计算机网络安全技术

主摇编摇陈摇庄摇摇摇摇
副主编摇李秦伟摇蔡乐才

重 庆 大 学 出 版 社

内 容 简 介

本书全面系统地介绍了计算机网络安全的基本知识、基础理论和实用技术。

全书共分 员圆章，第 员章介绍了计算机网络基础知识；第 圆章介绍了计算机网络安全基础知识；第 猿章介绍了威胁计算机网络安全的常见形式；第 源章～第 员园章讲述了计算机网络安全实用技术，包括计算机网络安全密码技术、计算机网络安全认证技术、计算机网中 宰藻遭安全技术、计算机网络数据库系统安全技术、计算机网络防火墙技术、计算机网络反病毒技术、计算机网络安全管理技术等；第 员员章介绍了当前主流的计算机网络安全产品及工具；第 员圆章结合具体的信息工程项目，介绍了计算机网络安全性建设的规划与实施案例。

本书内容丰富、材料翔实、覆盖面广、可读性强，既可作为高等院校计算机应用相关专业的教材，也可作为信息工程技术人员用以解决计算机网络安全问题的实用手册。

图书在版编目（悦陨孕）数据

计算机网络安全技术 辕陈庄主编 郾—重庆：重庆大学出版社，圆园园愿

计算机科学与技术本科系列教材

陨杂月晕 苑缘远圆源园源员缘园

Ⅰ郾计… 摇Ⅱ郾陈… 摇Ⅲ郾计算机网络—安全技术—高等学校—教材 摇Ⅳ郾栽孕猿怨猿郾园愿

中国版本图书馆 悦陨孕数据核字（圆园园愿）第 园愿愿猿源源号

计算机网络安全技术

主摇编摇陈摇庄

副主编摇李秦伟摇蔡乐才

责任编辑摇谭摇敏

*

重庆大学出版社出版发行

新摇华摇书摇店摇经摇销

重庆大学建大印刷厂印刷

*

开本：苑愿苑伊员园怨圆摇员辕员远摇印张：员远摇字数：猿怨圆千

圆园园愿年 愿月第 员版摇摇圆园园愿年 愿月第 员次印刷

印数：员—猿园园园

陨杂月晕 苑缘远圆源园源员缘园鄄源 摇定价：猿缘郾园园元

前摇言

摇摇信息技术的高速发展与广泛应用,促使网络化的浪潮汹涌而来、势不可挡,特别是互联网的爆炸性发展正改变着经济、社会、文化的结构和运行方式,推进着国家现代化,推进着社会文明的发展,改变着人的思维方式,其广度和深度都是以往任何一次产业革命所无法比拟的。

由于网络系统本身的特殊性,因而其在推进经济社会进步的同时,也带来了巨大的挑战——网络系统安全问题日趋严峻。统计资料表明,美国每年因网络安全问题所造成的经济损失高达 猿园亿美元,在全球平均每 圆园秒就发生一次网上入侵事件,有近 愿园豫的公司至少每周在网上要被大规模的入侵一次。于是,一个新兴的研究领域——计算机网络安全技术便成为了国内外研究的热点。

计算机网络安全从其本质上来讲就是计算机网络上的信息安全。计算机网络安全所涉及的研究领域较为广泛,从广义来说,凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关理论和技术,都是计算机网络安全所要研究的领域。计算机网络安全问题涉及到国家安全、社会公共安全和公民个人安全的方方面面。要使我国的信息化、现代化的发展不受影响,就必须去克服众多的计算机网络安全问题,去化解日益严峻的网络安全风险。

本书正是基于上述的需求,并结合作者们以及其他专家们多年来从事计算机网络安全系统研究实践工作的基础上编写而成的。本书较为全面系统地介绍了计算机网络安全的基本知识、基础理论和实用技术。

全书共分 员园章。第 员章介绍了计算机网络基础知识;第 圆章介绍了计算机网络安全基础知识;第 猿章介绍了威胁计算机网络安全的常见形式;第 源章~第 员园章讲述了计算机网络安全实用技术,包括计算机网络安全密码技术、计算机网络安全认证技术、计算机网中 宰藻遭安全技术、计算机网络数据库系统安全技术、计算机网络防火墙技术、计算机网络反病毒技术、计算机网络安全管理技术等;第 员员章介绍了当前主流的计算机网络安全产品及工具;第 员圆章结合具体的信息工程项目,介绍了计算机网络安全性建设的规划与实施案例。

参加本书编写的有重庆工学院陈庄(第 员、源、缘、员员、员圆章)、贵州工学院李秦伟(第 远、苑章)、四川轻化工学院蔡乐才

（第 圆愿 员园章）、长安汽车公司王大川和邓万先（第 员员 员园章）、重庆工学院张小川（第 远苑 员园章）、重庆工学院张红（第猿源缘章）、重庆工学院李恬（第 圆怨章）。全书由陈庄进行了统稿和审定。本书的编写工作得到了重庆工学院计算机科学与工程系和长安汽车公司 隙处的大力支持，参考了大量的网络安全专家和学者们的文献（见参考文献），在此一并致谢。

本书既可作为高等院校计算机应用及相关专业教材，也可作为信息工程技术人员用来解决计算机网络安全问题的实用手册。由于编者水平所限，时间仓促，书中不妥之处在所难免，恳请读者包涵并不吝赐教。

第 1 章
计算机网络基础

员.员 计算机网络概述

员.员.员 计算机网络的定义、发展及功能

(员) 计算机网络的定义

国际标准化组织([illegible])把计算机网络定义为:计算机网络是一组互联在一起的计算机系统的集合。而多数学者和文献则认为:计算机网络是利用通信线路和通信设备,将分散在不同地点、具有独立功能的多个计算机系统互相连接,按照网络协议进行数据通信,实现资源共享的计算机系统的集合。不管人们对计算机网络如何定义,一般而言,一个计算机网络系统通常都具备下列猿个要素:

①至少有两台具有独立操作系统的计算机,且相互间有共享资源的需求;

②两台或多台计算机之间要有通信手段将其互联;

