doi: 10.3969/j.issn.1006-1576.2010.03.019

# 基于 TCP/IP 的路由器远程实验系统

孙璐
（华南理工大学 自动化科学与工程学院，广东 广州 510641）

**摘要**：针对网络设备的管理特点及网络管理实验的具体要求，提出了一种利用代理服务器作为应用网关的远程路由器实验系统解决方案，并对其概念、需求、技术方案、业务处理模块设计等方面进行分析、介绍。该方案构建了一个可以提供 7x24 模式服务的无人远程网络实验室，能大大提高设备的利用时间及利用率，有良好的应用前景。

**关键词**：路由器；代理服务器；网关；远程实验
**中图分类号**：TP393.02 **文献标识码**：A

# Router's Remote Experimental System Based on TCP/IP

SUN Lu
(College of Automation Science & Engineering, South China University of Technology, Guangzhou 510641, China)

Abstract: For the features of network equipment management and the specific requirements of the network management experiment, it presents a router's remote experimental system solution which uses a proxy server as an application gateway, analyses and introduces its concepts, requirements, technical solutions, business processing module design, etc. The solution can be applied to build a no one remote network laboratory which provides 7x24 model services, can greatly increase the use of time and utilization of equipments, there is a good application prospects.

Keywords: Router; Proxy server; Gateway; Remote experiment

## 0 引言

路由器是应用最广泛的网络设备。掌握其配置方法是网络教学实验甚至设备管理的重要任务。几乎所有厂商的路由器都拥有一个符合 RS-232C 标准的 Console 口用于路由器的高级配置管理[1]，利用该端口，运行终端仿真软件的计算机可以最高级别的权限进入路由器的操作系统（如 CISCO 的 IOS），执行各类配置命令，进行路由器的各类配置管理任务。除了设备管理方面的需求外，这种利用一根串口电缆通过 Console 口进行设备配置的手段也是学习各类路由器（例如 Cisco、华为等厂商）配置使用的主流方法。目前，社会上的网络培训机构及各大学的网络实验室在进行路由器的实验时，一般采取“一人一机”这种应用模式，不利于设备的集中管理、不利于设计较为复杂的实验、设备的利用率低、管理成本较高。故针对网络设备的管理特点及网络实验的需求，提出远程路由器实验系统的解决方案，将一个普通的机房管理的网络实验室升级为 7x24 小时自动化管理的在线网络实验室。

## 1 需求分析

1) 可在不改变路由器配置模式的前提下（即仍然通过 Console 口访问路由器），使路由器等网络设备与使用者物理位置分离。各类路由器可以集中地以机架式存放在机房等地。

2) 支持通过串口（Console 口）的方式或通过 IP 的方式访问路由器。

3) 使用者可以在授权的前提下任意选择使用一台或多台路由器进行实验（串口访问方式的前提是所选择的设备当前没有人使用）。

4) 应用模式不再是“一人一机”，系统可支持 7x24 小时实验，在授权的前提下，使用者可在任意时间，在网络可连的任何位置，利用本系统选择任意的路由器进行操作。

5) 系统具有对使用者的强大管理功能，可针对不同需求特点对用户进行业务分组，并以组为单位对使用者的身份、系统访问时间、访问时长、允许使用的操作命令、允许使用的设备等要素进行授权及管理；并可以根据上述管理任务扩展计费功能。

6) 系统具有对远程客户端发来的路由器操作命令进行过滤的功能，根据用户所在组的权限设置，仅允许使用的操作命令可被发往指定的路由器。

7) 使用简单。系统在使用中应能对原有模式下（即通过串口用终端仿真软件访问路由器的“一人一机”模式）的路由器访问界面进行仿真，不改变用户原有的使用习惯。

收稿日期：2009-10-27；修回日期：2009-11-29
作者简介：孙璐（1968-），男，江苏人，华南理工大学讲师，硕士，从事计算机网络应用、数据库技术研究。

## 2 技术方案

设计思路：传统的“一人一机”模式下，使用者运行仿真终端软件，通过串口进入路由器进行操作，用户的所有操作都直接面向路由器的操作系统，操作系统将命令的结果直接返回到仿真终端的界面上供用户查看，设备的控制权在用户手上。而本系统是通过开发一对符合 TCP/IP 规范的客户端软件及代理服务器软件（网关）[2]，以隔离远程用户和后端的路由器设备，客户端软件面向远程用户，模拟传统的路由器使用界面，接收用户的操作命令（符合路由器要求的指令），并将操作命令发送至代理服务器软件，代理服务器发挥强大的管理功能，根据预定义的操作策略对命令进行过滤，将符合要求的操作命令转发至选定的后端路由器，路由器执行操作命令并将结果信息通过代理服务器返回至客户端软件供远程用户查看，这一流程就构成了整个系统的核心思路。系统的逻辑结构，如图 1。

