基 于 eNSP 的 防 火 墙 仿 真 实 验

孟 祥 成
(三江学院 计算机科学与工程学院,江苏 南京 210012)

摘　要: 介绍了防火墙的原理和工作模式,从防火墙教学实验出发,以工程案例为引导,设计教学实验目的、拓扑结构、实验环境。利用 eNSP 软件仿真防火墙技术实验,实验给出了详细的设计方法、拓扑结构、配置过程和配置命令,并对实验结果进行验证和分析。实验证明,通过防火墙仿真实验的设计和验证,学生能够更好地了解网络设备与加深巩固理论教学的内容,该仿真实验方法在计算机网络实践课程的实验教学中取得了良好的效果。

关键词: eNSP; 仿真; 防火墙
中图分类号: TP 393　　**文献标志码:** A
文章编号: 1006 - 7167(2016)04 - 0095 - 06

Firewall Simulation Experiment Based on eNSP

MENG Xiang-cheng
(Sanjiang College Department of Computer Science and Technology, Nanjing 210012, China)

Abstract: The article introduced the principle and working mode of firewall from the point of the view of the firewall experimental teaching. The article used the case of engineering as the guide, and discussed the design of teaching experimental purposes, experimental topology and experimental environment. It used the ENSP as simulation software to design topology and configure experiment, it first introduced the teaching environment of simulation laboratory, then discusseds and provided the detailed design procedures and configuration commands. It also testified and analyzed the experimental results. Experiments show that students can learn about the network devices, and also console the theory teaching content better through the specific design and test of firewall simulation experiments; at last the method has gained favorable effect in the experimental teaching of computer network practice course.

Key words: eNSP; simulation; firewall

0　引　言

随着“互联网 +”越来越火热,互联网作用又上升了一个层次,网络安全越来越受到重视,防火墙在互联网中的安全作用不言而喻。而现实中由于防火墙教学设备缺乏或因设备昂贵无财力购买,影响了实验教学[1]。笔者设计的防火墙仿真实验案例,能够很好地仿真防火墙技术,达到和现实中真实设备一样的效果。

收稿日期: 2015 - 09 - 22

作者简介: 孟祥成(1981 -),男,江苏灌南人,硕士,实验师,研究方向计算机网络技术。Tel.:15345185087; E-mail: mxiang5087@qq.com

1　防火墙的基本原理和工作模式

1.1　防火墙的基本原理

防火墙技术作为一种隔离内部安全网络与外部不信任网络的防御技术,已经成为计算机网络安全体系结构中的一个重要组成部分。所谓的防火墙指的是一个由软件与硬件设备组合而成、在内部网与外部网之间、专用网与公共网之间的界面上构造的保护隔离屏障,是一种获取安全性方法的形象说法,它是一种计算机硬件和软件的结合,使 Internet 与 Intranet 之间建立起一个安全网关(Security Gateway),从而保护内部网免受非法用户的侵入,防火墙主要由服务访问规则、验证工具、包过滤和应用网关 4 个部分组成,防火墙就是

一个位于计算机和它所连接的网络之间的软件或硬件。该计算机流入流出的所有网络通信和数据包均要经过此防火墙[2]。

1.2 防火墙工作模式

防火墙工作模式主要有 3 种: 路由模式、透明模式和混合模式。

路由模式是指设备接口具有 IP 地址,通过 3 层与外连接; 透明模式是指设备接口没有 IP 地址,通过 2 层对外连接; 混合模式是指设备接口既有工作在路由模式的接口,又有工作在透明模式的接口。

2 eNSP 仿真软件

eNSP(Enterprise Network Simulation Platform) 是一款由华为提供的免费的、可扩展的、图形化的网络设备仿真平台,主要对企业网路由器、交换机、WLAN 等设备进行软件仿真,完美呈现真实设备部署实景,支持大型网络模拟,可以在没有真实设备的情况下也能够开展实验测试,学习网络技术。目前最新版华为模拟器为 eNSP v1.2.00.360。

