

# 基于 Packet Tracer 的小型企业网络应用架构的仿真实验

张梁斌, 高 昆, 梁世斌

(浙江万里学院 计算机与信息学院 浙江 宁波 315100)

**摘 要:** 网络模拟器能完成组网、设备配置及验证的实验仿真,利用 Cisco 模拟器 Packet Tracer5.3 构建了一个典型的小型企业网络应用架构。主要涉及交换机的 DHCP、VLAN、RIP,路由器的 RIP、NAT、ACL 包过滤,和服务器 WEB、FTP、MAIL 及层次结构 DNS 等综合配置和仿真验证,实验结果内容详实且模拟逼真。该教学案例具备很好的通用性,有助于提高学生的网络工程综合配置和集成的能力。

**关键词:** Packet tracer5.3; 企业网络; 仿真实验

中图分类号: TP 391.9

文献标志码: A

文章编号: 1006-7167(2012)10-0372-05

## Simulation Experiment of Small Enterprise Network Application Infrastructure Based on Packet Tracer

ZHANG Liang-bin, GAO Kun, LIANG Shi-bin

(Computer Science and Information Technology College, Zhejiang Wanli University, Ningbo 315100, China)

**Abstract:** This paper puts forward a typical small enterprise network application architecture using Cisco simulator Packet Tracer5.3, which mainly concerns integrated configuration and simulation verification including switch technology of DHCP, VLAN and RIP, router technology of RIP, NAT and ACL packet filtering, and server technology of WEB, FTP, MAIL and level structure DNS with detailed and realistic experimental results. This simulation experiment has good universality, which can greatly improve student's ability of network configuration and integration.

**Key words:** Packet Tracer5.3; enterprise network; simulation experiment

## 0 引 言

在计算机网络技术教学中,实验实训是学生获取网络知识和技能的必要环节,而传统网络实验中,网络设备的匮乏、大量设备的拔插及网线的连接等都会影响实验效果<sup>[1-2]</sup>。在网络教学中引入虚拟网络平台,既可减少实验投资成本,又能提高学生实验动手能力,已成为目前学习和掌握网络技术的一种趋势<sup>[3-4]</sup>。

Packet tracer 5.3 是 Cisco 提供的一款网络模拟器,几年来引入到我院计算机网络工程的课程实验教学中,受到了学生的热捧。学生使用该模拟器能自己

设计和搭建网络拓扑图,完成对设备的配置和验证,而且还能看到数据包的格式及在网络运行的动画过程,为学生学习网络插上了飞翔的翅膀<sup>[5-9]</sup>。结合 Packet tracer 5.3 给出了一个典型的小型企业网络架构,涉及交换机和路由器的综合配置(DHCP、VLAN、RIP、NAT、ACL)及服务器 WEB、FTP、MAIL 和层次结构 DNS 配置等,该案例融合了诸多的网络应用,达到了良好的教学效果。

## 1 网络功能需求和拓扑图设计

通过调研部分企事业单位,借鉴已有的网络工程教学案例<sup>[10-13]</sup>,图1给出了一个典型的小型企业网络应用的架构模型。

本设计案例的架构模型集成了相关网络配置命令,具备了以下的功能:

(1) 小型企业的内网划分三个 VLAN。VLAN10 和 VLAN20 为两个部门用户,通过 DHCP 分配能自动获取 IP 信息;VLAN30 为企业内网服务器群,提供企

收稿日期: 2012-03-12

基金项目: 浙江省本科计算机教指委教改项目(2010-6),浙江省公益性技术应用研究计划项目(2011C31005)

