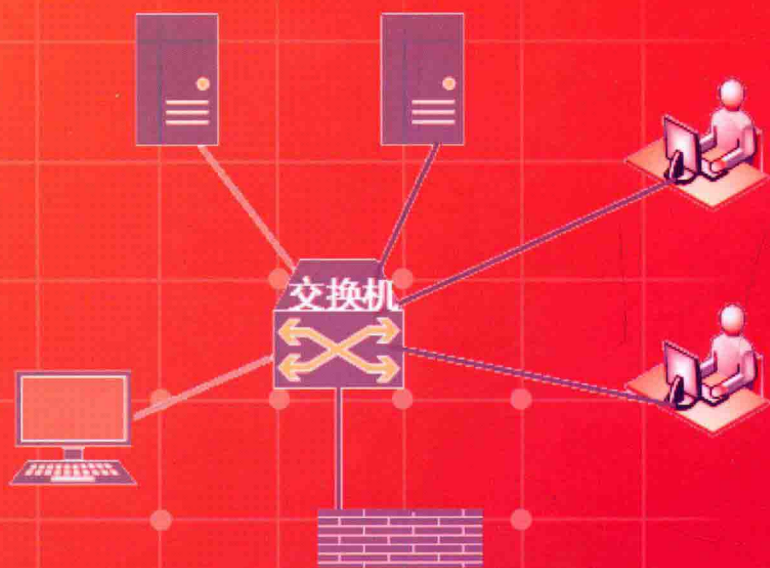


山东省高等教育名校建设工程课程改革教材

网络工程设计与施工

张殿明 申加亮 主编
安丰鹤 主审



 黄河水利出版社

山东省高等教育名校建设工程课程改革教材

网络工程设计与施工

主 编 张殿明 申加亮

副主编 黄鲁新

主 审 安丰鹤

黄河水利出版社

· 郑 州 ·

内 容 提 要

本书是本着高职教育的特色,依据中央财政支持专业建设方案和山东省特色名校建设方案要求进行编写的。本书内容以工作任务为依托,采用项目形式编写,全面、系统地介绍了网络工程设计的理论、技术,以及施工的工程标准与方法,主要涉及网络工程设计基本知识、高速局域网设计、广域接入网设计、服务器系统设计、网络存储与备份设计、网络安全设计以及综合布线系统工程等技术内容。为读者提供了大中型企业网、广域接入网、企业资源服务器与网络存储、网络安全接入、综合布线等技术方案。

本书可作为高等职业院校电气自动化、电子信息工程、通信技术、计算机网络技术等专业网络工程课程的教学用书,也可作为培养企业网络信息化人才的实用教材,同时可作为综合布线行业、智能管理系统行业和安全技术防范行业工程设计、施工和管理等专业技术人员的参考书。

图书在版编目(CIP)数据

网络工程设计与施工/张殿明,申加亮主编. —郑州:
黄河水利出版社,2015. 8

山东省高等教育名校建设工程课程改革教材
ISBN 978 -7 -5509 -1201 -4

I. ①网… II. ①张… ②申… III. ①计算机网
络—高等教育—教材 IV. ①TP393

中国版本图书馆CIP数据核字(2015)第198951号

组稿编辑:王路平 电话:0371-66022212 E-mail:hhsllwlp@163.com

出版社:黄河水利出版社

地址:河南省郑州市顺河路黄委会综合楼14层 邮政编码:450003

发行单位:黄河水利出版社

发行部电话:0371-66026940、66020550、66028024、66022620(传真)

E-mail:hhsllcbs@126.com

承印单位:郑州龙洋印务有限公司

开本:787 mm × 1 092 mm 1/16

印张:19.5

字数:450千字

印数:1—1 000

版次:2015年8月第1版

印次:2015年8月第1次印刷

定价:46.00元



前言

本书是依据中央财政支持提升社会服务能力重点建设专业和山东省高等教育名校建设工程重点建设专业人才培养方案和课程建设目标要求,当前电子信息工程、电气自动化技术、通信技术等专业的发展需要,并按照国家及行业有关网络工程项目设计与施工的新规范、新法规、新标准编写完成的。在吸收有关教材和技术文献资料精华的基础上,充实了新思想、新理论、新方法和新技术。

