

21

世纪高等院校计算机网络工程专业规划教材

网络设备配置项目化教程

许 军 鲁志萍 编著

可下载教学资料
<http://www.tup.tsinghua.edu.cn>

清华大学出版社

21世纪高等院校计算机网络工程专业规划教材

网络设备配置项目化教程

许 军 鲁志萍 编著

清华大学出版社
北京

内 容 简 介

本书以实际的网络环境为基础,把网络组建实际工程中所涉及的相关理论知识和操作技能分解到若干个教学项目中,每个项目包括若干任务。从基本的网络组建规划开始,通过对交换机的基本配置、网络隔离与广播风暴的控制、网络中链路的冗余备份、路由器的基本配置与远程管理、静态路由和动态路由实现网络互联、广域网协议的封装、访问控制列表的应用、利用 NAT 实现互联网的访问等项目任务的实现,使学生掌握相应的网络基础知识,具备一定的网络设备的配置调试能力。

本书适合作为高职高专计算机网络及相关专业的教材,也可以作为相关网络技术人员在实际网络设备配置调试中的技术参考用书。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

网络设备配置项目化教程/许军等编著. —北京:清华大学出版社,2012.7

(21世纪高等院校计算机网络工程专业规划教材)

ISBN 978-7-302-28557-1

I. ①网… II. ①许… III. ①计算机网络—高等学校—教材 IV. ①TP393

中国版本图书馆 CIP 数据核字(2012)第 067018 号

责任编辑:高买花 薛 阳

封面设计:常雪影

责任校对:白 蕾

责任印制:何 芊

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦 A 座 邮 编:100084

社 总 机:010-62770175 邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质 量 反 馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

课 件 下 载: <http://www.tup.com.cn>, 010-62795954

印 装 者:北京国马印刷厂

经 销:全国新华书店

开 本:185mm×260mm 印 张:20.75 字 数:507千字

版 次:2012年7月第1版 印 次:2012年7月第1次印刷

印 数:1~3000

定 价:34.00元

前 言

随着网络技术的广泛应用和不断发展,网络已经成为人们学习、工作和生活中不可缺少的一部分。小到一个家庭,大到一个企业,都有构建网络的需要。同时,社会对网络构建相关技术人员的需求也会越来越多。

本书根据高职高专院校当前普遍采用的“项目化、任务驱动”教学方式编写,内容选取上遵循“实用为主、够用为度、应用为目的、适当拓展”的基本原则,并通过对相关企业调研和相关工作职位的能力分析,尽可能地采用最新和最实用的相关网络知识。本书内容全面,从基本的网络规划到常见的网络设备的配置与调试都做了详细的介绍。

全书共有 12 个项目,项目 1 企业网络规划,主要介绍企业网络规划所需要的 IP 地址,子网划分以及常用网络测试命令的介绍;项目 2 实现企业交换机的远程管理,介绍交换机的基本配置方式及远程管理配置;项目 3 对企业各部门的网络进行隔离及广播风暴控制,介绍交换机上 VLAN 的使用;项目 4 实现企业网络中主干链路的冗余备份,介绍交换机上生成树协议(STP)及端口聚合的使用;项目 5 实现企业各部门 VLAN 之间的互联,介绍采用三层交换机和路由器实现 VLAN 之间路由的过程;项目 6 对企业路由器进行远程管理,介绍路由器的基本配置及远程管理配置;项目 7 通过路由协议实现企业总公司与分公司的联网,介绍静态路由和动态路由(RIP 和 OSPF)的配置;项目 8 在企业总公司与分公司之间进行广域网协议封装,介绍广域网协议(PPP)的封装配置;项目 9 通过路由器的设置控制企业员工的互联网访问,主要介绍访问控制列表(ACL)和网络地址转换(NAT)的使用;项目 10 构建无线局域网,介绍常用的家庭无线宽带路由器和企业无线 AP 的使用;项目 11 通过备份路由设备提供企业网络可靠性,介绍 VRRP 的基本配置;项目 12 介绍企业网络配置相关的防攻击措施,包括 DHCP 监听技术、IP 源保护技术和动态 ARP 监测技术等安全配置。