3 实验设计分析

3.1 实验目的

实验的目的为: ①了解防火墙基本原理; ②理解防火墙工作模式; ③掌握防火墙配置过程; ④掌握 eNSP 使用方法。

3.2 具体实训项目及指导思想

以工程案例为指导思想,以企业真实的工程项目为依据,将现实中的工程项目分解成多个子项目逐步完成,最终将实际任务搭建成实验室的具体实验项目来完成[3]。南京某 IT 公司因业务需要,在另一个城市昆山建立了子公司,现在要求子公司研发小组能够通过 Internet 把子公司关键业务机密数据安全地传给总公司。要求子公司可以访问总公司的 Web 服务器、FTP 服务器、Telnet 服务器。总公司通过防火墙连接 Internet,子公司通过路由器连接到 Internet。使用防火墙技术解决这个问题,采取的主要实验步骤为: ①需求分析; ②拓扑结构设计; ③实验环境的配置; ④具体实验步骤; ⑤实验结果验证。

3.3 网络拓扑结构仿真设计

在 eNSP 工作区绘制网络拓扑结构仿真图,如图 1 所示。

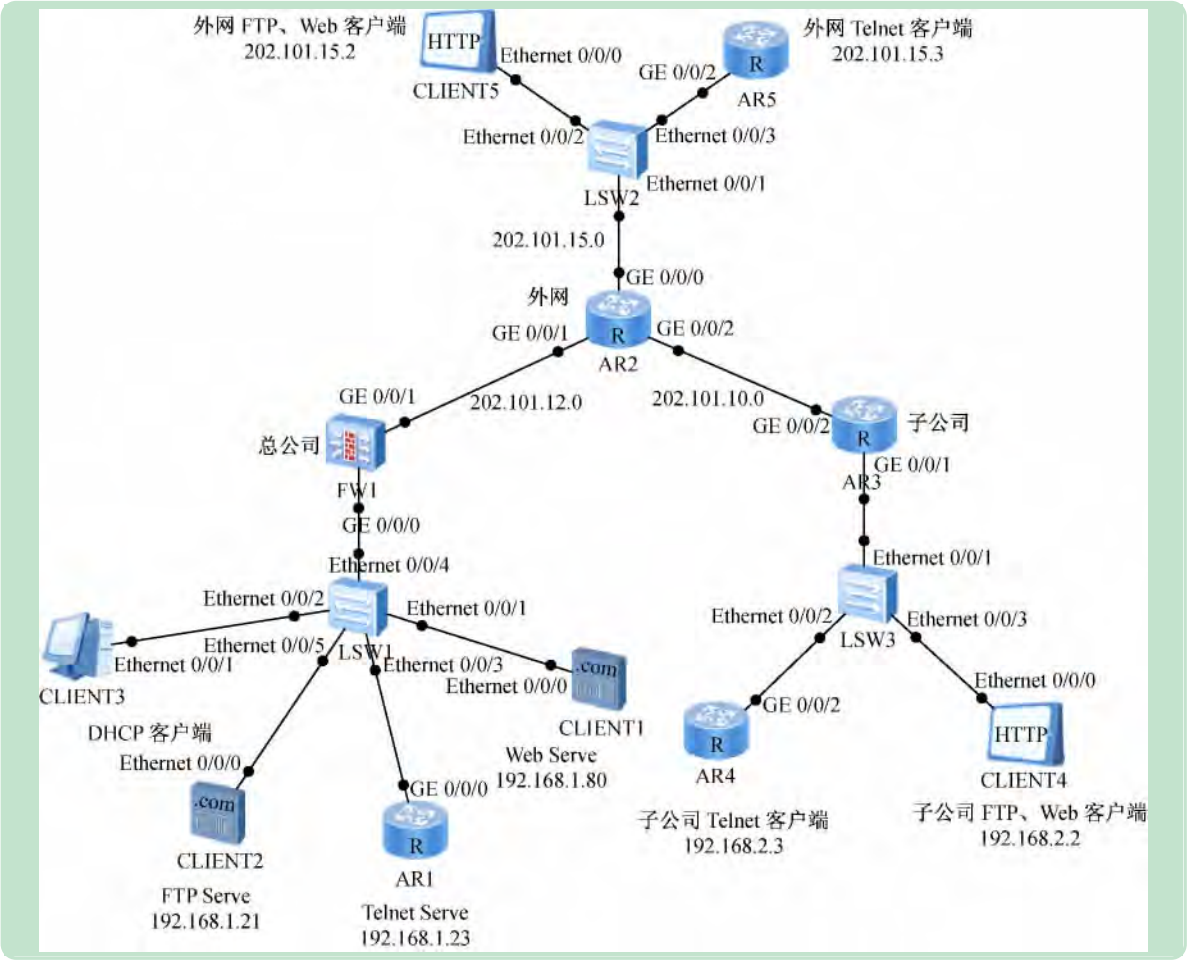

图 1 网络拓补结构图

3.4　实验环境配置

(1) 设备选择。在进行仿真实验时,选择设备防火墙 USG5500 1 台,为 FW1,作为总公司连接外网 Internet 接入设备; 路由器 AR2220 5 台,分别为 AR1 ~ AR5,其作用分别是: 模拟 Telnet 服务器、模拟 Internet 网络、子公司连接 Internet 接入设备、模拟子公司 Telnet 客户端、模拟 Internet 外网 Telnet 客户端; 服务器 Server 2 台,分别为 CLIENT1、CLIENT2,其中 1 台作为 Web Server,另外 1 台作为 FTP Server; PC 模拟器 3 台,分别为 CLIENT3、CLIENT4、CLIENT5,CLIENT3 作为公司南京总部内网普通 PC 