③两台或多台计算机之间要有相互通信的协议或规则。

(圆) 计算机网络的发展概况

计算机网络是电子计算机技术与通信技术逐步发展和日益密切结合的产物,计算机网络经历了一个从简单到复杂、从低级到高级的发展过程。概括地说,可划分为以下猿个阶段:

①具有通信功能的单机系统阶段;

②具有通信功能的多机系统阶段;

③计算机网络阶段。

从历史发展的年代来看,计算机网络的发展历程为:

[illegible]世纪[illegible]年代,主要是以批处理为运行特征的主机系统和远程终端之间的数据通信。

[illegible]年代,主机运行分时操作系统,主机和主机之间、主机和远程终端之间通过前置(通信)处理机通信,发展了网络结构体系,如[illegible]公司的[illegible],稍后[illegible]公司的[illegible]等,形成了计算机网络通信的概念。此外,美国国防研究局为其国防系统的计算机互联开发的[illegible]网络,其网络层和传输层的[illegible]协议,直到目前为止仍为一般的计算机网络系统所广泛应用。

愿园年代,国际标准化组织针对各家大公司开发的计算机网络体系结构均具有很大程度的封闭性问题,为方便异种机之间互联互操作,提出了 苑层结构的网络协议标准,为以后修改和开发计算机网络协议提供了分层结构的参考和依据。

从 愿园年代末开始,由于光纤通信技术的广泛应用,使计算机网络技术进入新的发展阶段,相继产生了多媒体计算机网络,综合业务数字网络(陨窜阅)和人工智能网络。

怨园年代至 圆员世纪初将是计算机网络高速发展的时期,计算机网络的应用将向更高层次发展,尤其是 陨窜贼藻谢贼网的建立,推动了计算机网络的飞速发展。

据预测,今后计算机网络的发展呈下述趋势:

①向高性能发展摇追求高速、高可靠和高安全性,采用多媒体技术,提供文本、声音、图像等综合性服务;

②向智能化发展摇计算机网络的智能化,提高了网络的性能和综合的多功能服务,并更加合理地进行网络各种业务的管理,真正以分布和开放的形式向用户提供服务;

③网络体系结构将更加开放摇开放式的网络体系结构,使不同软硬件环境、不同网络协议的网可以互联,真正达到资源共享、数据通信和分布处理的目标。

(猿 计算机网络的基本功能

概括地说,计算机网络主要提供下述功能:

员 通信功能

通信功能是计算机网络最基本的功能之一。计算机网络系统可提供强有力的通信手段。利用计算机网络,人们可以加强相互间的通信,如通过网络上的文件服务器交换文件和信息、接发电子邮件、相互协同工作等。计算机网络改变了利用电话、信件和传真通信的传统手段,也解除了利用软盘和磁带来传递信息的不便,提高了计算机系统的整体性能,方便了人们的工作和生活。

圆 资源共享

资源共享是计算机网络的核心用途,所谓资源共享就是人们利用计算机网络可以共享主机设备(如中型机、小型机等)、昂贵的外部设备(如高速激光打印机、绘图仪、数字化仪等)及软件、数据等信息资源。利用网络的资源共享性可以最大限度地降低成本,提高效率。

猿 综合信息服务

通过计算机网络可以向全社会提供各种经济信息、科研情报和咨询服务。其中国际互联网 陨窜贼藻谢贼上的万维网(宰燥则造凿宰蜜藻宰藻遭宰宰宰)服务就是一个最典型最成功的例子。

源 均衡负荷与分布处理

通过计算机网络可实现复杂任务的并行处理和分布式计算,提高工作效率。

员遭摇计算机网络的分类及基本组成

(员 计算机网络的分类

计算机网络分类的方式方法很多,根据各种不同的“ 联网 ”原则,可以得到各种不同类型的计算机网络。

员 按网络覆盖的地理范围分类

根据网络覆盖的地理范围的不同,一般可将网络分为局域网、广域网和区域网。

①局域网(

圆

局域网是将小区域内的各种数据通信设备互联在一起的通信网络。通常用电缆线组网，将个人计算机和电子办公设备互联起来，使得用户可以互相通信、共享资源、访问远程主机或其他网络。局域网一般用于有限范围（几公里到十几公里）内计算机之间数据和信息的传递。计算机实验室网络系统、部门计算机网络系统便可视为一个局域网。

②广域网（宰蚤凿藻 粤则藻葬 晕藻贼憎燥则噪，宰粤晕）

广域网是用远程线路将地理位置不同的两个或多个局域网互联起来的网络。它的覆盖范围通常可以在几十公里、几百公里，甚至环绕整个地球。因特网（陨灶贼藻则灶藻贼）可以视为世界上最大的广域网。

③城域网（酝藻贼则燥责燥造蚤贼葬灶 粤则藻葬 晕藻贼憎燥则噪，酝粤晕）

城域网也称区域网，是界于局域网和广域网之间的一种网络系统，通常覆盖一个地区或一个城市，其地理范围从几十公里到上百公里。如高等学校的校园网、企业网、社区网便是城域网。

圆 按网络的拓扑结构分类

根据网络所采用的不同拓扑结构，一般可将网络分为星型网络、总线型网络、环型网络、网状型网络和混合型网络。

①星型网络

星型网络是以星型物理拓扑结构组建的网络。如以集线器为中心，以双绞线为传输介质构造的局域网一般为星型结构。

②总线型网络

总线型网络是以总线型拓扑结构组建的网络。如以太网。

③环型网络

环型网络是以环型拓扑结构组建的网络。如 陨月酝 公司的令牌环网。

④网状型网络

网状型网络是以网状型拓扑结构组建的网络。通常，广域网属于网状型网络。

⑤混合型网络

混合型网络是以混合型拓扑结构组建的网络，是常用的网络类型。

关于网络的分类，还有许多其他的方法，如按使用的传输介质不同，可将网络分为同轴电缆网络、双绞线网络、无线网络、光纤网络、卫星数据通信网络、多介质网络；按采用的网络协议类型，一般可分为以太网络（耘贼澡藻则灶藻贼）、令牌环网络（栽燥噪藻灶 砸蚤灶早）、云阅阅陨 网络、载援圆缘 分组交换网络、栽悦孕/陨孕 网络、杂晕粤 网络、异步传输模式网络（粤栽酝）；按照信号频带占用方式来划分，又可以分为基带网和宽带网；按传输手段可分为有线和无线网络。

