# <<计算机网络安全与管理>>

## 图书基本信息

书名：<<计算机网络安全与管理>>

13位ISBN编号：9787302218180

10位ISBN编号：7302218188

出版时间：2010-3

出版时间：田庚林、田华、 张少芳 清华大学出版社 (2010-03出版)

作者：田庚林，田华，张少芳 著

页数：264

## 前言

本书是一本面向高等职业教育的教材，是计算机网络技术专业系列教材之一。
在计算机网络技术专业建设中，从网络工程、网络管理岗位需求出发，我们将专业技能重点放在网络技术和网站技术两个方面。
该专业系列教材中，将网络技术分为《计算机网络技术基础》、《计算机网络集成技术》、《计算机网络安全与管理》和《网络操作系统》4门课程；网站技术主要包括《网页制作工具》、《网络数据库》、《动态网站技术》和《.NET网站技术》4门课程。
本书主要介绍网络安全技术和基本的网络管理知识与基本管理技能。
本书以一个模拟的网络工程为主线，分析网络工程中的安全需求与管理任务；按照需求制定工程任务，按照任务需要介绍必备的知识，提出模拟工程中的解决方案，完成方案配置。
本书内容既以工程需求为主，同时还照顾了知识体系的完整性与系统性。
为了便于学生在实验室中对解决方案的配置、验证和测试，书中给出了一个网络安全与管理实训工程环境，实训环境可使用实际网络设备实现，也可使用模拟器软件实现。
第2章至第7章的每章章后都有实训内容和实训指导，让学生根据在模拟工程实践中学到的知识技能完成实训项目，提高学生的动手能力与实践技能。

# <<计算机网络安全与管理>>

## 内容概要

《计算机网络安全与管理》介绍了计算机网络安全与管理技术，是面向高职高专计算机网络技术专业的教材。

《计算机网络安全与管理》以一个模拟网络工程为主线，分析网络工程中的安全管理需求，根据需求制定工程任务，按照任务介绍必备的知识，提出模拟工程中的解决方案，完成方案配置。

《计算机网络安全与管理》共分7章，内容包括模拟网络工程环境和模拟网络工程中的网络安全与管理需求分析、访问控制列表技术、局域网安全、网络地址转换技术、VPN技术、防火墙技术、网络管理技术。