本书所有项目都能在锐捷的相关设备上实际配置测试完成,同时也提供了华为的相关命令参考,对于没有真实设备教学条件的,也可以通过思科的模拟器完成大部分的项目实训。

本书项目 1 至项目 11 由许军编写,项目 12 由鲁志萍编写。由于编者水平有限,书中难免存在疏漏和不足之处,殷切期望专家、同行和广大读者批评指正。

为了能让读者更好地理解相关命令,本书中使用的命令语法规则与产品命令参考手册中的命令语法相同。

- 方括号“[]”:表示可选项。

- 大括号“{}”：表示必选项。
- 竖线“|”：表示分隔符,用于分开可选择的选项。
- **粗体字**表示按照显示的文字输入的命令和关键字。
- *斜体字*表示需要用户输入具体的值替代。

编者

2012年3月

目 录

项目 1 企业网络规划	1
1.1 预备知识	1
1.1.1 IP 地址	1
1.1.2 子网掩码	2
1.1.3 子网划分	3
1.1.4 网关	5
1.1.5 常用网络测试命令	6
1.2 项目实施	9
任务 1: 企业网络子网划分	9
1.3 拓展知识	10
1.3.1 网络故障排除基本步骤	10
1.3.2 常用故障排除方法	10
1.3.3 思科模拟器 Packet Tracer 的基本介绍	12
1.4 项目实训	16
1.5 习题	16
项目 2 实现企业交换机的远程管理	18
2.1 预备知识	18
2.1.1 交换机的配置方式	18
2.1.2 CLI 配置方式	18
2.1.3 telnet 配置方式	24
2.1.4 交换机配置信息的保存	25
2.2 项目实施	26
任务 1: 熟悉交换机的 CLI 配置方式	26
任务 2: 配置交换机的远程 telnet 登录管理	32
2.3 拓展知识	36
2.3.1 Cisco 交换机常用 CLI 命令视图	36
2.3.2 华为交换机的常用命令视图	37

2.3.3	华为交换机的 telnet 远程登录配置	38
2.3.4	锐捷和华为相关命令的区别	38
2.4	项目实训	39
2.5	习题	39
项目 3	对企业各部门的网络进行隔离及广播风暴控制	41
3.1	预备知识	41
3.1.1	VLAN 概述	41
3.1.2	VLAN 的作用	41
3.1.3	VLAN 的划分	42
3.1.4	VLAN 数据帧	43
3.1.5	VLAN 数据帧的传输	44
3.1.6	VLAN 的端口类型	44
3.2	项目实施	45
任务 1:	给公司各个部门划分 VLAN	45
任务 2:	同一部门用户跨交换机的访问控制	50
3.3	拓展知识	54
3.3.1	PVLAN	54
3.3.2	华为的相关命令	59
3.4	项目实训	61
3.5	习题	62
项目 4	实现企业网络中主干链路的冗余备份	64
4.1	预备知识	64
4.1.1	生成树协议概述	64
4.1.2	生成树协议的工作过程	67
4.1.3	生成树协议的缺陷	71
4.1.4	快速生成树协议	71
4.1.5	多生成树协议	71
4.1.6	端口聚合	72
4.2	项目实施	73
任务 1:	生成树配置	73
任务 2:	快速生成树配置	76
任务 3:	端口聚合配置	79
4.3	拓展知识	82
4.3.1	网桥协议数据单元	82
4.3.2	STP 计时器	83

4.3.3	STP 端口状态	83
4.3.4	RSTP 端口状态和端口角色	84
4.3.5	RSTP 快速收敛原理	84
4.3.6	MSTP	84
4.3.7	华为的相关命令	85
4.4	项目实训	89
4.5	习题	90
项目 5	实现企业各部门 VLAN 之间的互联	92
5.1	预备知识	92
5.1.1	VLAN 间路由	92
5.1.2	理解三层接口	93
5.1.3	用路由器实现 VLAN 间路由(单臂路由)	93
5.1.4	三层交换机实现 VLAN 间路由	95
5.2	项目实施	96
任务 1:	利用三层交换机实现 VLAN 间互访	96
任务 2:	利用路由器实现 VLAN 间互访(单臂路由)	98
5.3	拓展知识	100
5.3.1	接口类型	100
5.3.2	子接口	101
5.3.3	华为的相关命令	101
5.4	实训项目	103
5.5	习题	104
项目 6	对企业路由器进行远程管理	106
6.1	预备知识	106
6.1.1	路由器	106
6.1.2	路由器的工作流程	106
6.1.3	路由器结构	108
6.1.4	路由器的基本配置方式	108
6.1.5	路由器的 CLI 配置界面	108
6.1.6	路由器远程 telnet 登录配置	112
6.2	项目实施	113
任务 1:	熟悉路由器的基本操作	113
任务 2:	配置路由器的 telnet 远程登录	117
6.3	拓展知识	121
6.3.1	路由器的接口类型	121

