后就可以用私钥解密再把它发送给服务器。

用这种方式,用户必须知道自己密钥的口令。但是,与 Password 验证相比,Publickey 验证不需要在网络上传送口令,它不仅加密所有传送的数据,而且不易受到“中间人”攻击方式的破坏(因为攻击者没有用户的私人密钥)。

3. 队 H3C 网络设备操作系统 Comware

使用命令行配置网络设备时,每条配置和查询命令均有对应的视图,对于初学者尤其要注意命令视图的切换问题。

Comware 是 H3C 网络设备运行使用的网络操作系统,是 H3C 网络设备共用的核心软件平台。它对硬件驱动和底层操作系统进行屏蔽与封装,集成了丰富的链路层协议、以太网交换、IP 路由及转发、安全等功能模块,制定了软硬件接口标准规范,对第三方厂商提供开放平台与接口。

Comware 由上至下被分为了四大平面:管理平面、控制平面、数据平面和基础设施平面。其中:基础设施平面在操作系统的基础上提供业务运行的软件基础;数据平面提供数据报文转发功能;控制平面运行路由、MPLS、链路层、安全等各种路由、信令和 control 协议;管理平面则对外提供设备的管理接口,如命令行、SNMP 管理、WEB 管理等。此外,作为一个完整的软件系统,运行 Comware 软件的产品还有自己的驱动和对应的硬件系统,构成完整的软硬件体系结构,只不过这部分是随着产品变化的,不作为 Comware 平台化的构件的一部分。

平面之下,Comware 被进一步划分成了 25 个子系统,分别完成一部分相对独立的系统功能。这些子系统各自相对独立,又有一定的依赖关系。每个子系统又可以分解成为大小规模不同的模块。这些模块才是 Comware 系统运行的基本单元。目前 Comware 系统已经