# <<网络应用技术等级考证教程>>

## 图书基本信息

书名：<<网络应用技术等级考证教程>>

13位ISBN编号：9787308094382

10位ISBN编号：7308094383

出版时间：2011-12

出版时间：浙江大学出版社

作者：闫晓勇，周燕霞　主编

页数：247

# <<网络应用技术等级考证教程>>

## 内容概要

本书是2010年度浙江省重点建设教材，项目编号(ZJG2010282)，适应不同层次、不同专业、不同类型、不同水平的学生学习要求。
本书着重对考试大纲规定的内容有重点地细化和深化，内容涵盖了考试大纲规定的所有知识点，给出了网络应用技术设计案例的解答方法和解题思路。
通过阅读本书，不仅可以掌握考试重点和难点、熟悉考试方法、了解试题形式、体会深度和广度，还可以清晰地把握命题的思路，掌握知识点在试题中的变化，以便在考试中洞察先机，提高通过效率。
全书内容包括：网络基础知识、局域网及应用技术、互联网基础及应用、网络安全技术、网络服务配置、网络操作系统、网络编程、网络设备应用，同步训练、全真试题、模拟试题及答案详解。

# <<网络应用技术等级考证教程>>

## 书籍目录

第1章 网络基础知识
理论知识
1.1 计算机网络的产生与发展
1.2 计算机网络的定义
1.3 计算机网络的分类
1.4 计算机网络体系结构
1.5 计算机网络拓扑结构
1.6 数据通讯基础
1.7 分组交换技术
同步训练
第2章 局域网及应用技术
理论知识
2.1 局域网概述
2.2 IEEE802参考模型及协议
2.3 局域网介质访问控制方法
2.4 高速局域网技术
2.5 局域网组网设备
同步训练
第3章 互联网基础及应用
理论知识
3.1 因特网组成
3.2 因特网功能
3.3 因特网接入
3.4 IP地址
3.5 子网划分
3.6 TCP与15DP协议
3.7 域名与域名服务
3.8 电子商务与电子政务
3.9 高速Internet2技术
同步训练
第4章 网络安全技术
理论知识
4.1 网络管理
4.2 信息安全技术
4.3 加密与认证技术
4.4 Web安全
4.5 计算机病毒
4.6 防火墙技术
4.7 计算机安全等级
同步训练
第5章 网络服务配置
理论知识
5.1 Web服务器配置
5.2 FTP服务器配置
5.3 DNS服务器配置

5.4 Telnet服务器配置
5.5 DHCP服务器配置
同步训练
第6章 网络操作系统
理论知识
6.1 网络操作系统概述
6.2 网络操作系统基本功能及特性
6.3 常见的网络操作系统
6.4 网络操作系统的选择
同步训练
第7章 网络编程
理论知识
7.1 ASP编程基础
7.2 ASP内置对象
7.3 VBScript编程
7.4 数据库访问
同步训练
案例学习
第8章 网络设备应用
理论知识
8.1 交换机
8.2 路由器
8.3 防火墙
同步训练
第9章 网络应用技术全真试题及解析
9.1 全真试题
网络应用技术全真试题1
网络应用技术全真试题2
网络应用技术全真试题3
网络应用技术全真试题4
网络应用技术全真试题5
网络应用技术全真试题6
9.2 答案详解
网络应用技术全真试题1
网络应用技术全真试题2
网络应用技术全真试题3
网络应用技术全真试题4
网络应用技术全真试题5
网络应用技术全真试题6
附录
附录1 模拟试卷
网络应用技术模拟试卷1
网络应用技术模拟试卷2
附录2 参考答案
1.同步训练参考答案
2.模拟试卷参考答案
附录3 考试大纲