作者简介: 张梁斌(1976-),男,浙江宁波人,硕士,副教授,研究方向: 图像处理、网络与信息安全。

Tel.: 0574-88222086, 15990598905; E-mail: zlb@zww.edu.cn

业内网用户的 DNS、Web、FTP、Mail 常用服务和公网用户的 Web 访问,VLAN 之间通过三层交换机 S3560-24PS 实现互连互通。

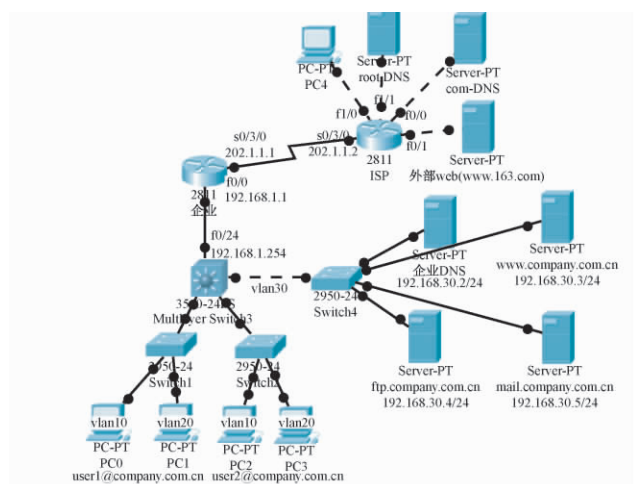


图1 基于 PT5.3 的小型企业网络应用架构

(2) 园区网在组网中常采用3层网络架构。即接入层、汇聚层和核心层<sup>[14]</sup>。小型企业由于部门少、规模小等特点,本案例使用接入层和核心层的二层网络架构。接入层由二层交换机 S2950-24 组成,有效控制用户的网络物理连入,主要功能是隔离广播流量。核

心层由三层交换机 S3560-24PS 组成,主要提供高带宽的内网之间、内外网之间的可靠数据传输。

(3) 出口路由器 Router 2811 配置 NAT 技术。允许授权的内网用户访问公网资源,也允许公网用户访问部分内网的服务资源,实现局域网与 Internet 互访;同时在出口路由器 Router 2811 上设置 ACL 包过滤策略,防止公网用户的非法攻击。

(4) ISP 路由器 Router 2811 连接公网上的信息资源。模拟 DNS 根域,二级域,以及公网上客户机和 Web 站点,用于内网和公网之间的相互访问测试。

## 2 网络设备的详细配置

网络模拟器 PT5.3 完成网络设备的选型、拖放和连线后,可进行网络设备的具体命令配置。PT5.3 支持命令粘贴功能,建议先把命令行写在 TXT 记事本上,然后直接在设备的 IOS 中复制和粘贴<sup>[15]</sup>。这种配置方法有二个好处:①能快速执行配置命令,命令集合以批处理方式在网络上快速执行;②方便学生检查原来的配置命令,有利于对设备命令的调试和改进。表1给出了拓扑图中网络设备及端口分配的信息。下面依次给出网络设备的主要配置命令,并做必要的阐述说明。

表1 网络设备及端口分配

位置	设备	端口及 ip 地址分配	备注	设备	端口及 ip 地址分配	备注
企业内部	Router 2811	f0/0: 192.168.1.1/24	连接内网	S3560	f0/24: 192.168.1.254/24	连接出口路由器
		s0/3/0: 202.1.1.1/24	连接 ISP		f0/1: 不分配 IP	连接 S1 的 f0/24
	S2950_1	f0/1 f0/13: 不分配 ip	分别接 pc0 和 pc1		f0/2: 不分配 IP	连接 S2 的 f0/24
		f0/24: 不分配 ip	连接 S3 的 f0/1		f0/3: 不分配 IP	连接 S4 的 f0/24
		f0/1 f0/13: 不分配 ip	分别接 pc2 和 pc3	S2950_4	f0/24: 不分配 ip	连接 S3 的 f0/3
		f0/24: 不分配 ip	连接 S3 的 f0/2		f0/1: 不分配 ip	连接企业 DNS
	服务器群	DNS、Web、FTP、Mail	网关为 192.168.30.1		f0/2: 不分配 ip	连接企业 Web
		Server 的地址依次为 192.168.30.2-5/24			f0/3: 不分配 ip	连接企业 FTP
					f0/4: 不分配 ip	连接企业 Mail
					Pc0-Pc3	自动获取 vlan10 和 vlan 20 的 IP 地址
ISP	Router 2811	s0/3/0: 202.1.1.2/24	公网 ip 地址		f1/1: 202.5.5.1/24	连接公网 root dns
		f1/0: 202.4.4.1/24	接公网测试用户		f0/0: 202.2.2.1/24	接公网 com dns
					f0/1: 202.3.3.1/24	接公网 163 站点

