

Dr. COM 认证环境下 Internet 接入共享与仿真

崔建涛¹, 赵晓君¹, 张烁²

(1. 郑州轻工业学院 软件学院, 河南 郑州 450001;

2. 中国铝业郑州研究院 设备与自动化研究所, 河南 郑州 450041)

摘要: 为了满足企业内、外网之间灵活访问的需求, 设计了一个改进的 Internet 接入共享方案。基于路由和远程访问服务和网络地址转换技术, 成功实现了 Dr. COM 宽带认证环境下主机和移动终端的网络接入共享。并在 VMware 虚拟机上仿真某企业网络。改进后的方案, 无需购置专用硬件路由器, 具有成本低、软硬件可扩充性强、组网灵活等优点, 尤其适用于中小型企业。并为工程技术人员研究 Internet 接入提供了有益参考。

关键词: 宽带认证; Internet 接入共享; 路由和远程访问服务; 网络地址转换

中图分类号: TP393.07 **文献标志码:** A **DOI:** 10.3969/j.issn.2095-476X.2013.06.020

Internet access share and the simulation under the Dr. COM authentication environment

CUI Jian-tao¹, ZHAO Xiao-Jun¹, ZHANG Shuo²

(1. College of Software Engineering Zhengzhou University of Light Industry Zhengzhou 450001, China;

2. Equipment&Automation Division Zhengzhou Research Institute of CHALCO Zhengzhou 450041, China)

Abstract: In order to meet the flexible access requirements between internal and external enterprise network, the improved Internet connection share scheme based on RRAS and NAT was designed. The simulation of the company network based on VMware virtual machine was carried out, and Internet access share of host and mobile terminal under the Dr. COM broadband authentication environment was successfully realized. Compared with traditional network access scheme, without purchasing dedicated hardware routers, the improved scheme has some advantages, such as the lower cost, the strong scalability of hardware and software, the flexible networking, etc, which was especially suitable for small and medium enterprises. This scheme provided the beneficial reference about studying Internet access for engineering and technical personnel.

Key words: broadband authentication; Internet access share; routing and remote access service (RRAS); network address translation (NAT)

0 引言

实现企业内部网络接入 Internet, 通常需要购置

专用的路由器或三层交换机等硬件设备^[1], 实施网络地址转换 (NAT)^[2], 再接入运营商 ISP 路由器。该传统接入方案具有数据吞吐量大、稳定可靠等优

收稿日期: 2013 - 09 - 17

基金项目: 国家自然科学基金项目 (61040025)

作者简介: 崔建涛 (1979—), 男, 河南省郑州市人, 郑州轻工业学院讲师, 硕士, 主要研究方向为计算机网络。

点,但由于需要购置专用的硬件设备,存在建网成本高、可扩展性不强、灵活性欠佳等问题^[3],并且在部署有宽带认证软件的网络环境下,还有共享接入受限等缺陷.例如,Dr. COM 宽带认证环境限制在主机端安装双网卡,限制使用代理、ICS、NAT 等共享技术,也限制接入无线路由器^[4],主机和移动终端无法共享现有的宽带认证账号接入 Internet.

针对 Dr. COM 宽带认证环境下共享接入受限的问题,目前国内外的研究侧重于 Dr. COM 原理分析和破解方法,而极少有利用 RRAS 和 NAT 在主机端实现共享接入的研究和实践.为了解决传统接入方案的不足,满足 Dr. COM 宽带认证环境下主机和移动终端共享接入 Internet 的需求,本文拟采用 RRAS 和 NAT 技术设计一个改进的 Internet 接入共享方案,并在 VMware 虚拟机平台上仿真某企业网络.