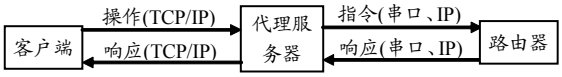


图 1 系统逻辑结构

系统的网络结构、系统结构及操作流程为：

1) 系统网络结构

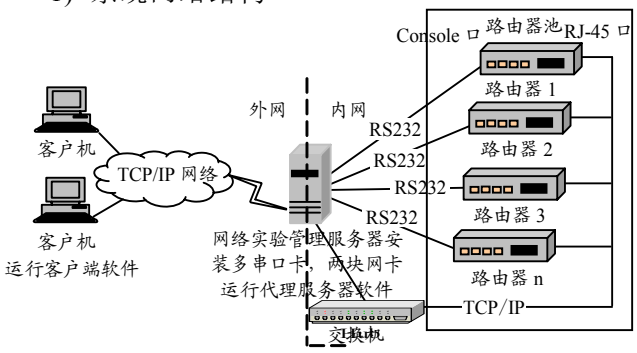


图 2 系统网络结构

如图 2，路由器远程实验系统由安装有多串口卡（提供大容量串口，可选择 MOXA、DIGI、Multitech 等产品）的网络实验服务器、路由器池、交换机、客户机组成。整个网络分为：内网部分由路由器池、交换机及实验服务器的内网卡组成，外网由客户机群、TCP/IP 网络、实验服务器的外网卡组成。利用 TCP/IP 网络[3]，客户机可以访问实验服务器，但不能直接访问路由器池中的设备。所有对路由器池中设备的访问都必须通过实验服务器经过滤验证后转发。实验服务器安装有多串口卡，每个串口通过一条标准的 RS-232C 电缆连接 1 台路由器设备。每台路由器除了连接一个实验服务器上的串口外，还通过 RJ-45 电缆连接交换机的一个端口，可实现路由器的串口访问（独占）或 IP 访问（共享）。模拟仿真终端的客户机软件采用 Java Applet 方式运行，可免除客户端软件的升级维护麻烦。

2) 系统功能结构（图 3）

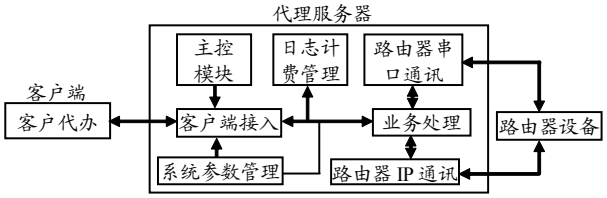


图 3 整个系统的功能结构

客户代办：运行在远程实验客户端上的进程，该进程以 TCP/IP 方式连接实验服务器上的代理服务器软件，登录实验服务器，选择路由器设备操作，一旦选中路由器，则系统将在“客户代办—代理服务器—路由器”之间建立一条通讯会话，用于传递路由器的操作命令及返回操作结果信息，该软件在操作路由器时，界面完全仿真终端软件的操作习惯。

主控模块：负责代理服务器软件内各模块间的协同合作及各模块间信息传递。

系统参数管理：对整个系统的环境运行参数进行集中管理，包括用户设置（用户组设置、用户账号设置、访问时间及时长设置）、路由器及串口设置（路由器 IP 等参数设置、路由器与串口的绑定及串口通讯参数设置）、非法指令集设置（不允许使用的指令集设置）、计费策略设置、权限设置（用户组的设备使用权限、指令权限设置）、计费策略设置等。

客户端接入：负责与客户端通信。客户端接入模块作为 TCP/IP 服务器端监听一个服务端口，同时接入一个或多个客户端连接，并作多任务并发处理，同时响应多客户的请求。本模块会为每个成功接入的客户创建一个独立的子线程。

业务处理：代理服务器软件的核心部分，负责对接入用户的身份及权限进行验证，对远程用户发来的操作命令进行缓存过滤后转发至相应的设备通讯线程，接收设备的响应并转发至远程用户，对用户会话及用户的系统操作进行日志记录等。