### 2.1 接入层交换机的配置

接入层交换机做基于端口的 VLAN 划分,主要用于隔离广播域。下面给出 S1 的主要配置命令,S2 的配置命令类似,不再重复给出。

```
S1( config) #vlan 10 //新建 vlan 10
S1( config) #interface range f
0/12 -23 //进入组端口
S1( config-vlan) #exit
S1( config-if-range) #switchport access vlan
```

20

```
S1( config) #vlan 20 //新建 vlan20
S1( config-if-range) #exit
S1( config-vlan) #exit
S1( config) #interface f0/24 //进入 f0/24 端口
S1( config) #interface range f 0/1 -11 //进入组端口
S1( config-if) #switchport mode trunk //设 trunk 模式
S1( config-if-range) #switchport access vlan 10
S1( config-if) #end
```

S1( config-if-range) #exit S1#copy run start //保存配置

## 2.2 核心交换机的配置

交换机 S3560 需要完成不同 VLAN 的 DHCP 分配、VLAN 间路由、自治系统内 RIP 协议配置等, 主要提供高带宽的内网之间、内网和公网之间数据传输。下面给出 S3 的主要配置命令。

```
S3( config) #vlan 10 S3( config-if) #ip add 192. 168. 20. 1
255. 255. 255. 0
S3( config-vlan) #exit S3( config-if) #no shut
S3( config) #vlan 20 S3( config-if) #inter vlan 30
S3( config-vlan) #exit S3( config-if) #ip add 192. 168. 30. 1 255.
255. 255. 0
S3( config) #vlan 30 S3( config-if) #no shut //设置 3 个 SVI 口
S3( config-vlan) #exit S3( config) #inter range f 0/1 -2
S3( config) #inter vlan 10 S3( config-if-range) #switchport mode
trunk
S3( config-if) #ip add 192. 168. 10. 1 255. 255. 255. 0 //端口为
trunk
S3( config-if) #no shut //设置 SVI 虚拟接口并启动 S3( config-
if-range) #inter f 0/3
S3( config-if) #inter vlan 20 S3( config-if) #switchport access vlan
30
S3( config-if) #inter f 0/24 S3( dhcp-config) #network 192. 168.
20. 0
S3( config-if) #no switchport //关闭交换端口 255. 255. 255. 0
S3( config-if) #ip add 192. 168. 1. 252 255. 255. 255. 0 S3( dhcp-
config) #exit //以上设置 DHCP 分配
S3( config-if) #no shut //启动 f0/24 为路由端口 S3( config) #ip
dhcp excluded-address 192. 168. 10. 1
S3( config-if) #exit S3( config) #ip dhcp excluded-address 192.
168. 20. 1
S3( config) #ip dhcp pool vlan10 //创建 dhcp 地址池 //排除
SVI 的 2 个 IP
S3( dhcp-config) #dns-server 192. 168. 30. 2 S3( config) #router
rip
//设置 vlan10 的 dns 地址 S3( config-router) #version 2
S3( dhcp-config) #default-router 192. 168. 10. 1 S3( config-
router) #no au
//设置 vlan10 的网关地址 S3( config-router) #network 192.
168. 10. 0
S3( dhcp-config) #network 192. 168. 10. 0 255. 255. 255. 0 //设置
vlan10 的掩码地址 S3( config-router) #network 192. 168. 20. 0
S3( dhcp-config) #exit S3( config-router) #network 192. 168. 30. 0
S3( config) #ip dhcp pool vlan20 S3( config-router) #network 192.
168. 1. 0
S3( dhcp-config) #dns-server 192. 168. 30. 2 S3( config-router) #
end //以上配置 RIP 协议
S3( dhcp-config) #default-router 192. 168. 20. 1 S3#copy run start
//保存配置
```