机,CLIENT4 作为昆山子公司 PC 客户端访问 Web Server 和 FTP Server,CLIENT5 作为外网 PC 客户端测试服务器; 交换机 S3700 3 台,为 LSW1、LSW2、LSW3,分别为总公司内部组网设备、子公司组网设备、外网设备。

(2) 设备互连。设备端口互连情况,如图 1 所示。

(3) IP 地址规划。为了达到逼真接近现实环境的效果,首先要规划一下 IP 地址。将南京总部与昆山子公司各自内部主机地址都设置为私有的 IP 地址,南京总部为 192.168.1.0/24,昆山子公司为 192.168.2.0/24。将南京总部与外网 Internet 相连部分的网段设置为 202.101.12.0/24,昆山子公司与外网 Internet 相连部分的网段设置为 202.101.10.0/24,外网 Internet 所包含网段为 202.101.15.0/24。

4　网络组建

4.1　总公司网络组建

对总公司防火墙、服务器端设备配置,可以组建一个总公司局域网,主要分为以下几个步骤:

4.1.1　Web Server 与 FTP Server 终端设备 IP 地址配置

双击 CLIENT1,在基础配置窗口中将 Web Server IP 地址设置为 192.168.1.80,子网掩码为 255.255.255.0,网关设置为 192.168.1.1,如图 2 所示。CLIENT2,作为 FTP 服务器, IP 地址设置方法与 CLIENT1 地址设置方法相同,设置为 192.168.1.21,子网掩码为 255.255.255.0,网关设置为 192.168.1.1。CLIENT3,作为总公司内网普通主机,采取 DHCP 自动分配获得 IP 地址。

4.1.2　Telnet 服务器配置

配置 Telnet 服务器接口与远程登录方式,双击路由器 AR1,在弹出窗口输入命令配置 Telnet Server,主要命令如下:

〈Huawei〉system-view //进入系统视图界面

[Huawei] sysname AR1 //修改设备名称为 AR1

[AR1] interface GigabitEthernet 0/0/0 //进入接口 GE0/0/0

图 2　Web 服务器 IP 地址配置

[AR1-GigabitEthernet0/0/0] ip address 192.168.1.23 24 //配置 IP 地址与子网掩码

[AR1-GigabitEthernet0/0/0] quit //退出接口界面

[AR1] ip route-static 0.0.0.0 0.0.0.0 192.168.1.1 //定义默认路由,实现网络连通

[AR1] user-interface vty 0 4 //为 AR1 配置登录方式为密码验证登录

[AR1-ui-vty0-4] authentication-mode password

Please configure the login password (maximum length 16): tel123 //设置密码为 tel123

4.1.3　防火墙 FW1 的配置

(1) 采取路由模式配置防火墙内网与外网的接口,并加入到相应的 zone,内网开启 DHCP。双击防火墙 FW1,在弹出窗口输入命令配置 FW1,主要命令如下:

〈SRG〉system-view //进入系统视图界面

[SRG] sysname FW1 //修改设备名称

[FW1] interface GigabitEthernet 0/0/0 //进入接口 GE0/0/0

[FW1-GigabitEthernet0/0/0] ip address 192.168.1.1 24 //配置 IP 地址与子网掩码

[FW1-GigabitEthernet0/0/0] dhcp select interface //关联接口

[FW1-GigabitEthernet0/0/0] dhcp server gateway-list 192.168.1.1 //配置客户端网关

[FW1-GigabitEthernet0/0/0] quit //退出接口界面

[FW1] ip route-static 0.0.0.0 0.0.0.0 202.101.12.2 //添加默认路由

[FW1] firewall zone trust //进入 trust 安全区域视图

[FW1-zone-trust] add interface GigabitEthernet0/0/0 //将接口加入到 trust 区域

[FW1-zone-trust] quit //退出

[FW1] firewall zone untrust //进入 untrust 安全区域视图

[FW1-zone-untrust] add interface GigabitEthernet0/0/1 //将接口加入到 untrust 区域

[FW1-zone-untrust] quit //退出

(2) 配置完成后,内网 PC 可以获得地址,防火墙可以 ping 外网设备的地址,但是外网设备没法进行

ping 防火墙，所以放行 untrust 到 local 的 inbound 的策略里面的 icmp 和 telnet，配置如下：

[FW1] policy interzone local untrust inbound

[FW1-policy-interzone-local-untrust-inbound] policy 1

[FW1-policy-interzone-local-untrust-inbound-1] action permit

[FW1-policy-interzone-local-untrust-inbound-1] policy service service-set icmp

[FW1-policy-interzone-local-untrust-inbound-1] policy service service-set telnet

[FW1-policy-interzone-local-untrust-inbound-1] policy service service-set ftp

[FW1-policy-interzone-local-untrust-inbound-1] policy service service-set http

(3) 开启 trust 到 untrust 的默认行为允许。

[FW1] firewall packet-filter default permit interzone trust untrust direction outbound

(4) 开启防火墙的 NAT，允许内网访问外网的 NAT 策略。

[FW1] nat address-group 1 202.101.12.1 202.101.12.1 //创建 NAT 地址池

[FW1] nat-policy interzone trust untrust outbound //配置 trust 到 untrust 的 NAT Outbound 规则

[FW1-nat-policy-interzone-trust-untrust-outbound] policy 1

[FW1-nat-policy-interzone-trust-untrust-outbound-1] action source-nat

[FW1-nat-policy-interzone-trust-untrust-outbound-1] policy source 192.168.1.0 mask 24

[FW1-nat-policy-interzone-trust-untrust-outbound-1] address-group 1

(5) 设置允许外网访问 telnet Server、FTP Server、Web Server，telnet 使用端口号为 2323，其它服务器选择默认端口。先做 NAT，再匹配策略。

[FW1] nat server 0 protocol tcp global interface GigabitEthernet0/0/1 2323 inside 192.168.1.23 telnet //配置 NAT Server telnet 规则

[FW1] nat server 1 protocol tcp global interface GigabitEthernet0/0/1 ftp inside 192.168.1.21 ftp //配置 NAT Server FTP 规则