参考文献

## 章节摘录

版权页： 插图： 建立包过滤防火墙的过程如下：①对来自专用网络的包，只允许来自内部地址的包通过，因为其他的包包含不正确的包头信息。
②在公共网络，只允许目的地址为80端口的包通过。
③丢弃从公共网络传人的包，而这些包都有用户的网络内的源地址，从而减少了IP欺骗性的攻击。
④丢弃包含源路由信息的包，以减少源路由攻击。
包过滤防火墙优点：①防火墙对每条传人和传出网络的包实行低水平的控制。
②每个IP包的字段都被检查，例如源地址、目的地址、协议、端口等。
③防火墙可以识别和丢弃带欺骗性源IP地址的包。
④包过滤防火墙是两个网络之间访问的唯一来源。
⑤包过滤通常被包含在路由器数据包中，所以不必额外的系统来处理这个特征。
包过滤防火墙缺点：①配置困难。
包过滤防火墙配置复杂，如果忽略了一些必要的规则，将留下漏洞。
②为特定的服务开放的端口存在危险，可能被用于其他传输。
例如Web服务器开放端口是80，软件RealPlayer可能会利用Web服务器的端口。
③可能还有其他方法绕过防火墙进入网络，例如拨号连接。
（2）状态检测防火墙 状态检测防火墙试图跟踪通过防火墙的网络连接和包，这样防火墙就可以使用一组附加的标准，以确定是否允许和拒绝通信。
状态检测防火墙优点：①检查IP包的每个字段的能力，并遵从基于包中信息的过滤规则。
②识别带有欺骗性源IP地址包的能力。
③基于应用程序信息验证一个包的状态的能力，例如基于一个已经建立的FTP连接，允许返回的FTP包通过。
④记录有关通过的每个包的详细信息的能力。
包括应用程序对包的请求、连接的持续时间、内部和外部系统所做的连接请求。
状态检测防火墙缺点：所有的记录、测试和分析工作可能会造成网络连接的某种迟滞，特别是在同时有许多连接激活的时候，或者是有大量的过滤网络通信的规则存在时。
（3）电路级网关 电路级网关工作与会话层，用来监控受信任端与不受信任的主机间的TCP握手信息。
它作为服务器接受外来的请求并转发请求，在TCP握手过程中，检查双方的SYN、ACK和序列数据是否合乎逻辑，来判断请求的会话是否合法。
一旦该网关认为会话是合法的，就会为双方建立连接，自此网关仅复制、传递数据，而不进行过滤。
电路级网关主要优点是提供NAT功能，在使用内部网络地址机制时为网络管理员实现安全提供了很大的灵活性。
电路级网关主要缺点是不能很好地区别好包与坏包、易受IP欺骗这类的攻击及复杂性。
电路级网关要求终端用户通过网关的认证。
（4）应用级网关防火墙 应用级网关可以工作在OSI／RM的任何一层上来检查进去的数据包，通过网关复制传递数据，防止在受信任服务器和客户机与不受信任的主机间直接建立联系。
应用级网关有较好的访问控制，是目前最安全的防火墙技术，但实现困难，而且有的应用级网关缺乏“透明度”。
在实际应用中，用户在受信任的网络上通过访问Internet时，经常会发现存在延迟并且必须进行对此登录才能访问Internet或Intranet。
应用级网关优点在于它易于记录并控制所有进出通信，并对Internet的访问做到内容级的过滤，控制灵活而全面，安全性高。
应用级网关具有登记、日志、统计和报告功能，有很好的审计功能，还可以具有严格的用户认证功能。
应用级网关需要为每种应用写不同的代码，维护比较困难，另外详细的检查也导致速度比较慢。

（5）代理服务器 代理服务器工作在应用层，用来提供应用层服务的控制，在内部网络向外部网络申请服务时起到中间转接作用。
内部网络只接受代理提出的服务请求，拒绝外部网络其他节点的直接请求。
代理服务器是隐蔽运行在防火墙主机上的专门的应用程序或者服务器程序；防火墙主机可以是具有一个内部接口和一个外部接口的双重宿主主机，也可以是一些可以访问Internet并被内部主机访问的堡垒主机。
代理技术能进行安全控制和加速访问，有效地实现防火墙内外计算机系统的隔离，安全性好，以及实施较强的数据流监控、过滤、记录和报告等功能。
缺点是对于每一种应用服务都必须为其设计一个代理软件模块来进行安全控制，而每一种网络应用服务的安全性问题各不相同，分析困难，因此实现也较困难。
在实际的应用过程中，防火墙很少采用单一的技术，通常是多种解决不同问题的技术的结合。
在实际设计中还涉及了用户的需求、用户可接受的风险等级、用户的资金、专长等因素。

## 编辑推荐

## 版权说明