6.3.2	华为路由器的相关设置	121
6.3.3	路由器或交换机系统的升级	122
6.3.4	利用 IIS 架设 FTP 服务器	129
6.4	项目实训	131
6.5	习题	131
项目 7	通过路由协议实现企业总公司与分公司的联网	133
7.1	预备知识	133
7.1.1	路由的概念	133
7.1.2	路由的类型	134
7.1.3	路由表	134
7.1.4	路由的匹配原则	136
7.1.5	静态路由	136
7.1.6	RIP 路由协议	137
7.1.7	OSPF 路由协议	141
7.1.8	路由重分发	144
7.2	项目实施	145
	任务 1: 利用静态路由实现总公司与分公司的网络互访	145
	任务 2: 利用 RIP 动态路由实现总公司与分公司的网络互访	150
	任务 3: 利用 OSPF 动态路由实现总公司与分公司的网络互访	156
	任务 4: 利用路由重分布实现总公司与分公司的网络互访	161
7.3	拓展知识	168
7.3.1	路由环路	168
7.3.2	路由环路的解决方法	169
7.3.3	路由黑洞	170
7.3.4	有类别路由协议与无类别路由协议	171
7.3.5	浮动静态路由	171
7.3.6	华为的相关命令	172
7.4	项目实训	178
7.5	习题	179
项目 8	在企业总公司与分公司之间进行广域网协议封装	181
8.1	预备知识	181
8.1.1	广域网	181
8.1.2	PPP 简介	183
8.1.3	PPP 的协商过程	184
8.1.4	PPP 的验证	184

8.2	项目实施	188
	任务 1: 配置广域网链路 PPP 封装	188
	任务 2: 配置广域网链路 PAP 验证	190
	任务 3: 配置广域网链路 CHAP 验证	192
8.3	拓展知识	193
	8.3.1 WAN 接入技术	193
	8.3.2 华为的相关命令	196
8.4	项目实训	198
8.5	习题	200
项目 9	通过路由器的设置控制企业员工的互联网访问	202
9.1	预备知识	202
	9.1.1 访问控制列表概述	202
	9.1.2 标准 IP 访问控制列表	207
	9.1.3 扩展 IP 访问控制列表	207
	9.1.4 基于时间的访问控制列表	207
	9.1.5 配置访问控制列表的步骤	207
	9.1.6 NAT 概述	207
	9.1.7 NAT 的工作过程	209
	9.1.8 静态 NAT	210
	9.1.9 动态 NAT	211
	9.1.10 端口复用 NAT	212
9.2	项目实施	213
	任务 1: 标准 IP 访问控制列表的应用	213
	任务 2: 扩展 IP 访问控制列表的应用	218
	任务 3: 基于时间的访问控制列表的应用	220
	任务 4: 静态 NAT 的应用	224
	任务 5: 动态 NAT 的应用	226
9.3	拓展知识	228
	9.3.1 基于 MAC 的 ACL	228
	9.3.2 专家 ACL	230
	9.3.3 地址空间重叠的网络处理	230
	9.3.4 TCP 负载均衡	232
	9.3.5 华为设备的相关命令	232
9.4	项目实训	239
9.5	习题	240

项目 10 构建无线局域网	242
10.1 预备知识	242
10.1.1 WLAN 的技术背景	242
10.1.2 802.11 协议	245
10.1.3 WLAN 组件	246
10.1.4 WLAN 拓扑结构	249
10.2 项目实施	250
任务 1: 利用家用无线宽带路由构建家庭或办公室小型无线局域网	250
任务 2: 利用企业级无线产品(AP+AC)构建无线网络	258
10.3 拓展知识	273
10.3.1 无线网卡与无线上网卡的区别	273
10.3.2 802.11 网络基本元素	273
10.3.3 WLAN 的安全	274
10.4 项目实训	275
10.5 习题	276
项目 11 通过备份路由设备提供企业网络可靠性	278
11.1 预备知识	278
11.1.1 VRRP 概述	278
11.1.2 VRRP 选举	280
11.1.3 VRRP 的应用模式	281
11.1.4 VRRP 接口跟踪	282
11.1.5 VRRP 抢占模式	282
11.2 项目实施	283
任务 1: 配置 VRRP 单组备份提高网络可靠性	283
任务 2: 配置多组 VRRP 进行负载均衡	287
11.3 拓展知识	289
11.3.1 VRRP 报文	289
11.3.2 VRRP 定时器	290
11.3.3 VRRP 验证	290
11.3.4 华为的相关命令	290
11.4 项目实训	292
11.5 习题	294
项目 12 对企业网络配置相关的防攻击措施	296
12.1 预备知识	296