本书教学内容以工作任务为依托,并结合多位编者多年来的教学实践以及在网络工程实施中的经验教训,遵循项目驱动的教学模式而编写的一本网络工程设计与实施项目教程。全书分为八个项目,每个项目都设置了6个教学环节:项目描述-任务展示-任务知识-任务实施-项目小结-项目检测,从项目准备到项目实施再到效果检查,过程完整。本书全面、系统地介绍了网络工程设计的理论、技术,以及施工的工程标准与方法,主要涉及网络工程设计基础、高速局域网规划设计与施工、广域网设计与施工、服务器系统设计与实施、网络存储和备份的设计与实施、网络安全设计与实施以及综合布线系统设计与施工等内容,可为读者提供大中型企业网、广域接入网、企业资源服务器与网络存储、网络安全接入、综合布线等技术方案和实施指导。本书内容丰富、图文并茂、深入浅出,对于帮助读者全面掌握网络工程设计方法,提高网络工程施工能力颇具实用价值。

本书具有以下特点:

(1)在编写中注重学生应用能力、分析能力和基本技能的培养,突出了高职、高专学生的培养目标,淡化理论的叙述,突出了学生实践技能的培养。

(2)以“工学结合”为主线,以培养学生的实践动手能力为目标,注重学生职业能力训练和综合素质培养,体现了高等职业教育的特点,突出了适用性、实践性、创新性的教材特色。结合当前应用最广泛的网络工程技术设计项目内容,保证学生能够获取跟实际紧密联系的知识和技能。

(3)适应高职高专学生的实际知识水平,注重学生专业的发展和就业的需要,各项目均从基础知识入手,循序渐进,有效激发学生的学习兴趣,理论学习和实践操作相结合,重在提高学生动手的实践能力。

本书在编写、修改过程中,有企业、行业的专家亲自参与,实用性和实时性强,内容更贴近网络工程实际,是一本典型的校企合作开发教材。

本书由山东水利职业学院主持编写工作,编写人员及编写分工如下:项目一和项目二由山东水利职业学院张殿明编写,项目三由中国网通(集团)有限公司日照市分公司工程部郭建峰编写,项目四由日照海博电子科技有限公司牟建中编写,项目五由山东水利职业学院申加亮编写,项目六由中国网通(集团)有限公司日照市分公司工程部杨毅编写,项目七由山东水利职业学院钱玉霞编写,项目八由山东水利职业学院张鹏编写。本书由张



殿明、申加亮担任主编,张殿明负责全书策划组织和统稿工作,申加亮负责编写人员的组织和协调工作;由黄鲁新担任副主编,负责稿件的校对修改工作;由日照市公路管理局安丰鹤担任主审。

由于编者水平有限,书中难免存在一些差错和问题,希望读者批评指正。

编者

2015年1月



目 录

前 言

项目一 网络工程设计基础	(1)
任务一 掌握网络工程设计的相关概念	(1)
任务二 网络工程需求分析	(3)
任务三 网络工程设计方法	(7)
项目二 高速局域网规划设计与施工	(22)
任务一 了解高速以太网技术概况	(23)
任务二 以太网设备的配置	(30)
任务三 网络多层交换与互联	(36)
任务四 无线局域网设计与实施	(44)
项目三 广域网设计与施工	(67)
任务一 了解广域网基本知识	(67)
任务二 路由器配置	(69)
任务三 广域网设计	(79)
项目四 服务器系统设计与实施	(106)
任务一 了解服务器的基本知识	(106)
任务二 Web 服务系统的架构	(113)
任务三 服务器软硬件的选择	(118)
任务四 服务器双机集群与热备	(128)
项目五 网络存储和备份的设计与实施	(143)
任务一 了解网络存储技术	(143)
任务二 网络存储系统设计	(152)
任务三 数据备份与恢复	(158)
任务四 中小型网络数据备份与恢复	(162)
项目六 网络安全设计与实施	(171)
任务一 了解网络安全设计的原则	(171)
任务二 网络安全威胁与防范	(173)
任务三 网络安全接入与认证	(182)
任务四 操作系统安全设计	(187)
任务五 Web 服务器安全设计	(191)