1 改进的 Internet 接入共享方案及仿真设计

某中小企业网络内部现有一定数量员工用计算机,另有 2 台配置较高的闲置服务器,该网络尚未接入 Internet.出于经费考虑,该企业要求利用闲置服务器作为企业内部路由器及 Internet 接入共享设备使用,实现内部网络所有主机都能访问 Internet,同时内部网络特定主机也能对外提供服务,并能实现在宽带认证环境下主机和移动终端仍能共享现有的宽带认证账号接入 Internet.

根据企业网络现状和联网需求,将 1 台闲置服务器作为企业内部路由器 R1,另 1 台服务器作为主机 1 使用.在主机 1 上运行一个用于 Internet 接入共享的虚拟机,即 Internet 接入共享主机 VM,同时可根据需要在企业内部网络上搭建无线路由器等设备,以便手机、笔记本等移动终端联网,笔者设计的网络拓扑结构,即改进后的 Internet 接入共享方案如图 1 所示.

其中,用 192.168.100.0/24 代表企业内部网络,用 192.168.12.0/30 代表企业内部路由器 R1 与运营商 ISP 路由器之间的企业核心网;企业内部网络中的主机通过企业内部路由器 R1 上的网络地址转换(NAT)访问 Internet,NAT 地址池为 202.196.1.0/28,即 202.196.1.1—202.196.1.14;用 202.196.8.0/24 模拟 Internet 中的某网络,Server1 代表 Internet 中的某台服务器,IP 地址为 202.196.8.189.

笔者利用虚拟机平台仿真该企业网络.由于所用虚拟机较多,若仅在单台物理主机上仿真,必然会占用物理主机的过多资源,建议在多台物理主机上运行不同角色的虚拟机^[5].本文为了方便起见,在单台物理主机上仿真主机 1、主机 2、企业内部路由器 R1、ISP 路由器、服务器 Server1.为了更直观识别各网络接口,分别重命名 R1、ISP 的本地连接 1、2 为 Out 接口、In 接口,各主要设备的接口描述、IP 地址/掩码、网关等设置,见表 1.

