

文章编号: 1005-8451(2007)11-0025-03

基于 Telnet 的网络设备配置软件的设计与实现

高 菲, 李红辉, 戴 钢

(北京交通大学 网络管理研究中心, 北京 100044)

摘要: 介绍网络管理中常用的 Telnet 协议, 分析其在网络设备配置上的作用, 提出基于 Telnet 协议的自动网络设备配置软件的设计思想, 并以 Cisco 路由器为例给出具体的程序实现方法。

关键词: Telnet; 网络管理系统; 网络设备配置; 设计

中图分类号: TP393.07 文献标识码: A

Design and implementation configuration software of network device based on Telnet

GAO Fei, LI Hong-hui, DAI Gang

(Network Management Research Center, Beijing Jiaotong University, Beijing 100044, China)

Abstract: It was introduced Telnet protocol and analysed its functions in network devices configuration. An idea of network devices automatic configuration based on Telnet was offered. Experiment program was introduced in detail.

Key words: Telnet; Network Management System; network devices configuration; design

随着计算机网络技术快速发展, 越来越多的业务应用都依赖于网络。网络管理系统是监视、配置和管理网络, 保证网络正常运行的重要工具。当网络出现问题时, 网络管理系统产生告警信息, 提示网络管理员进行相应处理。对于某些告警信息, 网络管理系统可以进行自动故障诊断及恢复。网络管理系统通常使用 SNMP 协议管理网络设备, 对网络设备进行信息提取及设置, 但是控制 MIB 对象的 Set 命令对设备的配置功能有限。由于网络设备都支持 Telnet 协议。通过 Telnet 登录到网络设备上, 可以对网络设备进行任意配置, 因此, 本文提出了一种基于 Telnet 协议, 用程序自动获取网络设备信息, 改变设备配置的软件设计思想, 并给出了在 Cisco4000 路由器上, 实现自动阻断 IP 或子网的一种 Java 程序实现。

1 Telnet简介

Telnet 是 TCP/IP 协议族中的一个虚拟终端协议, 它允许连接到远程主机。Telnet 运行在 OSI 参考模型的应用层, 利用 TCP 来保证在客户机和服务器之间正确和有序地传输数据。在日常的网管工作中, Telnet 最主要的作用是用来做远程连接到网络

收稿日期: 2007-03-29

基金项目: 北京交通大学校基金项目 (2005K2003)。

作者简介: 高 菲, 在读硕士研究生; 李红辉, 高级工程师。

设备, 进行设备的配置修改和状态检查工作。Telnet 协议以 23 号端口为传输端口, RFC845 定义了该协议的规范。

2 软件设计思想

网络管理系统对网络进行监视, 当网络中某一项指标超过阈值时, 产生告警信息, 需要网管系统自身或网管员调整网络状态以排除故障。由于网管系统对设备自动配置的局限性和网络管理员手工配置的繁琐性, 因此, 希望通过程序自动给网络设备发送命令, 完成配置的修改工作。基于以上思想, 网络设备配置软件配合网络管理系统自动完成网络设备配置的修改和更新。因网络设备都支持 Telnet 协议, 所以采用 Telnet 与网络设备进行交互。

网络设备配置软件是以程序的方式发送命令行来完成网络设备的配置管理。它主要分为 3 个模块。设备适配模块根据告警信息查找匹配设备及配置文件; 命令解析模块读取配置文件进行解析和替换, 生成目标命令脚本; 操作指令模块连接相应设备, 发送目标命令脚本进行配置。

以路由器为例, 应用程序根据告警信息自动找到相应的路由器, 并远程登录到该路由器上, 程序按照预先定义的格式和规则生成命令报文, 将此报文发送到 Telnet 协议, Telnet 协议完成打包和发送任务。当 Telnet 协议接收到响应报文时, 程序分析

该报文并列出报文内容及操作结果。发送给路由器的命令和参数按照一定的语法规则保存在配置文件中，程序将配置文件的内容解析和替换后生成目标脚本发送给路由器。

配置文件的作用是：存放各种型号网络设备对应的配置文件名称，对应网络设备的各个子功能的全部命令及参数列表。程序只需按照不同顺序读取配置文件中的各个子功能，就可以完成某个特定的功能。网络设备配置软件总体设计思路如图1。

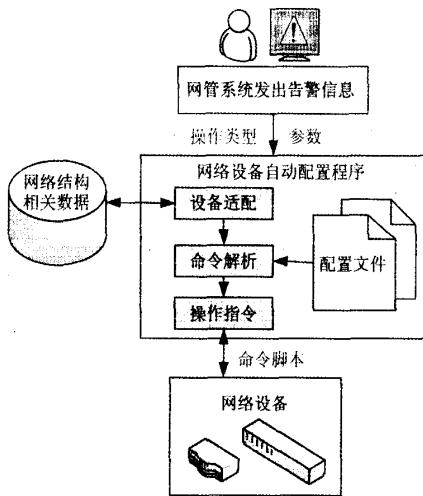


图1 网络设备配置软件总体设计思路

网络设备配置软件的目标是能够配置不同厂商、不同型号的网络设备。为了使程序与设备没有关联性，需要各种网络设备的命令列表，将命令相同的一类对应一个配置文件。如果各个厂商的某一类型的设备命令大致是相同的，例如：Cisco2500系列和Cisco4000的命令格式是相同的，就可使用相同的配置文件。

3 软件实现的关键技术

基于以上设计思想，开发了一个网络设备配置的实验程序，对Cisco4000路由器进行操作。该程序使用B/S结构，提供网页方式的操作界面，网管人员可以直接通过网页实现阻断或允许某个机器或某个子网的网络连接。

