

<<数据与计算机通信>>

图书基本信息

书名：<<数据与计算机通信>>

13位ISBN编号：9787121139253

10位ISBN编号：7121139251

出版时间：2011-9

出版时间：电子工业出版社

作者：（美）斯托林斯 著，王海，张娟，张艳 译

页数：648

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<数据与计算机通信>>

内容概要

《数据与计算机通信(第九版)》是著名计算机专业作家william stallings的经典著作之一，内容涉及基本的数据通信原理、各种类型的计算机网络以及多种网络协议和应用。

覆盖面广，信息量大。

这一版对上一版内容做了许多改进，使新版对通信领域各专题的阐述更清晰、更紧凑。

同时，新版增加了在线动画和示例，补充了双绞线传输标准、宽带因特网接入、第四代移动无线网络、虚拟局域网、移动ip等内容，修订了高速以太网、无线局域网、mpls的相关内容，彻底重写了安全相关章节。

此外，本书还包括术语表、参考文献、缩写词对照表。

每章都附有习题和建议，以便读者进一步阅读。

《数据与计算机通信(第九版)》可供通信或计算机、信息技术专业的本科生和研究生使用，同时也可用做广大通信和计算机领域相关人员的参考用书。

<<数据与计算机通信>>

作者简介

作者：(美国)斯托林斯 (William Stallings) 译者：王海 张娟 张艳 合著者：谢希仁

<<数据与计算机通信>>

书籍目录

第0章 读者及教师快速入门

- 0.1 概要
- 0.2 导读
- 0.3 因特网和万维网上的资源
- 0.4 标准

第一部分 概述

第1章 数据通信、数据网络和因特网

- 1.1 现代企业的数据通信和网络构成
- 1.2 通信模型
- 1.3 数据通信
- 1.4 网络
- 1.5 因特网
- 1.6 网络配置举例

第2章 协议体系结构, tcp/ip和基于因特网的应用程序

- 2.1 协议体系结构的必要性
- 2.2 简单的协议体系结构
- 2.3 tcp/ip协议体系结构
- 2.4 协议体系结构内的标准化
- 2.5 传统的基于因特网的应用程序

- 2.6 多媒体
- 2.7 推荐读物与网站
- 2.8 关键术语、复习题及习题

第二部分 数据通信

第3章 数据传输

- 3.1 概念和术语
 - 3.2 模拟和数字数据传输
 - 3.3 传输损伤
 - 3.4 信道容量
 - 3.5 推荐读物与网站
 - 3.6 关键术语、复习题及习题
- 附录3a 分贝和信号强度

第4章 传输媒体

- 4.1 导向传输媒体
- 4.2 无线传输
- 4.3 无线传播
- 4.4 视距传输
- 4.5 推荐读物与网站
- 4.6 关键术语、复习题及习题

第5章 信号编码技术

- 5.1 数字数据, 数字信号
- 5.2 数字数据, 模拟信号
- 5.3 模拟数据, 数字信号
- 5.4 模拟数据, 模拟信号
- 5.5 推荐读物

<<数据与计算机通信>>

5.6 关键术语、复习题及习题

第6章 数字数据通信技术

6.1 异步和同步传输

6.2 差错类型

6.3 差错检测

6.4 差错纠正

6.5 线路配置

6.6 推荐读物

6.7 关键术语、复习题及习题

第7章 数据链路控制

7.1 流量控制

7.2 差错控制

7.3 高级数据链路控制 (hdlc)