## 2.3 出口路由器的配置

借助 NAT 技术, 出口路由器需要完成内网用户访

问公网资源和公网用户访问内网资源; 借助 ACL 策略, 出口路由器可防止公网非法用户对内网的蓄意攻击, 同时还要设置 RIP 和默认路由等。以下是出口路由器的主要配置信息。

```
R2811( config) #inter f0/0
R2811( config-if) #ip add 192. 168. 1. 1 255. 255. 255. 0
R2811( config-if) #no shutdown
R2811( config-if) #ip nat inside //指定为 NAT 内端口
R2811( config-if) #inter s0/3/0
R2811( config-if) #ip add 202. 1. 1. 1 255. 255. 255. 0
R2811( config-if) #no shutdown
R2811( config-if) #ip nat outside //指定为 NAT 外端口
R2811( config-if) #exit
R2811( config) #access-list 1 permit 192. 168. 10. 0 0. 0. 0. 255
R2811( config) #access-list 1 permit 192. 168. 20. 0 0. 0. 0. 255 //
允许 vlan10 和 20 访问公网
R2811( config) #access-list 1 permit 192. 168. 30. 2 0. 0. 0. 0 //允
许内网 dns 访问公网
R2811( config) #ip nat inside source list 1 interface s0/3/0
overload //设置 pnat 重载允许内网访问公网
R2811( config) #ip nat inside source static tcp 192. 168. 30. 3 80
202. 1. 1. 1 80
R2811( config) #ip nat inside source static tcp 192. 168. 30. 4 20
202. 1. 1. 1 20
R2811( config) #ip nat inside source static tcp 192. 168. 30. 4 21
202. 1. 1. 1 21
R2811( config) #ip nat inside source static tcp 192. 168. 30. 5 21
202. 1. 1. 1 25
R2811( config) #ip nat inside source static tcp 192. 168. 30. 5 21
202. 1. 1. 1 110
//设置基于端口的静态 NAT, 允许公网访问内网资源
R2811( config) #router rip
R2811( config-router) #version 2
R2811( config-router) #no au
R2811( config-router) #network 202. 1. 1. 0
R2811( config-router) #network 192. 168. 1. 0
R2811( config-router) #default-information originate
//通过 rip 向内网宣告默认路由, 让内网的 S3 自动学习一条出
公网的默认路由
R2811( config-router) #exit
R2811( config) #ip route 0. 0. 0. 0 0. 0. 0. 0 s0/3/0
//设置一条出公网的默认路由
R2811( config) #access-list 110 deny udp any any eq 1434
R2811( config) #access-list 110 deny udp any any eq 135
R2811( config) #access-list 110 deny tcp any any eq 135
R2811( config) #access-list 110 deny udp any any eq 139
R2811( config) #access-list 110 deny tcp any any eq 139
R2811( config) #access-list 110 deny udp any any eq 445
R2811( config) #access-list 110 deny tcp any any eq 445
R2811( config) #access-list 110 deny udp any any eq 593
R2811( config) #access-list 110 deny tcp any any eq 593
```

```
R2811( config) #access-list 110 permit ip any any
//设置 110 扩展 ACL 列表
R2811( config) #inter s0/3/0
R2811( config-if) #ip access-group 110 in
//以上用 ACL 控制 Blaster 蠕虫的扫描攻击,阻止公网用户的
恶意攻击。
R2811( config-if) #end
R2811#copy run start //保存配置
```

## 2.4 ISP 路由器的配置

ISP 路由器主要完成端口的初始化 IP 封装,限于篇幅就不再给出详细命令。

## 3 服务器群的配置

网络模拟器 PT5.3 提供了强大的服务器功能,本案例中涉及的 Web、Ftp 和 Mail 服务器设置相对简单,而对 DNS 服务器的设置相对复杂。

内网 DNS 服务器有两个作用:其一,内网用户访问内网资源时,完成对字符域名的 IP 解析;其二,内网用户首次访问公网字符域名,内网 DNS 会向公网 DNS 服务器做 DNS 请求和转发<sup>[16]</sup>。该过程在互联网上常用迭代方法完成不同层次结构的 DNS 查询解析,并把返回的 IP 解析结果在内网 DNS 中做缓存,供内网用户下次重复查询使用,因此要求在出口路由器上设置对内网 DNS 服务器的 NAT 转发,这一点至关重要。

以下是 DNS 服务器的设置方法:首先,内网 DNS 分别设置 Web、Ftp 和 Mail 服务器的字符域名对应的 IP 解析,新建 Mail 服务器的 2 个别名(POP 和 SMTP 服务器);然后,内网 DNS 设置转发功能,向公网 DNS 根域 root-dns-server(202.5.5.2)做 DNS 请求和转发;最后,依次完成公网上的根域和顶级 COM 域的 DNS 设置,用于内网用户的迭代方法查询不同层次的 DNS,同时也为公网用户访问内网资源提供域名解析。图 2-4 分别给出了内网、公网上的根域、COM 域等 DNS 服务器的配置信息。