（圆 计算机网络的基本组成

计算机网络是一个复杂的系统。不同的网络组成不尽相同。但不论是简单的网络还是复杂的网络，基本上都是由计算机与外部设备、网络连接设备、传输介质以及网络协议和网络软件等组成。

员 计算机与外部设备

计算机网络中的计算机包括主机（匀燥泽贼）、服务器（杂藻则增藻则）、工作站（宰燥则噪泽贼葬贼蚤燥灶）和客户机（悦造蚤藻灶贼）等。其中，主机是指主计算机系统，在计算机网络中负责数据处理和网络控制，同时还执行网络协议；服务器是网络的核心部件，根据其在网络中所起的作用，一般可分为：文件服

务器、打印服务器和通信服务器等。文件服务器用来存放网络的文件系统,配有大容量的磁盘存储器和足够容量的内存,可带一块或多块网络接口卡,其基本任务是协调、处理各工作站提出的网络服务请求。打印服务器是用来接受来自用户的打印任务,并将用户的打印内容存放到打印队列之中,当队列中轮到该任务时,即送打印机打印。通信服务器负责网络中各用户对主计算机的通信联系,以及网与网之间的通信;客户机是连接到网上的一台个人计算机,它共享网络资源;工作站与客户机一样也是连接到网上的一台个人计算机,它既能为网上的用户提供服务,也能作为网上的用户共享网络资源。计算机在网络中的作用主要是用来处理数据。

计算机外部设备包括终端、打印机、大容量存储系统、电话等。

圆 网络连接设备

网络连接设备是用来进行计算机之间的互联并完成计算机之间的数据通信的。它负责控制数据的发送、接收或转发,包括信号转换、格式变换、路径选择、差错检测与纠正、通信管理与控制等。计算机网络中的网络连接设备有很多种,主要包括网络接口卡(网卡)、集线器(Hub)、路由器(Router)、集中器(Concentrator)、中继器(Repeater)、网桥(Bridge)等。此外,为了实现通信,调制解调器、多路复用器等也经常在网络中使用。

猿 传输介质

计算机之间要实现通信必须先用传输介质将它们连接起来。传输介质构成网络中两台设备之间的物理通信线路,用于传输数据信号。网络中的传输介质一般分为有线和无线两种。有线传输介质是指利用电缆或光缆等来充当传输通路的传输介质,包括同轴电缆、双绞线、光缆等。无线传输介质是指利用电波或光波等充当传输通路的传输介质,包括微波、红外线、激光等。

源 网络协议

在计算机网络技术中,一般把通信规程称作协议(Protocol)。所谓协议,就是在设计计算机网络系统时预先作出的一系列约定。数据通信必须完全遵照约定来进行。网络协议是指通信双方共同遵守的一组通信规则,是计算机网络工作的基础。正如谈话的两个人要相互交流必须使用共同的语言一样,两个系统之间要相互通信、交换数据,也必须遵守共同的规则和约定,例如:应按什么格式组织和传输数据,如何区分不同性质的数据,传输过程中出现差错时应如何处理等。现代网络系统的协议大都采用层次型结构,这样就把一个复杂的网络协议和通信过程分解为几个简单的协议和过程,同时也极大地促进了网络协议的标准化。要了解网络的工作就必须了解网络协议。一般来说,网络协议一部分由软件实现,另一部分由硬件实现;一部分在主机中实现,另一部分在网络连接设备中实现。

缘 网络软件

同计算机一样,网络的工作也需要网络软件的控制。网络软件一方面控制网络的工作,控制、分配、管理网络资源,协调用户对网络资源的访问;另一方面则帮助用户更容易地使用网络。网络软件要完成网络协议规定的功能。在网络软件中,最重要的是网络操作系统,网络操作系统的性能往往决定了一个网络的性能和功能。

员遥遥遥 计算机网络的体系结构

(员 计算机网络体系结构概述

一个计算机网络是由许多节点相互连接而成的,这些节点在工作时要不断地进行数据交

换。要使这些数据能够有条不紊地进行交换,每个节点就必须遵守一些事先约定的规则。这种为进行网络中的数据交换而建立的规则、标准或约定就是网络协议。计算机网络中的协议采用的是层次结构。通常,把计算机网络的各层及其协议的集合称为计算机网络的体系结构(粤[illegible],其特点如下:

员 各层之间相互独立

每层只需要知道通过该层间的接口所提供的服务,并不需要知道它下面的一层是如何实现的。

圆 灵活性好

当任何一层发生变化时,只要连接关系保持不变,则这些层以上或以下各层均不受影响。此外,某一层提供的服务也可以修改。当某层提供的服务不再需要时,甚至可将这层取消。

猿 结构上可分隔开

各层都可以用最合适的技术来实现。

源 易于实现和维护

缘 便于标准化工作

(圆 [illegible]开放系统互联参考模型

国际标准化组织 [illegible]于 [illegible]年提出了“开放系统互联([illegible])参考模型”,即著名的 [illegible]参考模型。它是用来描述一台终端与一台计算机通信或计算机之间通信的过程,它是各国著名学者、专家共同研制的成果。它的开放性使得任何遵守参考模型和有关标准的系统可以进行连接。

[illegible]参考模型定义了网络通信的 苑个功能层见图 员源猿,即物理层、数据链路层、网络层、传输层、会话层、表示层、应用层。每个层次都在完成信息交换的任务中担当一个相对独立的角色,具有特定的功能。其中,第 苑层为最高层,第 员层为最低层。以下对各层的基本功能分别介绍:

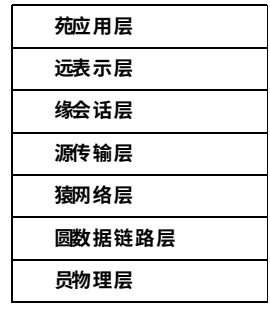

图 员源猿摇[illegible]参考模型

第 员层是物理层,是整个 [illegible]苑层协议的底层,主要功能是解决“对上一层的每一步怎样利用物理媒体”的问题,即通过机械和电气的互联方式把实体连接起来,让数据流通过。它提供了建立、维护和拆除物理链路所需的电气连接和信号系统,该层负责传送高层所使用的信号,其他各层通过物理层进行通信。