12.2	项目实施	307
	任务 1: 配置透明模式防火墙	307
	任务 2: 配置路由模式防火墙	309
12.3	拓展知识	312
	12.3.1 DHCP 攻击	312
	12.3.2 IP 地址欺骗及 IP 源防护技术简介	314
	12.3.3 ARP 攻击及 ARP 检测技术简介	314
12.4	项目实训	315
12.5	习题	316
	习题部分答案参考	318
	参考文献	320

项目描述

利用保留的 C 类网络号对企业网络进行子网划分,要求划分的子网数为 6 个,确定子网掩码、每个子网的有效 IP 地址范围和广播地址。

项目目标

- 了解 IP 地址的组成
- 了解子网掩码的作用
- 掌握子网的划分
- 掌握常用网络测试命令

1.1 预备知识

1.1.1 IP 地址

1. IP 地址的定义

IP 地址就是给每个连接到互联网中的计算机分配的一个 32 位的地址。如果把互联网中计算机相互传递信息的过程看成生活中进行邮寄信件的过程,IP 地址就好比是家庭住址,邮寄信件时,邮递员需要知道唯一的家庭住址才能准确地把邮件送到,同样,互联网中的计算机为了能相互正常通信,IP 地址在互联网中也是唯一的。

2. IP 地址的组成

按照 TCP/IP 协议规定,IP 地址用二进制来表示,每个 IP 地址长 32 位,例如一个采用二进制形式的 IP 地址是“11000000 10101000 00000001 00000001”,由于二进制形式的 IP 地址太长,人们不容易记忆和处理,所以 IP 地址经常采用“点分十进制表示法”,即将组成计算机的 IP 地址的 32 位二进制分成 4 段,每段 8 位,中间用小数点隔开,然后将每 8 位二进制转换成十进制数,上面的二进制形式的 IP 地址采用点分十进制表示法为“192.168.1.1”。

从另外一个角度来讲,32 位的 IP 地址可以分成两个部分,一部分为网络地址(即网络号);另一部分为主机地址(即主机号),如图 1-1 所示。

3. 公有地址和私有地址

公有地址是在因特网中可以直接使用的 IP 地址,这些地址由 Inter NIC (Internet Network

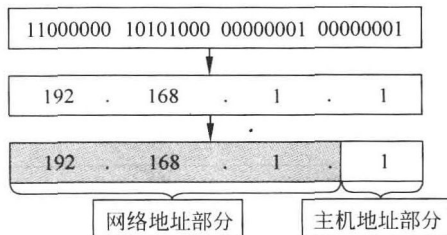


图 1-1 IP 地址的组成

Information Center, 因特网信息中心)负责分配给注册并向 Inter NIC 提出申请的组织机构。

私有地址属于非注册地址,专门用于局域网内部,而不能直接用于因特网中。留用的内部私有地址有:

A 类 10.0.0.0~10.255.255.255

B 类 172.16.0.0~172.31.255.255

C 类 192.168.0.0~192.168.255.255

4. 广播地址和网络地址

广播地址和网络地址是两个比较特殊的 IP 地址。IP 地址中主机地址部分全为 0 的为网络地址,它用来描述一个网段,例如:192.168.1.0。IP 地址中主机地址部分全为 1 的为广播地址,用于对网段内所有的主机广播,例如:192.168.1.255。

1.1.2 子网掩码

IP 地址由网络号和主机号两部分组成,那么在一个 IP 地址中有多少位是网络号,而又有多少位是主机号呢?这个可以通过子网掩码来确定。子网掩码不能独立存在,它必须结合 IP 地址一起使用。

1. 子网掩码的格式

子网掩码跟 IP 地址类似,也是由 32 位二进制数组成,也采用点分十进制来表示(在与 IP 地址一起书写时也经常采用子网掩码中二进制数“1”的位数来表示,例如:192.168.1.1/24 相当于 192.168.1.1 255.255.255.0)。跟 IP 地址不同的是,子网掩码中的二进制数“1”和“0”是分别连续的。左边连续的二进制数“1”对应的是网络号的位数;右边连续的二进制数“0”对应的是主机号的位数。