7.4 推荐读物

7.5 关键术语、复习题及习题

附录7a 性能问题

第8章 复用

8.1 频分复用

8.2 同步时分复用

8.3 统计时分复用

8.4 非对称数字用户线路

8.5 xdsl

8.6 推荐读物与网站

8.7 关键术语、复习题及习题

第9章 扩频

9.1 扩频的概念

9.2 跳频扩频

9.3 直接序列扩频

9.4 码分多址

9.5 推荐读物与网站

9.6 关键术语、复习题及习题

第三部分 广域网

第10章 电路交换和分组交换

10.1 交换式通信网

10.2 电路交换网

10.3 电路交换的概念

10.4 软交换体系结构

10.5 分组交换原理

10.6 推荐读物

10.7 关键术语、复习题及习题

第11章 异步传递方式

11.1 atm的角色

11.2 协议体系结构

11.3 atm逻辑连接

11.4 atm信元

11.5 atm信元传输

11.6 atm服务种类

<<数据与计算机通信>>

11.7 推荐读物与网站

11.8 关键术语、复习题及习题

第12章 交换网络中的路由选择

12.1 分组交换网中的路由选择

12.2 举例：arpanet中的路由选择

12.3 最小代价算法

12.4 推荐读物

12.5 关键术语、复习题及习题

第13章 数据网中的拥塞控制

13.1 拥塞的后果

13.2 拥塞控制

13.3 通信量管理

13.4 分组交换网络中的拥塞控制

13.5 atm通信量管理

13.6 atm-gfr通信量管理

13.7 推荐读物

13.8 关键术语、复习题及习题

第14章 蜂窝无线网络

14.1 蜂窝网络的概念

14.2 第一代模拟

14.3 第二代cdma

14.4 第三代系统

14.5 第四代系统

14.6 推荐读物与网站

14.7 关键术语、复习题及习题

第四部分 局域网

第15章 局域网概述

15.1 拓扑结构和传输媒体

15.2 局域网协议体系结构

15.3 网桥

15.4 集线器和交换机

15.5 虚拟局域网

15.6 推荐读物与网站

15.7 关键术语、复习题及习题

第16章 以太网

16.1 传统以太网

16.2 高速以太网

16.3 ieee 802.1q vlan标准

16.4 推荐读物与网站

16.5 关键术语、复习题及习题

附录16a 局域网的数字信号编码

附录16b 扰码

第17章 无线局域网

17.1 概述

17.2 无线局域网技术

17.3 ieee 802.11体系结构和服务

17.4 ieee 802.11媒体接入控制

<<数据与计算机通信>>

17.5 ieee 802.11物理层

17.6 ieee 802.11的安全考虑

17.7 推荐读物与网站

17.8 关键术语、复习题及习题

第五部分 网际协议和运输协议

第18章 网际协议

18.1 网际互连的基本原理

18.2 网际协议工作过程

18.3 网际协议

18.4 ipv6

18.5 虚拟专用网络和ip安全

18.6 推荐读物与网站

18.7 关键术语、复习题及习题

第19章 互联网的操作

19.1 多播

19.2 路由选择协议

19.3 移动ip

19.4 推荐读物与网站

19.8 关键术语、复习题及习题

第20章 互联网的服务质量

20.1 综合服务体系结构

20.2 资源预约协议

20.3 区分服务

20.4 服务级别协约

20.5 ip性能度量

20.6 推荐读物与网站

20.7 关键术语、复习题及习题

第21章 多协议标记交换

21.1 mpls的角色

21.2 背景

21.3 mpls的操作

21.4 标记

21.5 fec, lsp和标记

21.6 标记分发

21.8 虚拟专用网

21.9 推荐读物与网站

21.10 关键术语、复习题及习题

第22章 运输协议

22.1 面向连接的运输协议机制

22.2 tcp

22.3 tcp拥塞控制

22.4 udp

22.5 推荐读物与网站

22.6 关键术语、复习题及习题

第六部分 网络安全

第23章 计算机与网络安全威胁

23.1 计算机安全的概念

<<数据与计算机通信>>

23.2 威胁、攻击和资产

23.3 入侵者

23.4 恶意软件概览

23.5 病毒、蠕虫和机器人

23.6 推荐读物与网站

23.7 关键术语、复习题及习题

第24章 计算机与网络安全技术

24.1 虚拟专网和ipsec

24.2 安全套接字层和运输层安全

24.3 wi-fi保护访问

24.4 入侵检测

24.5 防火墙

24.6 恶意软件防御

24.7 推荐读物与网站

24.8 关键术语、复习题及习题

附录a 傅里叶分析

附录b 数据与计算机通信教学用项目及学生练习

参考文献

缩略语

章节摘录

版权页：插图：鉴别设施，访问控制设施以及防火墙均在反入侵中发挥作用。

另一条防线是入侵检测，也是最近几年来众多研究的焦点。

人们之所以对此感兴趣源于很多考虑，包括如下一些：1.如果能够尽快地发现入侵，就有可能在入侵者造成任何损害或窃取任何数据前被识别并踢出系统。

即便检测不够及时而无法抢得先机，那么入侵发现得越早，损失就越小，恢复也就越快。

2.有效的入侵检测系统（IDS）可以用作威慑，用以防止入侵。

3.入侵检测可以用来收集有关入侵技术的信息，而这些信息则可加强对入侵的防范。

入侵检测基于入侵者的行为与合法用户的行为之间存在可以量化的差异这一假设。

当然，我们不可能指望入侵者的攻击与合法用户正常使用资源之间存在鲜明的差异。

相反，它们之间很有可能是互相重叠的。

图24.6以抽象的形式表明了IDS系统的设计者面临任务的本质。

尽管典型入侵行为与典型授权用户行为是有差异的，但是这些行为之间存在重叠。

因此，如果对入侵行为解释得宽泛些，那么将抓住更多的入侵者，但同时也会导致许多“假阳性”，即许多授权用户被认为是入侵者。

另一方面，如果想限制假阳性，而对入侵行为的解释更严谨，则将导致“假阴性”的增加，即入侵者将不被视为入侵者。

因此，入侵检测在实践中存在折中与巧妙的成分。

在Anderson的研究[ANDE80]中，假设可以在合理的置信度下区分一个冒充者和一个合法用户。

合法用户行为的模式可以通过观察以往历史建立，如果与这个模式差异巨大则可以检测出来。

.Anderson指出检测一个类似入侵者（合法用户行为却类似非授权用户）的任务要困难得多，区分异常行为和正常行为的界限非常模糊。

Anderson总结说这种违例单靠查找异常行为是无法发现的。

然而，类似入侵者的行为可以通过智能地定义多类条件识别出来，这些分类条件可用于发现未授权操作。

最终，检测卧底用户的任务被公认为超出了纯自动化系统的范畴。

这一论断产生于1980年，迄今有效。

本节的剩余部分，将集中讨论基于主机的入侵检测。

<<数据与计算机通信>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>