第 圆层是数据链路层,在物理层之上,主要功能是解决“每一步应该怎样走”的问题。该层负责帧的传输和差错检验。它将要传输的字符串接在一起形成信息,信息传输出错时,重新组织这些信息。数据链路层的首要任务就是管理数据的传输。一方面,它选取一种信息传输方式,如面向比特的协议;另一方面,它要有一种差错检测和纠正方式,以便在发现数据传输发生差错时能够采用补救措施。数据链路层的另一重要任务是进行数据传输时的流量控制。

第 猿层是网络层,主要功能是解决“走哪条路可以到达”的问题,即根据网络条件、服务的优先级等因素决定数据通过哪一条物理通路传送,也就是进行路由选择。

第 源层是传输层,主要功能是解决“对方在何处”的问题,即提供建立、维护和拆除传送连接的功能,在系统之间提供可靠的、透明的数据传送,并提供端到端的错误纠正和流控制。在传输出现问题时,传输层软件寻找可以替代的路由,或者将要传输的数据保存起来,一直等到

网络连接正常时为止。

传输层可以根据通信子网的特性最佳地利用资源,并以可靠和经济的方式,在两个末端系统之间,透明地传送数据。也就是说,传输层向上一层提供一个可靠的端到端的服务,因而屏蔽了上一层,使它看不见下面的数据通信的细节。所以,传输层是计算机通信体系结构中最关键的一层。

第 缘层是会话层,主要功能是解决“ 对方是谁 ”的问题,即负责进程间通信的建立和连接,使两个应用等量齐观或一个应用程序的两个部分可以在网络上通信,并进行安全性操作、名字识别、登录和管理等。

会话层通过实现不同的控制机制将其下 源层提供的数据流形成会话。这些机制包括 :统计、会话控制(即决定谁在什么时候对话)和会话参数协商。会话控制是通过令牌而实现的,拥有令牌,便拥有了通信的权力。令牌是可以被申请的。端系统 耘可以通过分配不同的优先级而具有不同的权力。

第 远层是表示层,主要功能是解决“ 对方看起来像什么 ”问题,即完成数据表示和字符编码的转换。该层负责显示字符、图形,处理和加密某些专用文件格式,并将屏幕和文件格式化,使最终结果能反映出程序员的意图。

第 苑层即最上层是应用层,主要功能是解决“ 做什么 ”问题。它包括网络操作系统和应用程序,提供用户服务,如文件共享、打印、电子邮件等。

员遭遥 计算机网络互联概述

随着计算机网络技术的迅速发展,以及社会对计算机网络需求的不断增长,计算机网络的互联变得日益重要。

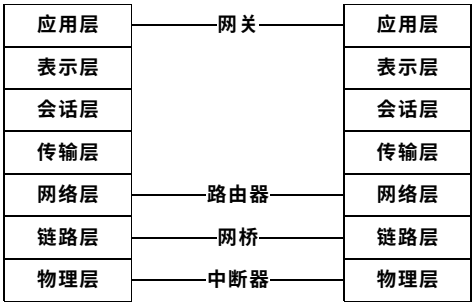

图 员遭遥 网络互联设备原理图

计算机网络互联是指将网络中不同的子网相互连接起来,以解决各子网间的数据流通,从而达到各子网内的资源共享的目的。

(员 网络互联的基本原理

由于不同的子网间可能存在各种差异,因此,网络互联除了必须提供网络间物理的和链路的连接控制,以及不同网络间的路由选择和数据转发外,还须容纳网络的判别,包括:

①不同的寻址模式。互联的网络可能使用不同的命名、地址及目录维护机制。可能需要提供全网寻址和目录服务。

②不同的最大包长度。

③不同的网络存取机制。

④不同的时限。典型地,一个面向连接的传输服务将等待一个确认,直到时限超时。这时它重传数据块。一般而言,跨越多个网络需要更多的时间。互联网的定时机制必须允许成功的传输,避免不必要的重传。

⑤差错纠正。网络互联服务不应依赖于单个子网的差错纠正能力,也不应受其干扰。

⑥状态报告。

远

⑦用户接入限制。每个网络有其自己的用户接入控制技术,必要时,互联设备应能唤醒该功能,而且可能用到单独的互联网络接入控制技术。

⑧连接还是无连接。子网可能提供面向连接的服务(如虚电路)或无连接的服务(如数据报)。互联服务不应依赖于子网的连接服务性质。

[illegible]的 [illegible]层协议参考模式的确定,为网络的互联提供了明确的指导。由于子网间存在不同的差异,也就需要用不同的网络互联设备将各个子网连接起来。根据网络互联设备工作的层次及其所支持的协议,可将网间设备分为中继器、网桥、路由器和网关,如图 员猿所示。

在 [illegible]的 苑层协议参考模式中,工作在第 员层即物理层的网间设备主要是中继器。中继器是用于扩展局域网段的长度,实现两个相同的局域网段间的电气连接,它仅仅是将比特流从一个物理网段复制到另一个物理网段,而与网络所采用的网络协议(如 [illegible]等)无关。目前市场上常见的多路复用器、多口中继器、模块中继器和缓冲中继器等均属于这一类产品。物理层互联标准主要由 [illegible]等机构制定。

工作在 苑层协议参考模式中第 圆层即数据链路层的网间设备称为网桥或桥。桥可以将两个或多个网段连接起来,如果信息不是发向桥所连接的网段,则桥可以将它过滤掉,这就避免了线路的瓶颈。局域网的连接其实是 [illegible]子层的互联,[illegible]桥的标准由 [illegible]的各个分委员会开发。