2. 子网掩码的作用

子网掩码的作用有两个:一是识别 IP 地址中的网络号和主机号;二是进行子网划分。

通过 IP 地址的二进制与子网掩码的二进制进行与运算,可以确定某个 IP 地址的具体的网络号和主机号。如果两个 IP 地址在子网掩码的按位与运算下所得结果相同(即网络号相同),那么表示这两个 IP 地址是在同一个子网中。

例如:IP 地址是 202.10.113.24,对应的子网掩码是 255.255.255.0。

十进制 IP 地址	202	10	113	24
二进制 IP 地址	11001010	00001010	01110001	00011000
子网掩码	11111111	11111111	11111111	00000000
AND 运算	11001010	00001010	01110001	00000000

网络号为:202.10.113.0

主机号为:0.0.0.24

例如:IP 地址是 120.12.1.2,对应的子网掩码是 255.255.0.0。

十进制 IP 地址	120	12	1	2
二进制 IP 地址	01111000	00001100	00000001	0000010
子网掩码	11111111	11111111	00000000	0000000
AND 运算	01111000	00001100	00000000	0000000

网络号为：120.12.0.0

主机号为：0.0.1.2

A类地址的默认子网掩码为：255.0.0.0。

B类地址的默认子网掩码为：255.255.0.0。

C类地址的默认子网掩码为：255.255.255.0。

1.1.3 子网划分

随着互联网应用的不断扩大,原先的 IPv4 的弊端也逐渐暴露出来,即网络号占位太多,而主机号位太少,所以其能提供的主机地址也越来越稀缺,目前除了使用 NAT 在企业内部利用私有地址自行分配以外,通常都对一个高类别的 IP 地址进行再划分,以形成多个子网,提供给不同规模的用户群使用。

子网划分实际上就是通过改变原有的子网掩码长度来改变原有网络规模的大小。子网划分能把原先一个大的网络划分成多个小的网络(增加子网掩码中“1”的位数),同样也可以把多个小的网络合并成一个大的网络(减少子网掩码中“1”的位数)。

1. 标准子网划分

标准子网划分就是在改变子网掩码长度时是按照 A/B/C 默认的掩码长度来改变的。

例如：一个 A 类的 IP 地址 10.10.10.1, 默认的子网掩码长度是 255.0.0.0, 这个 IP 地址所属的网络号是 10.0.0.0/8, 这时可以通过改变子网掩码长度为 255.255.0.0 来缩小网络的规模。同时也将 10.0.0.0/8 这个大的网络划分成 256 个小的网络：10.0.0.0/16~10.255.0.0/16。

	网络号	子网掩码
划分前的网络	10.0.0.0	255.0.0.0
划分后的网络	10.0.0.0	255.255.0.0
	10.1.0.0	255.255.0.0
	10.2.0.0	255.255.0.0

	10.254.0.0	255.255.0.0
	10.255.0.0	255.255.0.0

例如：一个 C 类的 IP 地址 192.168.1.1, 默认的子网掩码长度是 255.255.255.0, 这个 IP 地址所属的网络是 192.168.1.0/24, 这时可以通过改变子网掩码长度为 255.255.0.0 来扩大网络的规模。同时也将 256 个 C 类网络(192.168.0.0/24~192.168.255.0/24)合并成一个大的网络 192.168.0.0/16。

	网络号	子网掩码
划分前的网络	192.168.1.0	255.255.255.0
	192.168.2.0	255.255.255.0
	192.168.3.0	255.255.255.0

	192.168.254.0	255.255.255.0
	192.168.255.0	255.255.255.0
划分后的网络	192.168.0.0	255.255.0.0

2. 非标准子网的划分

非标准子网的划分相对标准子网的划分要复杂一些。但只要掌握基本方法后,也可以很容易实现。非标准子网是指子网掩码的长度不再是默认的 8/16/24 这三个位数,也有可能是其他的长度(例如:17 位,9 位等)。所以进行子网划分的关键就是如何确定子网掩码的长度。当把一个大的网络号划分成多个小的网络时,需要把原来主机号部分再次划分成子网号和新的主机号,由原来的网络号部分和子网号组成新的网络号。新的网络号的位数就是子网掩码的长度,如图 1-2 所示。



图 1-2 非标准子网划分

例如:某公司有 4 个部门,A 部门有 15 台 PC,B 部门有 20 台 PC,C 部门有 25 台 PC,D 部门有 10 台 PC,现在有一个 C 类地址 192.168.10.0/24,如何给每个部门划分单独的网段?