任务六 网络边界安全设计	(193)
项目七 综合布线系统设计与施工	(209)
任务一 认识网络综合布线系统	(209)
任务二 认识综合布线系统的器材和工具	(219)
任务三 网络综合布线系统的设计与实施	(231)
项目八 网络工程项目管理与验收	(269)
任务一 了解网络工程项目质量管理的相关内容	(269)
任务二 网络工程项目成本及效益分析	(273)
任务三 网络故障的诊断与排除	(282)
任务四 网络工程项目的验收	(298)
任务五 网络工程项目的评估	(302)
参考文献	(306)



项目一 网络工程设计基础

【项目描述】

在当前的网络工程项目建设中,企业网的建设是非常重要的,企业网内部各种不同业务的开展是企业网发展迅速的最主要原因。从早期的企业网主要是简单的数据共享、简单数据库的共享到现在内部全方位的数据共享,从过去单一的企业到现在异地甚至分布在全球的多个分支公司的全部互联,对网络的覆盖面要求越来越广,这一要求现在已经面向整个企业、整个行业,甚至整个互联网。

本项目要完成以下任务:

- (1)掌握网络工程设计的相关概念。
- (2)能够进行网络工程需求分析。
- (3)掌握网络工程设计的方法。

任务一 掌握网络工程设计的相关概念

【任务展示】

在进行网络工程设计时,网络工程设计者首先要搞清楚网络技术集成、网络设备集成和网络应用集成三方面的要求;其次,将用户方的需求用网络工程的语言表述出来,使用户理解设计者所做的工作。

【任务知识】

关键知识点 1:网络工程设计概念

计算机网络工程描述性定义:计算机网络工程是指为了达到一定应用的目标,根据相关的标准和规范,通过详细的分析、规划和设计,按照可行性的设计方案,将计算机网络技术、系统、管理,高效地集成到一起的工程。

也可简单地描述为:将系统化的、规范的、可度量的方法应用于网络系统的设计、建造和维护的过程,即将工程化应用于网络系统之中。

关键知识点 2:网络工程设计目标

网络设计遵循技术和行业标准的指导原则,确保设计的解决方案满足网络建设的需要,并符合 IT 建设的标准,为将来的网络升级提供向后兼容能力。在整体方案设计中,遵



循以下原则。

(一)有效性和可靠性

网络的有效性和可靠性即它的可连续运行性是网络建设必须考虑的首要原则,从用户的角度考虑,当网络所需的服务不再提供服务时,不管是何种原因,网络就失去了实际价值;从另一角度看,当某种网络服务的响应时间变幻莫测时,网络系统也就不可靠了。在网络设计上考虑以下的技术:

(1)选择的网络设备必须具有良好的可靠性保证,可热插拔的模块,快速的恢复机制等。

(2)冗余及负载均衡的电源系统。

(3)其他关键设备的冗余,如控制模块的冗余、负载均衡的网络链路冗余。确保不因单条线路的故障而导致整个网络系统的失效,而且确保在某条线路故障时对系统性能的影响最小。

(二)灵活性和扩展性

随着计算机应用的日益普及和进步,对网络系统的可伸缩性要求成为网络设计的一个重要考虑。一个设计良好的网络系统应能方便地对其规模或技术进行扩充。用户对网络资源的需求经常随着应用而发生变化,系统应具有一定的灵活性,为满足用户的不同需求而进行灵活的系统配置和资源的再分配。

网络将会是一个不断增长的网络,它的规模、应用范围和服务内容将随着计算机应用的不断普及而不断增加,因此在网络设计上必须非常重视网络的扩展能力。网络的扩展包括如下内容:

(1)网络规模的扩展。包括网络的地理分布,用户数。

(2)应用内容的扩展。包括视频和语音服务也会不断加入到 IP 网络中去需求,这就要求主干网络设备必须具有多种业务支持的能力。

(3)网络容量的扩展。随着规模和应用的扩展网络的传输容量也必须能相应地增加。

在网络设备选择上,模块化的系统在可伸缩性上亦有着固定式系统无法比拟的优越性。整个系统的性能将能随着模块数量的增加而得到相应的增加,因此也就更能适应不同规模网络对设备的要求。模块化的网络设备在多种技术的适应能力上也具有相当大的灵活性。网络系统具有统一的系统平台,具有平滑升级的能力,使系统能满足各种用户对应用处理不同程度的需求以及逐步升级的发展规划,以节约投资,避免系统性能的闲置和浪费。