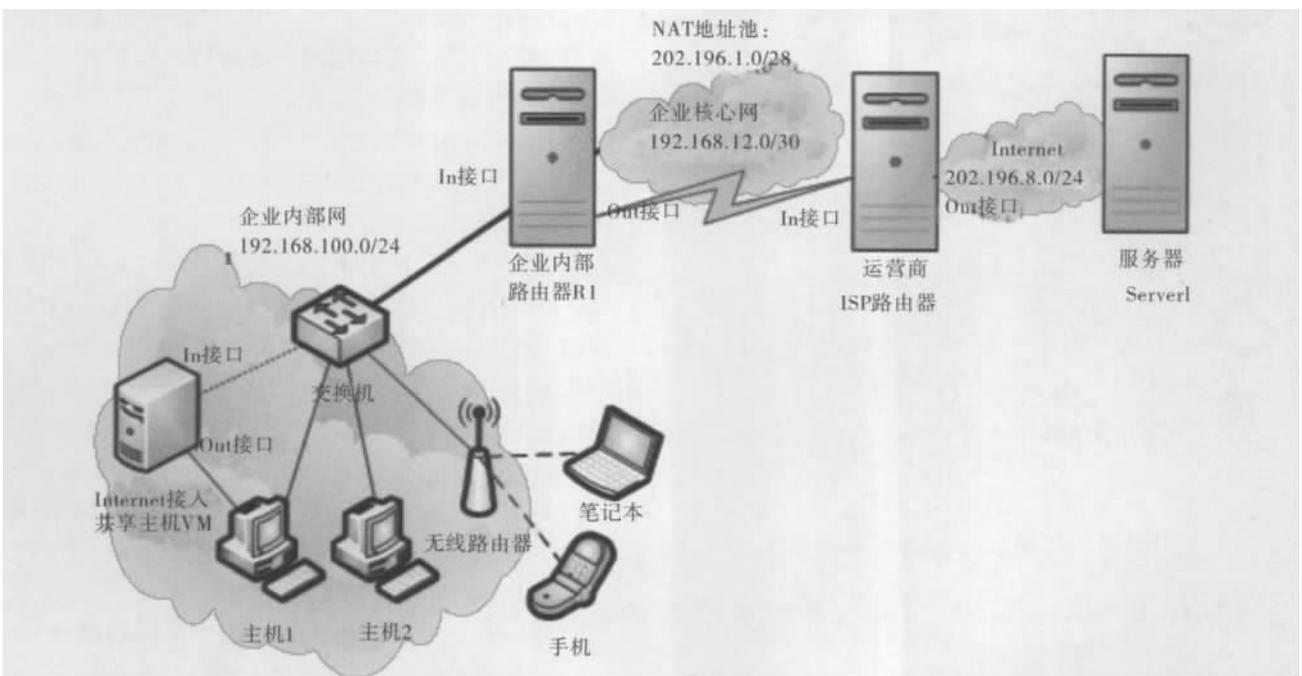


图 1 改进后的 Internet 接入共享方案

表 1 各主要设备网络配置

主要设备	接口描述: IP/掩码	网关
主机 1	本地接口: 192. 168. 100. 1/24	192. 168. 100. 254
主机 2	本地接口: 192. 168. 100. 2/24	192. 168. 100. 254(默认方式) 192. 168. 100. 253(共享方式)
内部路由器 R1	In 接口: 192. 168. 100. 254/24 Out 接口: 192. 168. 12. 1/30	—
ISP 路由器	In 接口: 192. 168. 12. 2/30 Out 接口: 202. 196. 8. 254/24	—
服务器 Server1	本地接口: 202. 196. 8. 189/24	202. 196. 8. 254
Internet 共享 主机 VM	In 接口: 192. 168. 100. 253/24 Out 接口: 利用 VM NAT 动态获取	利用 VM NAT 动态获取
无线路由器	WAN 接口: 192. 168. 100. 252/24 LAN 接口: 192. 168. 1. 1/24	192. 168. 100. 253
移动终端	从无线路由器动态获取	从无线路由器动态获取

企业网络内主机 1、主机 2 采用默认方案接入 Internet,需要在企业内部路由器 R1、ISP 路由器上分别配置并启用 RRAS;在 R1 上启用 NAT 并配置默认路由;在 ISP 路由器上配置到 NAT 地址池的静态路由;在 R1 上启用 DHCP 分配器;在 R1 上通过地址/端口映射对外开放内网中的某些网络服务.为了使得主机 2、移动终端等设备能共享主机 1 上现有的宽带认证账号接入 Internet,需要在 Internet 接入共享主机 VM 上启用 RRAS 和 NAT,改进后的共享接入方式如图 2 和图 3 所示.

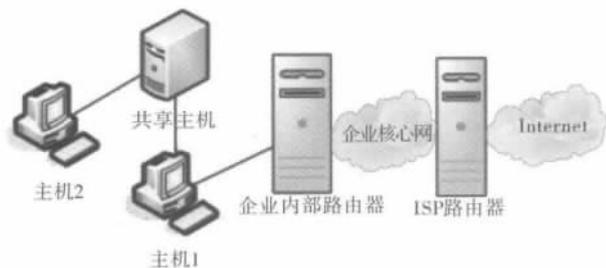


图 2 主机 2 改进后的共享接入图



图 3 移动终端改进后的共享接入图

2 具体实现

2.1 在 R1 上启用 RRAS 和 NAT 并配置默认路由
在 R1 上运行 rasmgmt. msc,打开“路由和远程

访问”控制台,依次选择“配置并启用路由和远程访问”、“自定义配置”,选择“LAN 路由”和“NAT 和基本防火墙”;在 R1 上配置到 Internet 的默认路由,确保 R1 Out 接口右侧的网络互通,目标 0.0.0.0,掩码 0.0.0.0,网关 192. 168. 12. 2;在 R1 上启用 NAT 的专用接口和公共接口,右击“NAT 和基本防火墙”,新增接口“link to LAN 1”、“link to ISP”,依次设置为“专用接口连接到专用网络”、“公共接口连接到 Internet”,并在公共接口上启用 NAT,地址池配置为 202. 196. 1. 1—202. 196. 1. 14.