号码	名称	类型	详情
1	com	NS	root-dns-server
2	ftp.company.com.cn	A Record	192.168.30.4
3	mail.company.com.cn	A Record	192.168.30.5
4	pop.company.com.cn	CNAME	mail.company.com.cn
5	root-dns-server	A Record	202.5.5.2
6	smtp.company.com.cn	CNAME	mail.company.com.cn
7	www.company.com.cn	A Record	192.168.30.3

图2 内网 DNS 服务器的配置信息

号码	名称	类型	详情
1	163.com	A Record	202.2.2.2
2	com	NS	163.com

图3 公网根域 DNS 服务器的配置信息

号码	名称	类型	详情
1	ftp.company.com.cn	A Record	202.1.1.1
2	mail.company.com.cn	A Record	202.1.1.1
3	pop.company.com.cn	CNAME	mail.company.com.cn
4	smtp.company.com.cn	CNAME	mail.company.com.cn
5	www.163.com	A Record	202.3.3.2
6	www.company.com.cn	A Record	202.1.1.1

图4 公网 COM 域 DNS 服务器的配置信息

## 4 实验结果验证

### 4.1 验证内网的互连互通

(1) 验证不同 VLAN 的 DHCP 预分配信息。打开 PC0 至 PC3 在“IP 地址配置”界面选择自动获取;或在 DOS 下输入命令 ipconfig /all 能自动获取和显示各 VLAN 段的 IP 信息。

(2) 验证 VLAN 内和 VLAN 间通信。PC0 和 PC2, PC0 和 PC1 都能相互 Ping 通,说明 VLAN 内可通信和 VLAN 间可路由。

(3) 验证 DNS 的解析效果。以 PC0 为例,输入命令 nslookup 均能得到 www. company. com. cn、ftp. company. com. cn、pop. company. com. cn、smtp. company. com. cn 内网域名对应的 IP 解析。输入 nslookup www. 163. com,客户机和服务器中分别得到图 5 和图 6 的信息,内网 DNS 把请求转发给外网 DNS,通过不同层次结构的 DNS 迭代查询后,把查询结果反馈给客户机,同时在内网 DNS 缓冲中存有备

```
命令提示符
Packet Tracer PC Command Line 1.0
PC>nslookup www.163.com

Server: [192.168.30.2]
Address: 192.168.30.2

Non-authoritative answer:
Name: www.163.com
Address: 202.3.3.2

PC>
```

图5 客户机得到转发后的 DNS 查询结果

号码	名称	类型	详情
1	com	NS	root-dns-server
2	ftp.company.com.cn	A Record	192.168.30.4
3	mail.company.com.cn	A Record	192.168.30.5
4	pop.company.com.cn	CNAME	mail.company.com.cn
5	root-dns-server	A Record	202.5.5.2
6	smtp.company.com.cn	CNAME	mail.company.com.cn
7	www.company.com.cn	A Record	192.168.30.3

图6 内网 DNS 中的缓冲信息

份,内网用户解析公网字符域名获得成功。

(4) 验证对内网服务器的资源访问。从 PC0 至 PC3,浏览器输入 `http://www.company.com.cn` 能显示主页;在 DOS 下输入 `ftp ftp.company.com.cn`,账号和密码均为 `cisco`,本机上自建一个记事本,可用 `put` 命令上传至 `ftp` 服务器,也可用 `get` 命令下载 `ftp` 服务器文件;每个客户机设置自己的 Email 信箱,则 PC0 至 PC3 之间能相互发送 Email 通信。

#### 4.2 验证内网和公网之间的相互访问

(1) 验证内网用户访问公网的资源。以 PC0 为例,浏览器输入 `http://www.163.com` 能显示公网的首页;在 dos 下输入 `tracert www.163.com`,图 7 显示从 PC0 到公网 Web 站点的路径跟踪,数据包经过了三个路由设备,这和我们实际情况相吻合。

```
PC>tracert www.163.com

Tracing route to 202.3.3.2 over a maximum of 30 hops:

  0  62 ms  48 ms  62 ms  192.168.10.1
  1  93 ms  94 ms  78 ms  192.168.1.1
  2  110 ms  94 ms  110 ms  202.1.1.2
  3  141 ms  141 ms  141 ms  202.3.3.2

Trace complete.
```