[FW1] nat server 2 protocol tcp global 202.101.12.1 www inside 192.168.1.80 www //配置 NAT Server http 规则

[FW1] policy interzone trust untrust inbound //配置 trust 到 untrust 的 NAT Inbound 规则

[FW1-policy-interzone-trust-untrust-inbound] policy 1

[FW1-policy-interzone-trust-untrust-inbound-1] action permit

[FW1-policy-interzone-trust-untrust-inbound-1] policy service service-set telnet

[FW1-policy-interzone-trust-untrust-inbound-1] policy service service-set ftp

[FW1-policy-interzone-trust-untrust-inbound-1] policy service service-set http

[FW1-policy-interzone-trust-untrust-inbound-1] policy destination 192.168.1.23 0

[FW1-policy-interzone-trust-untrust-inbound-1] policy destination 192.168.1.21 0

[FW1-policy-interzone-trust-untrust-inbound-1] policy destination 192.168.1.80 0

4.2 子公司网络组建

对子公司路由器、客户端设备配置，可以组建一个子公司小型局域网，主要分为 3 步，配置步骤如下：

(1) 路由器 AR3 配置。配置子公司路由器 AR3 连接内网的接口，并配置 Easy-IP 地址转换，双击路由器 AR3，在弹出窗口输入命令，主要配置命令如下：

〈Huawei〉system-view //进入系统视图界面

[Huawei] sysname AR3 //修改设备名称为 AR3

[AR3] interface GigabitEthernet 0/0/1 //进入接口 GE0/0/1

[AR3-GigabitEthernet0/0/1] ip address 192.168.2.1 24 //配置 IP 地址与子网掩码

[AR3-GigabitEthernet0/0/1] quit //退出接口界面

[AR3] interface GigabitEthernet 0/0/2 //进入接口 GE0/0/2

[AR3-GigabitEthernet0/0/2] ip address 202.101.10.2 24 //配置 IP 地址与子网掩码

[AR3] ip route-static 0.0.0.0 0 202.101.10.1 //添加默认路由

[AR3] acl 2001 //定义 ACL 2001

[AR3-acl-basic-2001] rule 5 permit source 192.168.2.0 0.0.0.255 //定义规则源地址

[AR3-acl-basic-2001] quit //退出

[AR3] interface GigabitEthernet0/0/2 //进入接口 G0/0/2

[AR3-GigabitEthernet0/0/2] nat outbound 2001 //对 ACL 2001 定义的地址段进行地址转换，并且直接使用 G0/0/2 接口的 IP 地址作为 NAT 转换后的地址

(2) Telnet 客户端配置。双击路由器 AR4，在弹出窗口输入命令配置 Telnet 客户端，主要命令如下：

〈Huawei〉system-view //进入系统视图界面

[Huawei] sysname AR4 //修改设备名称为 AR4

[AR4] interface GigabitEthernet 0/0/2 //进入接口 GE0/0/2

[AR4-GigabitEthernet0/0/1] ip address 192.168.2.3 24 //配置 IP 地址与子网掩码

[AR4-GigabitEthernet0/0/1] quit //退出接口界面

[AR4] ip route-static 0.0.0.0 0.0.0.0 192.168.3.1 //定义默认路由，实现网络连通

(3) FTP、Web 客户端配置。双击 CLIENT4，在基础配置窗口中将 IP 地址设置为 192.168.2.2，子网掩码为 255.255.255.0，网关设置为 192.168.2.1，与 Web 服务器 IP 地址配置方法相同，可参照图 2。