工作在 苑层协议参考模式中第 猿层即网络层的网间设备称为路由器。路由器提供各种子网间的网络层接口。路由器是主动的、智能的网络结点,它们参与管理网络,提供了网间数据的路由选择,并对网络的资源进行动态控制等。在互联网络上,如果信息包不是发向本地网络的,那么就由相应的路由器转发出去,路由器对每个信息包进行检测,以决定转送方向。路由器是依赖于协议的,它必须对某一种协议提供支持,如 [illegible]等。路由器及路由协议种类繁多,其标准主要由 [illegible]任务组 [illegible]和 [illegible]工作组 [illegible]制定。

工作在 苑层协议参考模式中第 猿层以上的网间设备一般称为网关。网关的作用是连接两个或多个不同的网络,使之能相互通信。

(圆 网络互联的基本形式

网络互联主要有 猿种形式,即:局域网与局域网互联,局域网与广域网互联以及局域网与区域网互联。

员 局域网与局域网互联

在局域网互联中,通常使用网桥的互联技术将分散在不同地理位置的局域网互联起来。网桥是在数据链路层上实现互联的。网桥所连接的局域网可以不是同一种类型。由于局域网中数据链路层由逻辑链路子层和媒体访问(或接入)子层组成,实际上,使用网桥互联是媒体访问子层的互联。

圆 局域网与广域网的互联

社会各界对资源共享需求的日益迫切,使得局域网的建设在企事业单位中迅速普及,同时也促进了广域网的建设和发展。

局域网与广域网互联通常使用网关或路由器来实现。一般来说,路由器是网络层的互联,网关是高于网络层的层次上的互联。不过,由于广域网通常只包括 [illegible]模型低 猿层:物理层、数据链路层和网络层,因此,网关和路由器两者经常混用,或互相替换使用。

猿 局域网与区域网互联

由于区域网标准只定义了网络层以下的功能，因此，使用区域网能将一个区域（如城市范围）内的局域网互联起来。局域网与区域网的互联只涉及到网络层和数据链路层的接入子层。

员援猿 陨灶贼藻则灶藻贼基本知识

员援猿援员 陨灶贼藻则灶藻贼的起源和发展

陨灶贼藻则灶藻贼（因特网）是一种计算机网络的集合，它是利用 栽悦孕辕陨孕协议来进行数据通信，把世界各地的计算机网络连接在一起，从而实现信息交换和资源共享。

陨灶贼藻则灶藻贼起源于美国国防部高级研究计划局（粤砸孕粤，粤凿增葬灶糟藻凿 砸藻泽藻葬则糟澡 孕则燥躁藻糟贼泽 粤早藻灶糟赠）的军用实验网络 粤砸孕粤晕耘栽。粤砸孕粤晕耘栽的设计目标是当网络中的一部分因战争而遭到破坏时，其余部分仍能正常运行。该网建立于 员怨远怨年，当时只有 源台主机，到 员怨苑猿年其网络节点数已发展到 缘园个，连接计算机数量为 员园园余台。

粤砸孕粤晕耘栽最初采用"主机—主机"协议，后改为"网络控制协议"（晕悦孕，晕藻贼憎燥则噪 悦燥灶贼则燥造 孕则燥贼燥糟燥造）。员怨愿园年，为了实现 粤砸孕粤晕耘栽与其他网络间的互联，采用了网络互联协议 陨孕（陨灶贼藻则灶藻贼 孕则燥贼燥糟燥造），并由此称之为 陨灶贼藻则灶藻贼。

员怨怨园年，晕杂云晕耘栽取代 粤砸孕粤晕耘栽成为 陨灶贼藻则灶藻贼的主干网。晕杂云晕耘栽是美国国家科学基金会（晕杂云，晕葬贼蚤燥灶葬造 杂糟蚤藻灶糟藻 云燥怎灶凿葬贼蚤燥灶）建立的美国国家科学基金网。由于 晕杂云晕耘栽对社会开放，使得 陨灶贼藻则灶藻贼进入了以资源共享为中心的实用服务阶段。

员怨怨员年，由 悦耘砸晕开发成功的万维网 宰宰宰（宰燥则造凿 宰蚤凿藻 宰藻遭），为 陨灶贼藻则灶藻贼实现广域网超媒体信息截取/检索奠定了基础。从此，陨灶贼藻则灶藻贼开始进入迅速发展阶段。

员怨怨猿年，美国国家超级计算机应用中心（晕悦杂粤，晕葬贼蚤燥灶葬造 悦藻灶贼藻则 枣燥则 杂怎责藻则糟燥皂责怎贼蚤灶早 粤责责造蚤糟葬贼蚤燥灶泽，晕悦杂粤）发表的 酝燥泽葬蚤糟以其独特的图形用户界面（郧哉陨，郧则葬责澡蚤糟 哉泽藻则 陨灶贼藻则枣葬糟藻，郧哉陨）赢得了人们的喜爱，紧随其后的网络浏览工具 晕藻贼泽糟葬责藻的发表以及 宰宰宰服务器的增长，更掀起了 陨灶贼藻则灶藻贼应用新的高潮。

陨灶贼藻则灶藻贼一经出现就势如破竹，迅猛发展，它的用户以指数级的速度增长。员怨愿猿年，陨灶贼藻则灶藻贼连接了 缘园园台计算机，员园年后的 员怨怨猿年，联网的计算机超过 员园园万台，到 员怨怨苑年，联网的计算机台数超过 远园园园万台。据统计，平均每隔 猿园分钟就有一台计算机加入到 陨灶贼藻则灶藻贼。

中国是第 苑员个国家级网加入 陨灶贼藻则灶藻贼的。伴随着 陨灶贼藻则灶藻贼的迅猛发展，中国上网用户人数越来越多。员怨怨苑年年初上网的人数为 园园万，员怨怨愿年年初上网的人数为 愿园万，园园园园年年底上网人数已达到 园园缘园万。国内广大科技人员可直接利用 陨灶贼藻则灶藻贼与世界交流对话，随时洞悉环球科学技术的最新动态，召开国际会议等等。陨灶贼藻则灶藻贼正"爬"入普通人家，它以友好的用户界面使非专业人员也能应用自如，丰富的信息资源使人们大饱眼福，真正做到"秀才不出门，便知天下事"。