图 7 内网用户 tracert 至公网 Web 站点的路径

(2) 验证公网用户访问内网的资源。公网 PC4 的 DNS 设置为 COM 域 DNS 服务器地址,浏览器输入 `http://www.company.com.cn` 后见图 8。在 dos 下输入 `ftp ftp.company.com.cn` 可以和内网 `ftp` 服务器进行文件传输;自定义 Email 信箱,也能与内网用户进行 Email 通信。

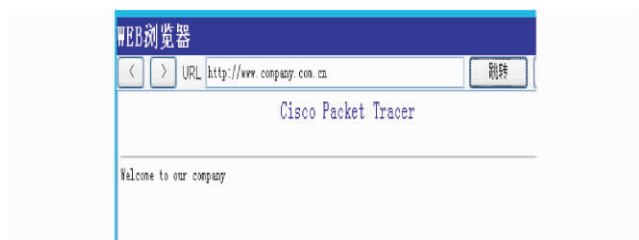


图 8 公网用户访问内网 Web 站点

(3) 验证 NAT 技术的非对称性。实验中用内网 PC0 能 ping 通公网 PC4,反之则不行。说明使用 NAT 技术可以隐藏内网结构,保护内网数据资源。

在实验配置和验证中遇到难以解决的问题,可利用 PT5.3 提供的强大的抓包功能来进行调试和分析,从而对配置命令加以改进和提高。实验结果表明,我

们对网络设备的配置信息能够满足网络应用的需求,在网络模拟器 PT5.3 中得到了很好的模拟和仿真。

## 5 结 语

本文提供了一个小型企业的网络架构应用案例。该应用案例麻雀虽小,但五脏俱全,具备了一个通用的网络工程实训项目功能模型,涵盖了 CCNA 考证大部分的网络知识要点,对学习和掌握常见网络命令配置起到举一反三、融会贯通的作用。这个在实际环境中很难实现的工程项目,却可用网络模拟器 Packet tracer5.3 引入到教学中,能加深学生对网络工程中的组网、配置、调试和验证过程的认识和理解,提高了学生的综合配置和集成能力。

#### 参考文献(References):

- [1] 黄声烈,黄毅.构建网络协议仿真教学系统平台的研究[J].实验室研究与探索 2006(2):187-188,197.
- [2] 王春枝,李红,欧阳勇.计算机网络课程实验教学研究[J].实验室研究与探索 2007(12):350-352.
- [3] 张刚,黄小波.思科虚拟实验平台的构建[J].实验室研究与探索 2010(8):216-217,225.
- [4] 潘江波,邓建高.仿真软件在计算机网络教学中的作用[J].实验技术与管理 2011(7):91-94.
- [5] 徐巧枝.基于 Packet Tracer 的计算机网络实验教学方案[J].内蒙古师范大学学报 2012(3):144-146.
- [6] 苟全登.网络仿真软件 Packet Tracer 在《网络工程实训》教学中的应用[J].现代计算机 2011(3):83-85.
- [7] 薛琴.基于 Packet Tracer 的计算机网络仿真实验教学[J].实验室研究与探索 2010(2):57-59.
- [8] 张梁斌.网络职业认证为指引促进计算机网络工程课程建设[J].浙江万里学院学报 2011(5):110-113.
- [9] 梁世斌.基于 Packet Tracer 的多路由协议重分发的仿真实验[J].浙江万里学院学报 2012(2):85-89.
- [10] 张选波.设备调试与网络优化学习指南[M].北京:科学出版社,2009.
- [11] 曹学峰.计算机网络配置、管理与应用[M].北京:机械工业出版社 2010.
- [12] 赵昕.企业网络架构的实例分析[J].淮南师范学院学报 2002(3):31-32.
- [13] 倪旭澜.企业网络架构的设计及应用[J].铁道机车车辆工人,2006(6):23-26.
- [14] 唐天平.利用 Packet tracer 模拟组建大型单核心网络研究[J].实验室研究与探索 2011(1):186-190.
- [15] 肖学华.网络设备管理与维护实训教程-基于 Cisco Packet tracer 模拟器[M].北京:科学出版社 2011.
- [16] 于存江.Windows Server 中 DNS 的层次结构和名称解析的实现[J].长春大学学报 2008(2):51-53.