2.2 在 ISP 路由器上启用 RRAS 并配置到 NAT 地址池的静态路由

在 ISP 路由器上运行 rasmgmt. msc,打开“路由和远程访问”控制台,依次选择“配置并启用路由和远程访问”、“自定义配置”,选择“LAN 路由”;在 ISP 上配置到 NAT 地址池 202. 196. 1. 0/28 的静态路由,确保 Internet 上的主机能访问到地址池,目标 202. 196. 1. 0,掩码 255. 255. 255. 240,网关 192. 168. 12. 1.

2.3 在 R1 上启用 DHCP 分配器

为了确保公司内网计算机能动态获取到 IP 地址,可以在内网中部署 DHCP 服务器,也可以启用 DHCP 分配器^[6].本方案在 R1 上启用 DHCP 分配器,右击“NAT 和基本防火墙”,打开“地址指派”选项卡,启用“使用 DHCP 分配器自动分配 IP 地址”,设置 IP 地址 192. 168. 100. 0,掩码 255. 255. 255. 0,点击“排除”,可以排除某些 IP 地址,例如网关 192. 168. 100. 254 及预留的 IP 地址等.

2.4 在 R1 上对外开放内网中的某些网络服务

以对外开放主机 1 上的远程桌面为例.在 R1 上,右击“Out 接口”,打开“服务和端口”选项卡,点

击“添加”,输入服务描述,例如 open pc01 remote desktop,公用地址选择在此地址池项 202.196.1.1,传入、传出端口均设置为 Windows 终端服务的端口 3389,专用地址设置为主机 1 通过 DHCP 分配器动态获取的 IP 地址(例如 192.168.100.70),如图 4 所示。

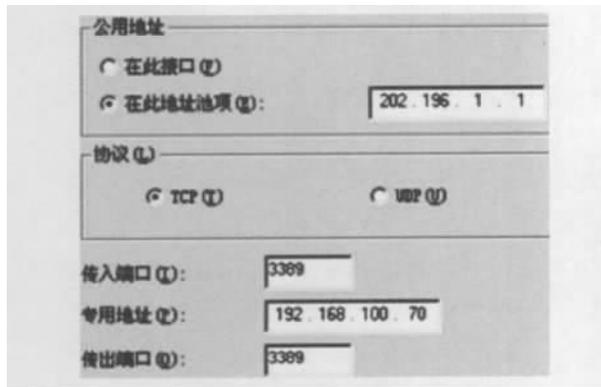


图 4 设置服务和端口

2.5 Internet 接入共享主机 VM 关键技术

VM 上启用 RRAS 和 NAT 的过程和路由器 R1 类似。建议在实际网络环境中仿真该操作,在物理主机 1 上登录 Dr. COM 宽带认证客户端,确保主机 1 能正常访问 Internet,并在主机 1 上运行一台基于 Windows Server 2003/2008 操作系统的虚拟机,即 Internet 接入共享主机 VM。在共享主机 VM 上添加 2 个网络接口卡(NIC),其中 NIC 1 网络连接类型设置为 NAT,重命名本地连接 1 为 Out 接口,其利用虚拟机内置 NAT 动态获取 IP、掩码、网关、DNS 等网络配置^[7]。NIC 2 网络连接类型设置为桥接,重命名本地连接 2 为 In 接口,手工配置地址 192.168.100.253/24。由于共享主机 VM 的 NIC 1 选择的网络连接类型是 NAT,则无需登录宽带认证客户端就能共享主机 1 的 Internet 连接,并且在其上安装双网卡,主机 1 上的宽带认证客户端不会发出任何警告,也不会注销主机 1 上的 Internet 连接,这为移动终端、无线路由器共享接入 Internet 提供了条件。