3.1 访问控制列表

Cisco路由器通过访问控制列表（access control

list, ACL）提供了基本的通信流量过滤能力。路由器的访问控制列表是网络安全保障的第一道关卡。访问控制列表提供了一种机制，它可以控制和过滤通过路由器的不同接口去往不同方向的信息流。这种机制允许用户使用访问控制列表来管理信息流，以制定公司内部网络的相关策略。这些策略可以描述安全功能，并且反映流量的优先级别。例如，某个组织可能希望允许或拒绝Internet对内部Web服务器的访问，或者允许内部局域网上一个或多个工作站能够将数据流发到广域网上。这些情形，以及其他的一些功能都可以通过访问控制列表来达到目的。

3.2 Jakarta Commons Net 介绍

程序使用Java语言开发，可以用代码实现Telnet协议也可以使用Jakarta Commons Net包。Jakarta Commons Net是一个用于操作Internet基础协议（Finger, Whois, TFTP, Telnet, POP3, FTP, NNTP, 以及SMTP）的底层API。Net包不仅支持对各种低层次协议的访问，而且还提供了一个高层的抽象。它使得开发者不再需要直接面对各种协议的Socket级的低层命令。可以使用Net中telnet包的connect方法与路由器建立连接，write方法向路由器发送命令。具体方法的使用请参看API文档。

3.3 禁止IP通信流量的实验程序实现

禁止某个IP，首先要找到该IP地址连接的路由器端口，然后修改端口的ACL。网络的相关数据需要存放在数据库中，以便程序进行端口的匹配。数据库中存放有路由器端口表，包括每个路由器的编号、端口名、IP及掩码信息。路由器子网表包括子网及掩码。路由器基本信息表，包括路由器的编号、名称、用户名、密码和型号。用户历史操作表记录用户的操作。设备状态表记录路由器上的ACL的情况。

本程序的重点就是解析配置文件，包含以下两个配置文件：device.ini，设备匹配文件。

cisco2500serial.ini，路由器对应的配置文件，存放各个子功能的命令行及参数表。

程序主要流程：程序获得给定的IP地址、子网掩码、操作类型（如：封禁、解封等），首先判断IP是否合法。如果合法，根据该IP地址、子网掩码，查询在路由器端口表和基本信息表，找到IP所在的路由器的记录。这样就得到了路由器的信息：编号、路由器端口IP、路由器端口IP的子网掩码、用户名、

密码、路由器型号和路由器所连网段。与路由器建立连接。再根据路由器型号读取设备匹配文件以找到设备配置文件；根据操作类型及参数，读取该路由器的配置文件，生成命令脚本，向路由器发送命令，从而完成指定操作。

程序的数据处理流程如图2。

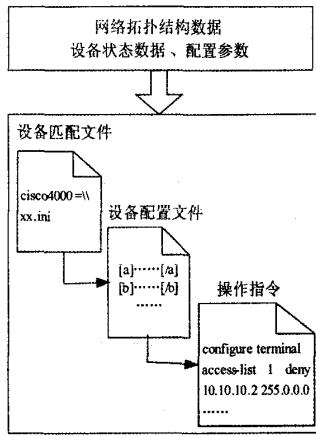


图2 数据处理流程图

程序与设备建立连接后，进行文件的读取，以获取有用的信息。

步骤1：device.ini的读取

该文件中存放了不同型号的路由器对应配置文件。程序找到cisco4000对应的配置文件是cisco2500serial.ini。文件内容如下：

```

cisco4000=\file\cisco2500serial.ini
cisco2500serial=\file\cisco2500serial.ini
cisco2600serial=\file\cisco2600serial.ini
...
  
```

步骤2：cisco2500serial.ini的读取

该文件的内容包括Cisco路由器的各个子功能。以“创建标准ACL”子功能为例，在[createStdACL]与[/createStdACL]之间是创建标准ACL的全部命令。以\$开头的是命令参数。[createStdACL_arguments]与[/createStdACL_arguments]之间的是参数个数、解释、名称和类型，这些是程序进一步完善时用到的。[createStdACL_comment]与[/createStdACL_comment]之间是命令的解释。程序读出相应的命令，将参数替换成实际值。发送给路由器就可以完成创建一个标准ACL的工作。接下来的工作程序将调用配置文件中的其它子功能模块完成，从而最终到达禁止某

个IP或网段通信流量的配置目的。文件中“创建标准ACL”子功能的内容为：

```

[createStdACL]
configure terminal
access-list $name deny $ip $wildcard
access-list $name permit any
interface $port
ip access-group $name $direct
exit
exit
[/createStdACL]
[createStdACL_arguments]
[argument_count]4[/argument_count]
[argument_comment]acl 表号,IP 地址,端口,流向
[/argument_comment]
[argument_name]acl_name,IP_address,port,direct
[/argument_name]
[argument_type]input,input,select,select
[/argument_type]
[/createStdACL_arguments]
[createStdACL_comment]创建标准ACL
[/createStdACL_comment]
...
  
```

4 结束语

本软件可以根据要求自动地完成网络设备的特定配置工作。将它作为网管系统的一个子系统，与其他功能模块配合使用，会提高网络管理系统的功能性。例如：当某一机器中了病毒时，网管系统的告警模块发出告警事件，激活网络配置模块，网络配置模块根据网络拓扑模块发现的网络结构相关数据，定位网络设备并对子网实行阻断操作，这样就阻止了病毒的传播。Telnet协议传输的数据都是用明文方式传送的，因此，很容易被第三方嗅探工具捕获到，我们可以通过路由器的访问控制列表来限制Telnet到设备的IP地址来解决。

参考文献：

- [1] Cisco Systems公司.思科网络教育学院教程[M].(第2版)北京：人民邮电出版社，2002，6.
- [2] 马坤，杨波.Telnet协议在网管系统中的应用[J].信息技术与信息化，2006（4）：125-130.