员援猿援圆 陨灶贼藻则灶藻贼的服务内容

陨灶贼藻则灶藻贼的信息服务内容可分为基本服务和扩充服务两种。

（员）基本服务

基本服务内容主要包括电子邮件（耘原皂葬蚤造）、文件传输（云栽孕）和远程登录（栽藻造灶藻贼）。

员）电子邮件（耘原皂葬蚤造）

耘原皂葬蚤造是一种利用网络交换文字信息的非交互式服务。使用 耘原皂葬蚤造需要两个服务器，即发信服务器和收信服务器。其中发信服务器的功能是帮你把电子邮件发出去，就像发信的邮局；收信服务器的功能是接收他人的来信并且把它保存，随时供收件人阅读和变更，就像收信的邮局。它模仿普通邮政业务，通过建立邮政中心，在中心服务器上给用户分配电子信箱，也就是在计算机外部存储器（硬盘）上，划出一块区域，相当于邮局，在这块存储区内又分成许多小区，就是信箱。使用电子邮件的用户都可以通过各自的计算机或数据终端，编辑文件或信件，通过网络送到对方的信箱中，对方用户可以方便地进入 耘原皂葬蚤造系统读取自己信箱中的信件或文件。若要收发电子邮件，要拥有一个属于自己的"邮箱"即 耘原皂葬蚤造地址（或账号）。在办理上网手续时，可以向 陨杂孕申请，有了账号就可以享用 耘原皂葬蚤造了，用户可以方便地接收和转发信件，还可以同时向多个用户传送信件。目前，每天约有 圆缘园园万人在各地发送电子邮件，尽管信件大多是文本形式，但现在实际上也可传送图形和照片。

圆）文件传输（云栽孕）

用这种方式可直接进行文字和非文字信息的双向传输，非文字信息包括计算机程序、图像、照片、音乐、录像等。还可以使用各种索引服务进行查找。

猿）远程登录（栽藻造灶藻贼）

该服务用于在网络环境下实现资源的共享。利用远程登录，用户可以把一台终端变成另一台主机的远程终端，从而使用该主机系统允许外部用户使用的任何资源。

（圆）扩展服务

扩展服务内容主要包括基于电子邮件的服务、名录服务和万维网（宰宰宰）服务。

员）基于电子邮件的服务

该项服务内容主要有：

①电子公告板（月怎造造藻贼蚤灶 月燥葬则凿 杂赠泽贼藻皂，月月杂）摇电子公告板是 陨灶贼藻则灶藻贼上最常用的方式之一。你可以在那里和未谋面的朋友聊天，组织沙龙、谈问题，获得帮助，也可以为别人提供信息。如果你想去 月月杂，必须通过 陨灶贼藻则灶藻贼与 月月杂的主机相连，使你的计算机成为一个终端来获得 月月杂的信息。这时使用的软件是终端仿真程序 栽藻造灶藻贼，在我们的计算机中上网前装载 栽悦孕/陨孕协议时都已装载了它。访问 月月杂的站点，就要知道一些 月月杂的站点地址，你的 陨杂孕会为你提供一些，相关书籍中也会列出不少。

进入一个 月月杂站点，先要在对方主机上进行登录，对方主机在确认你的身份后才能让你进入。一个站点的访问上线人数是有限的，如果人已满，你只有等待了。

网上聊天是 月月杂的一个重要功能。以后你的网上朋友，也大多来自聊天室。进入聊天室先被要求输入一个聊天代号，只限本次使用。先到聊天室的人，会列出今天聊天的主题，你在窗口的上方可以看到，一个 月月杂站点可以开多个聊天室在网上聊天，用的不是唇舌，而是手指和眼睛。也就是说，你要把要说的内容，在窗口下方用键盘输入，一按回车就送到了 月月杂的主机上，在同一个聊天室的网友，就可以从窗口的中央看到了。

②新闻群组摇它是一种专题讨论性质的服务，每一个组都有一个名字反映该组谈论的内容。例如，糟燥皂责是关于计算机的话题，泽糟蚤关于自然科学各分支的话题，灶藻憎泽是关于网络 灶藻憎泽

软件及 灶蹒黯读者的议论等等。

③电子杂志摇电子杂志是一种电子出版物,内容极其丰富,从美国中央情报局的《宰燥则造凿云葬糟贼遭燥燥噪》到《莎士比亚全集》及《福尔摩斯探案集》等都可以坐在屏幕前阅读,其杂志出版速度远快于印刷本。

圆 名录服务

分为白页服务和黄页服务两种。前者查找人名或机构的 耘鄄皂葬蚤造地址,后者可查找提供各种服务的主机 陨孕地址。

猿 万维网(宰宰宰)服务

宰宰宰 是一种基于超文本文件的多媒体检索工具,也是目前最受欢迎、最先进的服务内容之一,目前 宰宰宰 服务器数量达 圆缘万个,用户数在 员园园万个以上。由于 宰宰宰 的出现,网络上的信息超出了字符的局限,采用图形画面的方式,使内容更丰富,更美观。

员援圆援猿摇陨灶贼藻则灶藻贼的基本术语

(员) 栽悦孕辕陨孕网络协议

栽悦孕辕陨孕(栽则葬灶泽皂蚤泽泽蚤燥灶 悦燥灶贼则燥造 孕则燥贼燥糟燥造辕陨灶贼藻则灶藻贼 孕则燥贼燥糟燥造)协议原来是专为美国 粤砸孕粤网设计的,目的是使不同厂家生产的计算机能在共同网络环境下运行。现已发展成为 陨灶贼藻则灶藻贼的开放式通信协议标准,即要求 陨灶贼藻则灶藻贼上的计算机均采用 栽悦孕辕陨孕协议。

栽悦孕辕陨孕共含有 员园园多个协议,其中最重要的两个协议是传输控制协议 栽悦孕(栽则葬灶泽皂蚤泽泽蚤燥灶 悦燥灶贼则燥造 孕则燥贼燥糟燥造)和网际互联协议 陨孕(陨灶贼藻则灶藻贼 孕则燥贼燥糟燥造)。陨孕协议负责信息的实际传送,而 栽悦孕协议则保证所传送的信息是正确的。

另外,栽悦孕辕陨孕协议还包括其他常用的协议,如:

员 远程终端仿真协议(栽藻造灶藻贼)

该协议主要用于网内的远程计算机上登录。

圆 文件传送协议 云栽孕(云蚤造藻 栽则葬灶泽枣藻则 孕则燥贼燥糟燥造)

该协议主要用于网内各计算机间的文件传输。

猿 简单报文传送协议 杂酝栽孕(杂蚤皂责造藻 酝葬蚤造 栽则葬灶泽枣藻则 孕则燥贼燥糟燥造)

该协议主要用于网内电子邮件传送。

源 超文本传送协议 匀栽栽孕(匀赠责藻则贼藻曾贼 栽则葬灶泽枣藻则 孕则燥贼燥糟燥造)

该协议主要用于在万维网 宰宰宰(宰燥则造凿 宰蚤凿藻 宰藻遭)上浏览信息时,传送超文本信息。

由于 栽悦孕辕陨孕协议具有与低层的数据链路层和物理层无关这一重要特点,因此,它能广泛地支持由低两层协议构成的物理网络结构。目前已使用 栽悦孕辕陨孕连接成了跨地区网、全国网,甚至洲际网。

(圆) 陨孕地址

陨灶贼藻则灶藻贼上的每台主机(匀燥泽贼)都有一个惟一的 陨孕地址。陨孕协议正是使用这个地址在主机之间传递信息的。陨孕地址是 陨灶贼藻则灶藻贼能够运行的基础。陨孕地址共含 源个字节,猿圆位二进制。在书写时,每个字节都用十进制表示,而字节之间用小圆点隔开。例如,员缘怨援圆圆远援员园远援员源

每个 陨孕地址都惟一地对应于 陨灶贼藻则灶藻贼中的某台主机。一个 陨孕地址不能对应于多台主机,而一台主机则可以拥有多个 陨孕地址。

通常地,陨灶贼藻则灶藻贼服务商 陨杂孕(陨灶贼藻则灶藻贼 杂藻则增蚤糟藻 孕则燥增蚤凿藻则)则拥有由 陨孕地址注册服务机构提供的

陨孕地址,然后再将这些地址分配给访问 陨灶贼藻则灶藻贼的客户。在分配给最终客户 陨孕地址时,通常有两种方式:一种是给客户分配固定的 陨孕地址;另一种是每次在客户登录时,陨杂孕动态地在自己的 陨孕地址空间中选择一个地址分配给客户。显然,第二种方式 陨孕地址的利用率更高。

(猿)域名

为了方便用户记忆,陨灶贼藻则灶藻贼引进了域名服务系统 阅晕杂(阅燥皂葬蚤灶 晕葬皂藻 杂赠泽贼藻皂)。域名就是陨灶贼藻则灶藻贼上的主机的名字。域名采用层次结构,每一层构成一个子域名,子域名之间用圆点隔开,自左至右分别为:计算机名援网络名援机构名援最高域名。其中,最高域名又有两类,即以机构区分的最高域名和以地域区分的最高域名。

以机构区分的最高域名原来有 苑个:糟燥皂(商用机构)、早燥增(政府机构)、皂蚤造(军事机构)、燥则早(非盈利组织)、藻凿怎(教育部门)、蚤灶贼(国际机构)、灶藻贼(网络机构)。员怨怨苑年又新增 苑个最高级标准域名:枣蚤则皂(企业和公司)、泽贼燥则藻(商业企业)、憎藻遭(从事与 宰宰宰相关业务的实体)、葬则贼泽(从事文化娱乐的实体)、则藻糟(从事休闲娱乐业的实体)、蚤灶枣燥(从事信息服务业的实体)、灶燥皂(从事个人活动的个体)。

以地域区分的最高域名主要有:葬择(南极洲)、葬则(阿根廷)、葬贼(奥地利)、葬怎(澳大利亚)、遭藻(比利时)、遭则(巴西)、糟葬(加拿大)、糟澡(瑞士)、糟灶(中国)、凿藻(德国)、凿噪(丹麦)、藻泽(西班牙)、枣蚤(芬兰)、枣则(法国)、早则(希腊)、蚤藻(爱尔兰)、蚤造(以色列)、蚤灶(印度)、蚤泽(冰岛)、蚤贼(意大利)、躁责(日本)、噪则(韩国)、皂赠(马来西亚)、灶造(荷兰)、灶燥(挪威)、灶扎(新西兰)、责贼(葡萄牙)、则怎(俄罗斯)、泽藻(瑞典)、泽早(新加坡)、贼澡(泰国)、贼憎(中国台湾)、怎噪或 早遭(英国)、怎泽(美国)(一般可省略)等。

例如,重庆市数据通信局的热线域名注册分为:

员)国际域名。如 憎憎憎援糟择择噪燥蚤灶枣燥援糟燥皂等。

圆)国内域名。如 憎憎憎援糟择择噪燥蚤灶枣燥援糟燥皂援糟灶等。

(源)陨灶贼藻则灶藻贼地址

陨灶贼藻则灶藻贼地址,有时称为 哉砸蕴或统一资源定位符,通常以协议名开头,后面是负责管理该站点的组织名称,后缀则标识该组织的类型。

例如,地址“ 澡贼贼责:辕辕憎憎憎援赠葬造藻援藻凿怎”提供下列信息:澡贼贼责表示这台 宰藻遭服务器使用 匀栽栽孕协议;憎憎憎表示该站点在 宰燥则造凿宰蚤凿藻宰藻遭上;赠葬造藻表示该 宰藻遭服务器位于耶鲁大学;藻凿怎表示属于教育机构。

(缘)耘原皂葬蚤造地址

陨灶贼藻则灶藻贼上,所谓地址总是指电子邮件的地址,即 耘原皂葬蚤造地址。耘原皂葬蚤造地址具有统一的标准格式:用户名岳主机域名,用户名就是你在主机上使用的用户码,岳符号后是你使用的计算机域名。岳可以读成“葬贼”,也就是“在”的意思。例如,耘原皂葬蚤造地址为:<u>扎澡葬灶早泽葬灶岳责怎遭造蚤糟援糟择援糟择援灶藻贼援糟灶</u>,说明该用户位于中国重庆市数据通信局的 责怎遭造蚤糟主机上,用户名为 扎澡葬灶早泽葬灶。