《计算机网络安全与管理》可以作为高职高专计算机网络技术及相关专业的教材，也可以作为网络工程技术人员和本科院校学生的参考书。

# <<计算机网络安全与管理>>

## 书籍目录

第1章 计算机网络安全与管理任务分析 1.1 公司网络环境 1.1.1 企业网络应用概况 1.1.2 企业网络拓扑结构 1.2 模拟公司网络安全及管理需求 1.2.1 模拟公司的网络安全管理需求 1.2.2 模拟公司的网络管理需求 1.3 网络安全及管理实验环境 第2章 访问控制列表技术 2.1 模拟公司分支机构网络边界安全任务分析 2.1.1 模拟公司分支机构网络边界安全风险分析 2.1.2 模拟公司分支机构网络边界安全配置方案 2.2 访问控制列表的基础知识 2.2.1 访问控制列表的概念 2.2.2 ACL类型 2.2.3 ACL工作过程 2.2.4 ACL配置规则和应用位置 2.3 无状态ACL配置方法 2.3.1 标准ACL配置步骤 2.3.2 扩展ACL配置步骤 2.3.3 定时ACL配置步骤 2.3.4 分片ACL配置 2.4 有状态ACL配置 2.4.1 反射ACL简介 2.4.2 反射ACL配置方法 2.5 基于上下文ACL配置 2.5.1 CBAC简介 2.5.2 CBAC配置方法 2.6 模拟公司分支机构网络边界安全访问控制列表配置示例 2.7 小结 2.8 习题 2.9 实训 2.9.1 无状态ACL配置 2.9.2 有状态及基于上下文ACL配置 第3章 局域网安全 3.1 模拟网络局域网安全任务分析 3.2 AAA技术 3.2.1 AAA及RADIUS简介 3.2.2 AAA配置方法 3.2.3 模拟网络的AAA配置 3.3 IEEE 802.1x技术 3.3.1 IEEE 802.1x技术简介 3.3.2 IEEE 802.1x配置方法 3.3.3 模拟公司总部局域网IEEE 802.1x配置案例 3.4 交换机访问控制列表技术 3.4.1 交换机访问控制列表技术简介 3.4.2 配置VACL 3.4.3 配置PACL 3.4.4 模拟公司总部局域网交换机访问控制列表配置案例 3.5 端口安全技术 3.5.1 端口安全技术简介 3.5.2 交换机端口安全配置方法 3.5.3 模拟公司总部局域网端口安全配置案例 3.6 DHCP监听、IP源防护与ARP检测技术 3.6.1 DHCP攻击及DHCP监听技术简介 3.6.2 IP地址欺骗及IP源防护技术简介 3.6.3 ARP攻击及ARP检测技术简介 3.6.4 DHCP监听配置方法 3.6.5 IP源防护技术配置方法 3.6.6 DAI配置方法 3.6.7 模拟公司总部局域网DHCP监听、IP源防护与.ARP检测配置案例 3.7 私有VLAN 3.7.1 私有VLAN与受保护端口技术简介 3.7.2 受保护端口、私有VLAN配置方法 3.7.3 模拟公司总部局域网PVLAN配置 3.8 VLAN跳跃攻击与防护 3.9 小结 3.10 习题 3.11 实训 3.11.1 AAA配置 3.11.2 交换机端口安全配置 3.11.3 局域网IEEE 802.1x配置 3.11.4 局域网交换机访问控制 3.11.5 DHCP攻击、IP地址欺骗攻击、ARP攻击防护 第4章 网络地址转换技术 4.1 模拟公司分支机构网络地址转换任务分析 4.2 网络地址转换简介 4.2.1 地址转换工作过程 4.2.2 网络地址转换类型及术语 4.2.3 地址转换与访问控制 4.2.4 网络地址转换存在的问题 4.3 路由器网络地址转换配置 4.3.1 静态NAT配置 4.3.2 动态NAT配置 4.3.3 动态PAT配置 4.3.4 端口地址重定向配置 4.3.5 外部地址转换配置 4.4 模拟公司分支机构地址转换配置方案 4.5 小结 4.6 习题 4.7 实训 第5章 VPN技术 5.1 模拟公司网络安全通信配置任务分析 5.2 VPN简介 5.2.1 VPN技术及通信安全 5.2.2 IPSec VPN 5.3 IPSec VPN配置 5.3.1 站到站VPN配置 5.3.2 远程访问VPN配置 5.4 模拟公司网络安全通信配置方案 5.5 小结 5.6 习题 5.7 实训 5.7.1 站到站VPN配置 5.7.2 远程访问VPN配置 第6章 防火墙 6.1 模拟公司总部网络内外网边界安全任务分析 6.2 防火墙简介 6.3 网络连通性配置 6.3.1 接口及路由配置 6.3.2 路由配置及检查 6.3.3 地址转换配置 6.3.4 无状态访问控制配置 6.4 VPN配置 6.4.1 站到站VPN配置 6.4.2 远程访问VPN配置 6.5 模拟公司总部边界防火墙配置方案 6.6 小结 6.7 习题 6.8 实训 6.8.1 防火墙网络连通性及访问控制配置 6.8.2 防火墙预共享密钥站到站VPN配置 第7章 网络管理技术 7.1 模拟公司网络管理任务分析 7.2 网络管理技术概述 7.2.1 网络管理模型 7.2.2 网络管理体系结构 7.2.3 SNMP协议 7.2.4 MIB与SMI 7.2.5 网络管理工具 7.3 网络配置管理 7.4 网络故障管理 7.4.1 网络故障监测 7.4.2 网络故障分析定位 7.5 网络安全管理 7.5.1 网络安全管理概述 7.5.2 网络安全审查 7.5.3 入侵检测与入侵防御 7.5.4 防病毒技术 7.5.5 记录安全日志 7.6 网络性能管理 7.6.1 网络性能管理概述 7.6.2 利用网络节点上的网管代理监测网络性能 7.6.3 网络服务质量与网络性能保证 7.7 模拟公司网络管理实现 7.8 小结 7.9 习题 7.10 实训 附录A 利用网络模拟器GNS3搭建模拟实训环境 A.1 安装并配置GNS3初始环境 A.1.1 安装GNS3 A.1.2 配置GNS3初始环境 A.2 使用GNS3模拟网络设备进行实验 参考文献

## 章节摘录

插图：IEEE802.1X是一个两层安全访问控制标准框架，提供基于端口的网络接人控制，即连接在局域网接人控制设备（例如接人交换机）端口上的用户设备只有通过身份验证，才能通过所连接的端口访问局域网中资源。
IEEE802.1X标准框架中，完成端口访问控制有3个角色：请求者（IEEE802.1X客户端）、授权者（交换机）和认证者（认证服务器）。
其中交换机是IEEE802.1X客户端与认证服务器间的中介，它与IE：EE802.1X客户端使用封装在以太网帧中的EAP消息交换身份验证有关信息，然后将EAP消息封装在RADIUS报文中，中继给RADIUS认证服务器。
图3-11所示为I：EEE802.1x工作过程示意图。
1.初始化认证IEEE802.1X客户端和交换机任一方都可以初始化认证过程。
IEEE802.1X客户端会在用户运行该客户端时，向交换机发出EAPOL-start消息来初始化认证过程。
交换机收到EAPOL-start消息后，会向客户端发出一个EAPReqllest／Identity消息，来请求身份验证所需的用户名；交换机会在启用了端口认证，端口状态由down向up迁移时，向IEEE802.1X客户端发出一个EAPRequest／Identity消息，来初始化认证过程。

## 编辑推荐

《计算机网络安全与管理》：21世纪高职高专规划教材网络专业系列

# <<计算机网络安全与管理>>

## 版权说明