4.3 外网 Internet 配置

(1) 路由器 AR2 配置。配置路由器 AR2 接口，并运行 rip 协议关联网络。

〈Huawei〉system-view //进入系统视图界面

[Huawei] sysname AR2 //修改设备名称为 AR4

[AR2] interface GigabitEthernet 0/0/1 //进入接口 GE0/0/1

[AR2-GigabitEthernet0/0/1] ip address 202.101.12.2 24 //配置 IP 地址与子网掩码

[AR2-GigabitEthernet0/0/1] quit //退出接口界面

[AR2] interface GigabitEthernet 0/0/2 //进入接口 GE0/0/2

[AR2-GigabitEthernet0/0/2] ip address 202.101.10.1 24 //配置 IP 地址与子网掩码

[AR2-GigabitEthernet0/0/2] quit //退出接口界面

[AR2] interface GigabitEthernet 0/0/0 //进入接口 GE0/0/0

[AR2-GigabitEthernet0/0/0] ip address 202.101.15.1 24 //配置 IP 地址与子网掩码

[AR2-GigabitEthernet0/0/0] quit //退出接口界面

[AR2] rip //开启 rip 进程

[AR2] version 2 //运行 v2 版本

[AR2-rip-1] network 202.101.12.0 //宣告网络

[AR2-rip-1] network 202.101.10.0 //宣告网络

[AR2-rip-1] network 202.101.15.0 //宣告网络

(2) Internet Telnet 客户端配置。双击路由器 AR5,在弹出窗口输入命令配置外网 Telnet 客户端,主要命令如下:

〈Huawei〉system-view //进入系统视图界面

[Huawei] sysname AR5 //修改设备名称为 AR5

[AR5] interface GigabitEthernet 0/0/2 //进入接口 GE0/0/2

[AR5-GigabitEthernet0/0/2] ip address 202.101.15.3 24 //配置 IP 地址与子网掩码

[AR5-GigabitEthernet0/0/2] quit //退出接口界面

[AR5] ip route-static 0.0.0.0 0.0.0.0 202.101.15.1 //定义默认路由,实现网络连通

(3) 外网 FTP、Web 客户端配置。双击 CLIENT5,在基础配置窗口中将 IP 地址设置为 202.101.15.2,子网掩码为 255.255.255.0,网关设置为 202.101.15.1,与 Web 服务器 IP 地址配置方法相同,可参照图 2。

4.4　防火墙策略配置

要实现子公司客户端可以访问总公司服务器,限制外网 Internet 客户端访问总公司服务器,还需在总公司防火墙做以下配置:

[FW1] policy interzone trust untrust inbound //配置 trust 到 untrust 的 NAT Inbound 规则

[FW1-policy-interzone-trust-untrust-inbound] policy 1

[FW1-policy-interzone-trust-untrust-inbound-1] policy source 202.101.10.2 0//添加策略,指定子公司网段地址可以访问总公司服务器

5　实验结果验证

5.1　全网互通仿真实验结果

通过上述 4.1 ~ 4.3 节实验过程操作,可以实现子公司与总公司、外网 Internet 与总公司之间相互通信。通过验证外网客户端、子公司客户端可以访问总公司的 Web 服务器、FTP 服务器、Telnet 服务器。

5.2　仿真实验最终结果

在全网互通的基础上,总公司防火墙添加策略配置,见 4.4 节实验过程操作,实现了外网 Internet 不能访问总公司服务器,而子公司客户端可以访问总公司的 Web 服务器、FTP 服务器、Telnet 服务器。双击子公司 Telnet 客户端 AR4,输入“telnet 202.101.12.1 2323”,回车,提示输入密码,输入 Telnet 服务器远程登录密码“tel123”,即成功登录 Telnet 服务器 AR1,见图 3 所示。而在外网客户端 AR5 中输入“telnet 202.101.12.1 2323”,则提示不能访问 Telnet 服务器。