路由器串口通讯：设备通讯线程之一，负责与路由器的串口（Console）进行通信。

路由器 IP 通讯：负责与路由器进行 TCP/IP 通信。

日志计费管理：对日志、计费信息进行管理（查询、浏览）、利用计费策略的设置对接入用户进行计费（如果有需要），客户端接入模块可利用该项服务

产生的数据决定是否自动中断远程用户的连接。

3) 系统操作流程

远程网络实验系统的业务操作流程为：

(1) 用户登录认证（客户代办与代理服务器建立通信连接，并由客户代办向代理服务器发送账号和密码，代理服务器对用户账户的合法性及连接时段的有效性进行验证）。

(2) 代理服务器对认证失败用户报错，对认证成功用户告知用户权限（IP 用户或串口用户）及可使用的路由器列表。

(3) 用户选定路由器（指串口用户）或输入要连接的 IP 地址（指 IP 用户）。

(4) 代理服务器根据指定的设备通过串口或 TCP/IP 与其建立连接。

(5) 如果连接失败，代理服务器向用户报错，如果连接成功，则告知用户连接成功，如果是串口用户，则要将该设备设置为串口已用。

(6) 日志及计费服务启动，记录用户实时连接数据。

(7) 用户向代理服务器发送操作指令。

(8) 代理服务器对其指令校验。

(9) 代理服务器对校验成功的指令往对应设备转发。

(10) 代理服务器接收设备的应答。

(11) 代理服务器向客户代办转发设备应答。

(12) 用户接收设备应答。

(13) 用户注销或用户与代理服务器的通信连接中断。

(14) 代理服务器释放设备连接。

注：其中 7～12 操作步骤是循环执行的。

可以看出，代理服务器中的业务处理模块是整个系统的核心，仅对整个系统的业务处理模块中的设计重点进行简要阐述。

## 3　业务处理模块设计

业务处理模块是整个代理服务器的核心组件，其主要处理的任务有 3 大项：用户身份及权限的验证、命令过滤以及日志记录。

1) 用户身份及权限验证

包括用户身份校验、用户权限认证和用户注销等 3 小项，主要用于管理接入用户的合法性及赋予接入用户相应的权限，考虑到网络实验这类业务的应用特点，在设计中重点考虑了以下几点：

以用户组为单位进行管理。将用户划分为若干虚拟组进行组织，以组为单位分配设备、设备通讯方式（串口、IP）、操作指令（允许或不允许的指令）、访问时限等权限。用户登陆后，系统将根据其所在组的身份决定其可用的设备及可作的操作。

黑名单管理。为了避免某些用户使用不允许的指令浪费系统的连接资源，除了后面的命令过滤措施以外，设置一个系统黑名单，当用户的非法行为（如使用不允许的指令或在不允许的时段连接或已经超出使用时长）超过一定次数后，系统可自动将该用户列入黑名单拒绝连接。

单一登录。系统不允许用户用同一账号重复登录，每个登录成功的用户，系统将其标注为“在线”，拒绝其它同一账号的登录请求，同时系统将为其分配内存记录其可使用的权限及指令列表。

用户登录系统验证身份及获取权限流程如图 4。

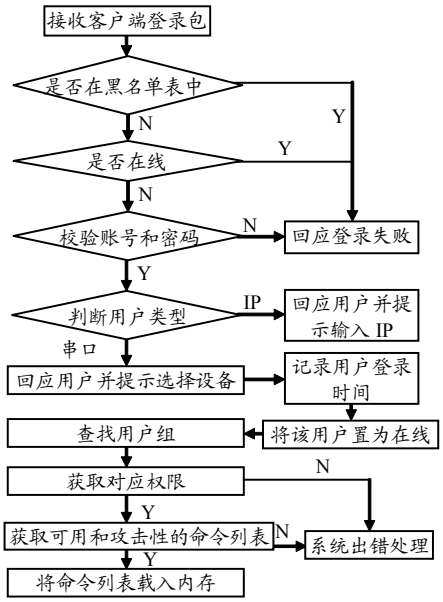


**图 4　用户身份验证及权限认证流程**

2) 命令过滤

由于系统不仅用于网络培训的用户，也供管理员进行设备管理之用，且路由器的一个操作指令的格式一般如下[4]：

操作码　参数码 1　参数 1　参数码 2　参数 2……

因此操作命令过滤的需求主要包括 3 类：管理员可使用任何指令。用户不允许使用某项操作码。用户不允许使用某项指令的某些参数码。

为此，从以下几个方面来实现命令过滤的需求：

(1) 将用户组分为管理类及用户类两类，管理类用户具有任意权限，可使用任意指令（不需要过滤）。用户类用户必须进行命令过滤。

（下转第 57 页）

制及安全策略及其实现（常规驻车制动功能、坡道辅助起步功能及相关扩展功能）、CAN 总线通讯协议的软件设计、CAN 总线应用层协议的设计、中央控制节点的软件设计、参数采集及制动系统控制节点的软件设计。此外，还应确定系统中 CAN 总线上的通讯机制及 CAN 总线的传输速率。