分析:首先每个部门要有一个单独的网段,公司有 4 个部门,所以需要至少划分 4 个子网。在知道子网数的前提下,可以通过公式 $2^n \geq m$ (n 为子网号的位数, m 为子网数)来求得子网号的位数。根据上面的公式计算,此时的子网号的位数 $n=2$ 。所以从原有的主机号中取出最高的两位用做子网号,跟原来的网络号组成新的网络号。新的子网掩码长度就是 $24+2=26$ 位,如图 1-3 所示。

划分前网络号	11000000 . 10101000 . 00001010 . 00 000000
	192 . 168 . 10 . 0
划分前子网掩码	11111111 . 11111111 . 11111111 . 00 000000
	255 . 255 . 255 . 0
划分后子网掩码	11111111 . 11111111 . 11111111 . 11 000000
	255 . 255 . 255 . 192

图 1-3 子网划分前后的子网掩码

知道新的子网掩码长度(即新的网络号位数)后,就可以写出划分后的不同子网的网络号,每个子网的可用 IP 地址范围(每个子网的可用 IP 地址的数量可通过公式 $2^n - 2 = m$ 求得, n 为主机号位数, m 为可用的 IP 地址数量)及每个子网的广播地址,如图 1-4 所示。

子网 1 的可用 IP 地址范围为 192.168.10.1~192.168.10.62;广播地址为 192.168.10.63,如图 1-5 所示。

子网 2 的可用 IP 地址范围为 192.168.10.65~192.168.10.126;广播地址为 192.168.10.127。

子网 3 的可用 IP 地址范围为 192.168.10.129~192.168.10.190;广播地址为 192.168.10.191。

划分前网络号	11000000 . 10101000 . 00001010 . 00 000000
	192 . 168 . 10 . 0 /255.255.255.0
划分后子网1网络号	11000000 . 10101000 . 00001010 . 00 000000
	192 . 168 . 10 . 0 /255.255.255.192
划分后子网2网络号	11000000 . 10101000 . 00001010 . 01 000000
	192 . 168 . 10 . 64 /255.255.255.192
划分后子网3网络号	11000000 . 10101000 . 00001010 . 10 000000
	192 . 168 . 10 . 128 /255.255.255.192
划分后子网4网络号	11000000 . 10101000 . 00001010 . 11 000000
	192 . 168 . 10 . 192 /255.255.255.192

图 1-4 划分后的子网网络号

子网1网络号	11000000 . 10101000 . 00001010 . 00 000000	此为子网1网络号
	192 . 168 . 10 . 0 /255.255.255.192	
192.168.10.1	11000000 . 10101000 . 00001010 . 00 000001	此为子网1广播地址
192.168.10.2	11000000 . 10101000 . 00001010 . 00 000010	
192.168.10.3	11000000 . 10101000 . 00001010 . 00 000011	
...	11000000 . 10101000 . 00001010 . 00 ...	
192.168.10.62	11000000 . 10101000 . 00001010 . 00 111110	
192.168.10.63	11000000 . 10101000 . 00001010 . 00 111111	

图 1-5 子网 1 的 IP 地址范围

子网 4 的可用 IP 地址范围为 192.168.10.193~192.168.10.254；广播地址为 192.168.10.255。

1.1.4 网关

按照不同的分类标准,网关有很多种,有协议网关、应用网关、传输网关、安全网关等。在这里所讲的“网关”均指 TCP/IP 协议下的网关。那么网关到底是什么呢?简单地说,网关就是一个网络连接到另外一个网络的“关口”。网关实质上是一个网络通向其他网络的 IP 地址。如图 1-6 所示,有网络 A 和网络 B,网络 A 的 IP 地址范围为 192.168.1.1~192.168.1.254,子网掩码为 255.255.255.0;网络 B 的 IP 地址范围为 192.168.2.1~192.168.2.254,子网掩码为 255.255.255.0。在没有路由器的情况下,两个网络之间是不能进行 TCP/IP 通信的,即使是两个网络连接在同一台交换机(或集线器)上,TCP/IP 协议也会根据子网掩码(255.255.255.0)判定两个网络中的主机处在不同的网络里。而要实现这两个网络之间的通信,则必须通过网关。如果网络 A 中的主机发现数据包的目的主机不在本地网络中,就把数据包转发给它自己的网关,再由网关转发给网络 B 的网关,网络 B 的网关再转发给网络 B 的某个主机。

默认网关的意思是一台主机如果找不到可用的网关,就把数据包发给默认指定的网关,