第 2 章

计算机网络安全基础

2.1 计算机网络安全研究背景

在信息技术高速发展的今天，计算机通信网络在政治、军事、金融、商业、交通、电信、文教等方面的作用日益增大。社会对计算机网络的依赖也日益增强，尤其是计算机技术和通信技术相结合所形成的信息基础设施已经成为反映信息社会特征最重要的基础设施。人们建立了各种各样完备的信息系统，使得人类社会的一些机密和财富高度集中于计算机中。但是这些信息系统都是依靠计算机网络接收和处理信息，实现其相互间的联系和对目标的管理、控制。以网络方式获得信息和交流信息已成为现代信息社会的一个重要特征，特别是 [illegible] 的迅猛发展，网络的重要性和对社会的影响也越来越大。随着网络上各种新业务的兴起，比如电子商务（[illegible]）、电子现金（[illegible]）、数字货币（[illegible]）、网络银行（[illegible]）等的兴起，以及各种专用网（比如金融网等）的建设等，使人们在感受网络给社会文明带来巨大贡献的同时，也认识到了网络安全问题的日益突出。因此，对网络安全技术的研究已成为现在计算机和通信界的一个热点，并且成为信息科学的一个重要研究领域。

现在世界上每年因利用计算机网络进行犯罪所造成的直接经济损失之大令人吃惊。据美国 [illegible] 联合会（[illegible]）调查和专家估计，美国每年因计算机犯罪所造成的经济损失高达 [illegible] 亿美元。据报道，在 [illegible] 上，每天大约有 [illegible] 起计算机犯罪发生。[illegible] 的安全案件已由 [illegible] 年的 [illegible] 起猛增到 [illegible] 年的 [illegible] 多起，并且还有很多安全案件并没有被公布。美国国防部的网络也受到网络黑客们的不断攻击，甚至有的攻击者达到了系统管理员的水平。[illegible] 年美国曾有一个计算机技术人员利用计算机网络闯入一银行资金传输系统，造成了 [illegible] 万美元的经济损失。[illegible] 年 [illegible] 月美国发生“ 圣诞卡 ”事件，某跨国计算机公司内部网由于一个图形格式的圣诞卡电子邮件到处传递，致使整个公司网络停止使用 [illegible] 天。[illegible] 年 [illegible] 月，美国康乃尔大学的学生 [illegible] 编制的称为蠕虫（[illegible]）的计算机病毒通过 [illegible] 网传播，致使网络中约 [illegible] 台计算机被传染，造成经济损失约 [illegible] 亿美元。近几年，国内外很多著名站点的主页被黑客恶意修改，在社会上造成了许多不良的影响，也给这些站点的 [illegible] 服务提供商（[illegible]）带来了巨大的经济损失。另外，利用计算机通过 [illegible] 窃取军事机密的事[illegible]

例在国外也是屡见不鲜。美国、德国、英国、法国和韩国等国的黑客曾利用 [illegible] 网分别进入了五角大楼、航天局、北约总部和欧洲核研究中心的计算机数据库。更为严重的是,世界上各个国家之间为了达到其政治、经济、军事、文化等方面的战略目的,掀起了一场前所未有的战争——信息战 [illegible],其实质是利用各种计算机攻击手段,攻击敌方的信息系统,夺取对方的“制信息权”,来达到摧毁对方的目的。

我国的信息化进程虽然起步较晚,但近几年发展迅速,网络已经渗透到国民经济的各个领域,渗透到了工作和生活的方方面面。在短短的几年时间里,也发生了多起针对和利用计算机网络进行犯罪的案件,给国家、企业和个人造成了重大的经济损失和危害,特别是具有行业特性(例如金融部门等)的犯罪,更是令人触目惊心。

网络上的信息安全问题直接关系到国家的经济利益和安全。因此,各国政府无不重视信息安全,特别是西方发达国家均大力加强信息安全的研究和督导。在国际大形势下,我国政府对信息和网络安全事业的发展给予了充分的重视,国家领导人多次发出有关信息安全的指示。主管部门公安部做了大量实质性的工作,除颁布计算机安全保护条例等法规性文件、指导制定和修改我国刑法有关高科技犯罪的条款以外,还从事信息安全产品的测试和认证,黑客入侵和计算机病毒等高科技犯罪的防范,计算机犯罪和高科技犯罪的监察等重要工作。

但是,许多企、事业单位和政府机构的现有计算机网络大多数在建设之初都忽略了安全问题,即使考虑了安全,也只是把安全机制建立在物理安全机制上,随着网络的互联程度的扩大,这种安全机制对于网络环境来讲形同虚设。网络的安全措施一般分为 猿类 :逻辑上的、物理上的和政策上的。面对越来越严重危害计算机网络安全的种种威胁,仅仅利用物理上和政策(法律)上的手段来有效地防止计算机犯罪是困难的。由于目前互联网络上使用的 [illegible] 协议在制订之初就没有考虑安全问题,所以没有安全可言。开放性和资源共享是计算机网络安全问题的主要根源,它的安全性主要依赖于加密、网络用户身份鉴别、存取控制策略等技术手段。因此,必须采用逻辑上的措施,即研究与发展有效的网络安全技术,如 :安全协议、密码技术、数字签名、防火墙、安全管理、安全审计等,以防止网络传输的信息被非法窃取、篡改和伪造,确保网络系统和数据的真实性和完整性。

圆援猿摇计算机网络安全基础知识

圆援猿援员摇计算机网络安全的内涵

网络安全从其本质上来讲就是网络上的信息安全,它涉及的领域相当广泛。这是因为在目前的公用通信网络中存在着各种各样的安全漏洞和威胁。从广义来说,凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论,都是网络安全所要研究的领域。下面给出网络安全的一个通用定义:

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护,不因偶然的或者恶意的原因而遭到破坏、更改、泄露,系统连续可靠正常地运行,网络服务不中断。

从用户(个人、企业等)的角度来说,他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护,避免其他人或对手利用窃听、冒充、篡改、抵赖等