## 4　仿真实验

建立高效、稳定的系统开发环境，在系统开发中发挥着重要的作用，它能够提高系统开发效率、缩短系统开发周期、保障系统程序的稳定运行。本系统在整个调试过程中，使用了单片机开发编译器 Keil C、WAVE E2000S 型仿真器、CAN232B 智能 PC-CAN 总线接口卡、PC 上位机以及硬件调试工具示波器、万用表等。其中，CAN 总线采用屏蔽双绞线，发动机和车速信号用信号发生器模拟产生，根据计算，系统中确定 CAN 的传输速率为 100 kbps。

## 5　小结

通过对基于 CAN 总线的电子驻车系统进行调试，中央控制节点、左右驻车制动控制节点及各参数采集节点均能正常工作，参数采集准确，CAN 总线发送与接收报文正确，并实现了预期的设计功能。

## 参考文献：


[1] 饶剑, 黄妙华, 刘飞. 汽车线控技术的应用及关键技术[J]. 汽车电器, 2005, 09(9): 1-4.

[2] Philips Semiconductors. CAN Specification 2.0 Part A, 1991.

[3] Philips Semiconductors. CAN Specification 2.0 Part B, 1991.

[4] 国家质量监督检验检疫总局. GB7258—2005. 机动车运行安全技术条件[S]. 2005.

[5] Peter Hank, Egon Jhnk. SJA1000 Stand-alone CAN controller[Z]. Germany: Philips Semiconductor, 1997.

[6] 张平, 焦彦平, 单玉泉. 美军军民融合一体化装备保障实践及启示[J]. 四川兵工学报, 2009(9): 138-139.


**********

（上接第 53 页）

(2) 将命令的权限分为安全及不安全指令，安全指令可直接使用，不安全指令需进行命令过滤。

(3) 对于无参数码指令，仅需要判断指令是否在用户允许的命令集中，对于带参数码，需要进行参数解析，判断用户是否可使用某项参数码，图 5 为命令过滤的流程。

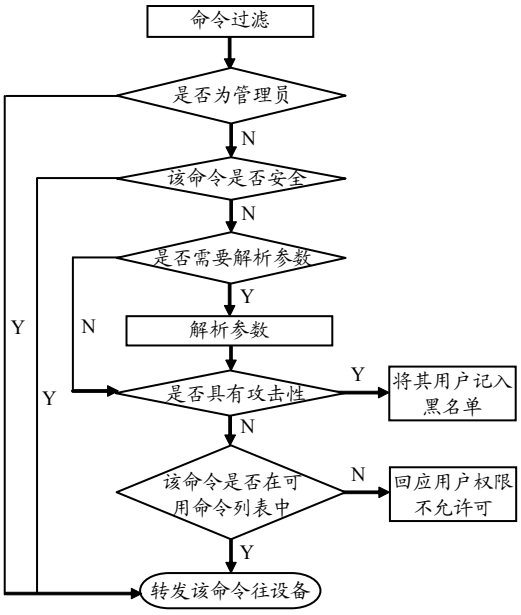


**图 5　命令过滤流程**

3) 日志记录

代理服务器系统的操作日志是以文本文件方式记录，它包括用户账号、发生时间、用户使用的操作命令及参数、客户端 IP 地址、用户访问设备及用户的使用设备的方式。上述数据再配合用户的计费策略设置，可用于用户使用系统的计费[5]。

## 4　结束语

该系统利用代理服务器软件的强大管理功能，对传统的“一人一机”模式的路由器访问管理进行了彻底改良，提高了设备的利用时间及利用率，同时，其操作命令的可管理性也避免了管理上的不确定性。并且，结合计费功能，可使远程网络实验室发挥有偿服务的能力。远程网络实验系统是解决路由器等网络设备基于 TCP/IP 网络实时培训、学习的较好解决方案。该方案不仅可用于路由器等设备的网络学习，还可通过更换指令集的方式适用于所有具有串行接口、符合终端规范的设备。

## 参考文献：


[1] 黎连业, 张维, 向东明. 路由器及其应用技术[M]. 北京: 清华大学出版社, 2004: 110-135.

[2] 朱星宇, 方湘涛, 顾保磊. 基于 Internet 的网络空调远程监控系统[J]. 兵工自动化, 2006, 25(1): 69-70.

[3] 束长宝, 于照, 张继勇. 基于 TCP/IP 的网络通讯及其应用[J]. 微机算计信息（管控一体化）, 2006, 12(3): 157-159.

[4] 希尔(Hill,B.). Cisco 完全手册[M]. 肖国尊, 等. 译. 北京: 电子工业出版社, 2006: 22-148.

[5] 胡武堂, 李锋, 黄万荣, 等. 模块化装备维修分队对口调度模型[J]. 四川兵工学报, 2009(5): 121-123.