通讯协议	方向	专用地址	专用端口	公用地址	公用端口	远程地址	远程端口	空闲时间
TCP	入站	192.168.100.70	3,389	202.196.1.1	3,389	202.196.8.189	1,046	0
TCP	出站	192.168.100.70	1,208	202.196.1.1	1,208	202.196.8.189	23	46
TCP	出站	192.168.100.107	1,083	202.196.1.2	1,083	202.196.8.189	23	36

图 6 网络地址转换映射表

3 测试结果

3.1 默认接入测试

在服务器 Server1 上启用网络服务(以 Telnet 为例)。通过 R1 上的 DHCP 分配器功能,主机 1 成功获取 192.168.100.0/24 子网内地址(例如 192.168.100.70),并能成功访问服务器 Server1(202.196.8.189)上的 Telnet 服务(服务器 Server1 需提前启用 Telnet 网络服务)。在 Server1 上,运行 mstsc 输入 202.196.1.1,成功访问主机 1 上的远程桌面(主机 1 需要提前启用远程桌面)。主机 2 若启用 DHCP,也能成功获取 192.168.100.0/24 子网内地址(例如 192.168.100.107)。

在服务器 Server1 上,运行 netstat-n,查看网络连接状态,如图 5 所示。

Proto	Local Address	Foreign Address	State
TCP	202.196.8.189:23	202.196.1.1:1221	ESTABLISHED
TCP	202.196.8.189:23	202.196.1.2:1088	ESTABLISHED
TCP	202.196.8.189:1046	202.196.1.1:3389	ESTABLISHED

图 5 Server1 网络连接状态

在企业内部路由器 R1 上,查看网络地址转换映射表,如图 6 所示。

测试结果表明,主机 1、主机 2 的内网专用地址已经通过企业内部路由器上启用的 NAT 转换为地址池中的公用地址,并已成功建立了到服务器 Server1 的 Telnet 连接(远程端口为 23); Server1 已经建立了到 202.196.1.1 的远程桌面连接(外部端口为 3389),公用地址 202.196.1.1 将映射为主机 1 的内网专用地址 192.168.100.70。

3.2 主机 2、移动终端共享接入测试

将主机 2 的默认网关指向 Internet 接入共享主机 In 接口的 IP 地址,即 192.168.100.253,主机 2 此时无需登录宽带认证客户端便可以访问 Internet。将无线路由器的 WAN 口接入到如图 2 所示的企业内部交换机上,并将 WAN 接口设置为企业内部网

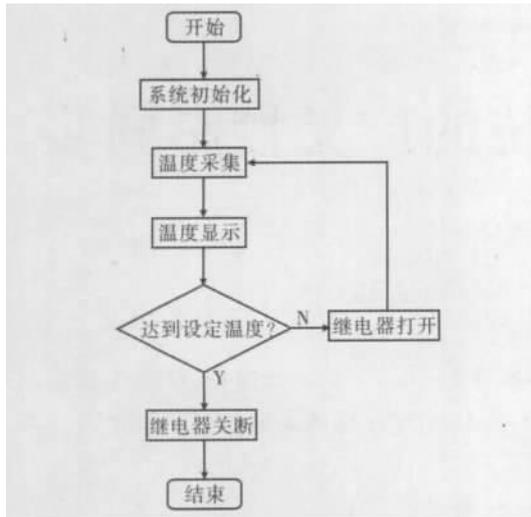


图 6 温度检测控制单元软件流程图

换电站内所需的 100 台分箱充电机和 220 台整车充电机的老化状态监测、控制和老化数据自动记录等。运行过程中采样数据正确率、老化温度控制范围、各项报警功能和系统可靠性等指标均达到了预期的效果。