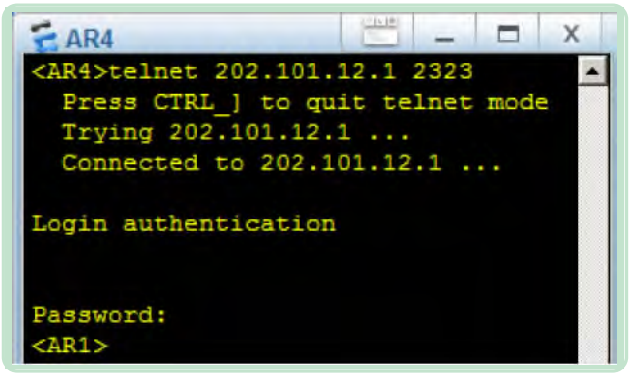

图 3　子公司客户端成功登录 Telnet 服务器

开启总公司 FTP、Web 服务器,在子公司客户端访问 FTP 服务器和 Web 服务器,显示可以登录访问。而在外网 Internet 客户端访问总公司服务器,则显示不能访问。

6　结　语

笔者所设计的防火墙仿真虚拟实验,以工程案例为背景,逼真地模拟了现实环境,让学生可以完成实际工程项目积累真实的经验,既达到了教学的目的,又能降低设备财力投入。

参考文献(References):

[1] 唐灯平,朱艳琴,杨　哲. 计算机网络管理仿真平台防火墙实验设计[J]. 实验技术与管理,2015(4):156-160.

[2] 孟祥丰,白永祥著. 计算机网络安全技术研究[M]. 北京: 北京理工大学出版社,2013.10.

[3] 唐灯平. 基于 PacketTracer 的 GRE 隧道配置实验教学设计[J]. 实验室研究与探索,2010(11):378-381.

[4] 范　君,高成强. 基于 Packet Tracer 的帧中继实验设计与分析[J]. 实验室研究与探索,2012(4):208-212.

[5] 曹腾飞,孟永伟,黄建强. 西部高校计算机网络实验[J]. 实验室研究与探索,2014(4):129-131.

[6] 龙艳军,欧阳建权,俞佳曦. 基于 GNS3 和 VMware 的虚拟网络系统集成实验室研究[J]. 实验技术与管理,2013(2):90-93.

[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] 田安红,付承彪. NAT 原理实验在仿真器中的设计与实现[J]. 实验技术与管理,2013(2):135-138.

[9] 姜恩华. 基于 Packet Tracer 软件的防火墙技术实验教学设计[J]. 通化师范学院学报,2013(8):45-47.
[10] 张 磊. 安全网络构建中防火墙技术的研究与应用[D]. 济南:山东大学,2009.
[11] 姜恩华,窦德召. Packet Tracer 软件在无线网络技术实验教学中的应用[J]. 实验技术与管理,2011(10):88-91.
[12] 邹 航,李 梁. 整合 ACL 和 NAT 的网络安全实验设计[J]. 实验室研究与探索,2011(4):61-65.
[13] 唐灯平. 构建安全的虚拟专用网环境技术[J]. 实验科学与技术,2011(3):49-50.
[14] 唐灯平. 基于 Packet Tracer 的 IPv6 静态路由实验教学设计[J]. 实验科学与技术,2011(3):49-50.
[15] 周 敏,龚 箭. “计算机网络安全”实验教学研究[J]. 实验技术与管理,2011(9):145-148.
[16] 肖宇峰,沈 军. 电信运营商防火墙测试技术的研究与应用[J]. 电信技术,2013(10):9-13.
[17] 唐灯平. 利用 Packet Tracer 模拟组建大型单核心网络的研究[J]. 实验室研究与探索,2011(1):186-189.

(上接第 42 页)

参考文献(References):