5 结语

本文以 ATmega64 芯片为核心,设计了电力直

流电源产品老化监控系统。系统采用 RS485 总线作为主要通信方式,采用功能单元模块化结构,各模块挂在 RS485 总线上,易于系统的实现与扩展;上位机使用 PC 工控机,以图形方式方便直观地对各个节点进行监控,保证了系统可靠运行。实际应用证明该系统具备控制效果好、可靠性高、控制灵活等优点。

参考文献:

- [1] 金家峰. 产品早期失效与老化筛选 [J]. 铁路通信信号工程技术, 2008(6): 29.
- [2] 赖应杰, 骆德汉. 基于 RS485 总线的电源老化测试系统的设计 [J]. 家电科技, 2009(12): 51.
- [3] 海涛. ATmega 系列单片机原理及应用——C 语言教程 [M]. 北京: 机械工业出版社, 2008.
- [4] 张宏伟, 路康, 袁超. 基于 LonWorks 现场总线的智能小区监控系统设计 [J]. 郑州轻工业学院学报: 自然科学版, 2011, 26(4): 98.
- [5] 彭荣涛, 林玛丽. 提高老化测试设备系统控制稳定性的研究 [J]. 合成材料老化与应用, 2010, 39(3): 26.
- [6] 王中武. 电源老化测试系统 [J]. 电子质量, 2005(6): 22.

(上接第 89 页)

络 192.168.100.0/24 可用的地址,例如 192.168.100.252/24, 网关指向 192.168.100.253; 将无线路由器的 LAN 接口保持默认设置不变,例如 192.168.1.1/24; 在无线路由器上设置 SSID 及无线网络安全密钥、路由器管理口令等必需参数。在移动终端(例如笔记本电脑、手机等)开启 WIFI 功能,搜索到相应 SSID 信号后,输入相应无线网络安全密钥,便可获取到无线路由器 LAN 192.168.1.0/24 内可用的地址,此时移动终端无需登录宽带认证账号便可共享接入 Internet。

4 结论

本文在传统 Internet 接入方案的基础上,提出了基于 RRAS 服务和 NAT 技术而无需购置专用硬件路由器的 Internet 接入共享方案,并利用虚拟机平台仿真了某企业网络,成功解决了企业内网接入 Internet,内网对外开放某些网络服务以及 Dr.COM 宽带认证环境下在主机端启用 Internet 接入共享等问题。这种接入方式具有软硬件容易扩充、组网灵

活、联网成本低廉、运行稳定可靠等优点,尤其适用于中小型企业。本文也为工程技术人员利用虚拟机平台研究 Internet 接入共享提供了有益的参考。

参考文献:

- [1] 兰勇, 张博. 私有 IP 地址环境中的嵌入式设备实时控制技术 [J]. 测控技术, 2011, 30(4): 67.
- [2] 刘向东, 李志洁, 王德高, 等. NAT 原理实验的设计与实现 [J]. 实验室研究与探索, 2012, 31(1): 58.
- [3] 姚敦红, 石元泉. 基于动态命令树算法的路由器仿真软件设计 [J]. 计算机仿真, 2013, 30(4): 194.
- [4] 黄桂敏, 朱晓妹. 基于 UDP 协议穿透 NAT 设备的对等网络模型研究 [J]. 计算机工程与设计, 2010, 31(2): 317.
- [5] 崔建涛, 王文冰, 邓璐娟. 基于虚拟机的 OSPF 动态路由协议的研究 [J]. 郑州轻工业学院学报: 自然科学版, 2012, 27(3): 15.
- [6] 韩丽, 崔建涛. DHCP 中继代理在虚拟机上的实现 [J]. 太原理工大学学报, 2010, 41(2): 163.
- [7] 张素智, 崔建涛, 梁树军. Windows Server 2003 配置与管理 [M]. 郑州: 河南科学技术出版社, 2008.