[1] 方建钢. 太阳能跟踪控制系统的研究与设计[D]. 武汉:武汉理工大学,2011.
[2] 赵 杰. 基于超声电机的双轴太阳能跟踪系统[D]. 南京:南京航空航天大学,2012.
[3] 徐海鹏. 双轴式太阳能自动跟踪系统[D]. 北方工业大学,2014.
[4] 樊峰鸣,马良涛. 单轴太阳能跟踪系统的研究[J]. 河南城建高等专科学校学报,2000(3):43-45.
[5] 邸 斌,宋宏明. 一种新型太阳能跟踪系统的研究[J]. 哈尔滨理工大学学报,2012(2):67-71.
[6] 王 成,钟登翔,高峻峣. 两自由度太阳能跟踪系统设计[J]. 机床与液压,2012,13:124-128.
[7] 魏浩然,李传江,翁志明,等. 小型被动式双轴太阳能跟踪装置的设计与应用[J]. 电子制作,2012(12):97-98,151.
[8] 张翠云,陈学永,陈仕国,等. 基于 PLC 的双轴太阳能跟踪控制系统设计[J]. 福州大学学报(自然科学版),2013(6):1051-1055.
[9] 黄 勇. 关于斜单轴太阳能跟踪器的轴承简易密封问题[J]. 大众科技,2010(7):120-122.
[10] 牟 娟. 光伏电站可调式支架经济效益分析[J]. 可再生能源,2013,31(6):23-25.
[11] 黄天云. 倾角可调光伏支架结构的研究[J]. 太阳能,2013(15):34-37.
[12] 陈 艳. 大型光伏电站中不同支架方案比较分析[J]. 电气技术,2013(8):16-19.
[13] 青海省水利水电勘测设计研究院工程勘察分院,青海省发展投资有限公司扎苏合 10 MW 光伏发电工程电站勘察报告[R]. 2012.9
[14] 上海电力设计院,青海省发展投资有限公司扎苏合 10 MW 光伏发电工程电站可行性研究报告[R]. 2012.9
[15] GB50009-2012,建筑结构荷载规范[S]. 北京:中国建筑工业出版社,2012.

(上接第 89 页)

[4] 魏天锋,龚荣洲. 智能在线测厚系统的设计[J]. 仪表技术与传感器,2006(8):39-40,43.
[5] Syasko V A, Measuring the thicknesses of nonferromagnetic metal coatings on nonferrous metal products using the eddy-current frequency method[J]. Russian Journal of Nondestructive Testing, 2010, 46(12): 898-905.
[6] 郑 岗,刘 丁. 基于提离点的脉冲涡流测厚研究[J]. 仪器仪表学报,2008,29(8):1745-1749.
[7] 岳秀芳,王召巴,张东利. 涡流检测的厚涂层高精度方法[J]. 仪表技术与传感器,2014(2):99-101.
[8] Zilian Q. Improvement of sensitivity of eddy current sensors for nano-scale thickness measurement of Cu films[J]. Nondestructive Testing and Evaluation International. 2014(61):53-57.
[9] Tian S, Chen K, Bai L, *et al*. Frequency feature based quantification of defect depth and thickness[J]. Review of Scientific Instruments. 2014, 85(6): 64705.
[10] 任吉林. 碳纤维复合材料涂层厚度涡流法测量的研究[J]. 仪器仪表学报,2011,32(12):2662-2668.
[11] 柯 海,武新军. 基于信号斜率的铁磁材料脉冲涡流测厚研究[J]. 仪器仪表学报,2011,32(10):2376-2381.
[12] 任芳芳,雷银照. 三层平板导体厚度及电导率的涡流检测[J]. 无损检测,2013,35(8):50-53.
[13] 周德强,李 勇,张秋菊. 脉冲涡流金属厚度检测信号及其特征提取[J]. 中国机械工程,2012(15):1771-1773+1778.
[14] Ribeiro A Lopes, Ramos H. Liftoff insensitive thickness measurement of aluminum plates using harmonic eddy current excitation and a GMR sensor[J]. Measurement, 2012, 45(9): 2246-2253.
[15] 王旻玥,康宜华,叶志坚. 多通道电磁超声测厚系统[J]. 仪表技术与传感器,2015(6):75-76+91.
[16] Zilian Q, Qian Z, Yonggang M. In-situ measurement of Cu film thickness during the CMP process by using eddy current method alone[J]. Microelectronic Engineering, 2013(108): 66-70.

·名人名言·

没有伟大的品格,就没有伟大的人,甚至也没有伟大的艺术家,伟大的行动者。

——罗曼·罗兰