(三)开放性和先进性

系统具有开放性,意味着遵循计算机系统和网络系统所共同遵循的标准。园区主干网络的特点注定系统应具备有与其他系统和网络互操作和互联的能力,以实现内部各系统之间,以及有关其他领域的交流,如与 Internet 的互联,与各外地分支网络的互联等。开放性还意味着更多的选择和最佳的性能价格比,有利于在众多满足同一开放性标准的硬件、软件系统中选择最符合要求的产品。同时,可以保证在不降低性能的前提下使用第三方标准的产品,以降低用户投入成本。



(四) 可管理性和可维护性

在一个网络系统中,网络管理已经越来越受到人们的重视。因为它关系到网络系统的使用效率、维护、监控甚至系统资源的再分配。

网络管理对系统的重要性越来越大,这是由于系统对网络环境的依赖性不断增加,一方面,由于网络中断而使业务被迫中止造成的损失会越来越大;另一方面,由于越来越多的用户连入网络,对网络管理的要求提高了,以确保网络达到最高的效率。

关键知识点 3: 网络工程标准

计算机网络的体系结构和国际标准化组织(ISO)提出的开放的系统互联参考模型(OSI)已得到广泛认同,并提供了一个便于理解、易于开发和加强标准化的统一的计算机网络体系结构。

IEEE 802.3 标准是一种永久载波传感多路访问局域网。其基本思想是:当有一个站希望发送时就监听电缆。如果此时电缆忙,该站就等待,直到电缆空闲后再发送;如果在一根空闲电缆上有两个或多个站同时开始传送,便会产生冲突,所发生冲突的站都结束发送,等待时机,然后再重复上述整个过程。

所有 IEEE 802 实现的产品都直接使用曼彻斯特编码。IEEE 802 允许的最大电缆长度为 500 M,为了使网络扩展到较大范围、多根电缆可以用中继器联接起来。一个系统可以有段电缆和多个中继器,但两个收发器之间不能超过 2.5 km,任何两个收发器之间的路径上不能跨过多于 4 个中继器。IEEE 802.3 是基于概率统计的媒体访问控制协议,某个站的运气稍差一点其发送一个帧可能要等任意长的时间。另外,IEEE 802.3 的帧没有优先级,从而 IEEE 802.3 不适应实时系统。

网络产品符合 IEEE 802.3 标准的以太网(Ethernet),其拓扑结构是总线型的,访问控制采用 CSMA/CD 方式,传输速率为 10 Mbps。

除此之外,在双绞线以太网的基础上发展起来的快速以太网(100BASE-T),符合 IEEE 802.3u 标准。IEEE 802.3u 标准与 IEEE 802.3(10BASE-T)标准在媒体访问方法、协议和数据帧结构方面基本相同,不同的是 IEEE 802.3u 标准在速度上进行了升级。在拓扑结构上,快速以太网不是总线型拓扑结构,而是采用星型拓扑结构,快速以太网支持全双工方式,使得实际数据传输速率能够达到 200 Mbps。快速以太网便可使原来 10BASE-T 以太网的用户在不改变网络布线、网络管理、检测技术以及网络管理软件的情况下,顺利地向 100 Mbps 快速以太网升级。

任务二 网络工程需求分析

【任务展示】

需求分析是网络设计过程的基础。无论是从工作量,还是从重要性来看,它都占到了网络系统工程约 60% 的份额。对网络系统的设计和经费预算有直接的影响。

【任务知识】

关键知识点 1: 网络工程人员

系统集成人员应了解用户需求,用户方应了解技术方面的需求,两者缺一不可。用户需求的问题:

- (1) 提不出具体需求,仅凭想象。
- (2) 提出不切实际的、过高的要求。
- (3) 不断变化需求,使人无所适从。

因此,系统集成人员要引导用户,将自己的想法告诉用户,取得共识与谅解。

关键知识点 2: 需求分析

(一) 需求分析的目的

需求分析是网络设计的基础,需求分析需要我们与用户沟通,并将用户模糊的想法明确化以及具体化,不正确的需求分析会导致网络设计结果跟用户应用需求不一致,这就会产生所谓的蠕动效果,这就会使得我们的项目被不断地延期甚至被迫终结。需求分析通常包括以下部分:

(1) 分析技术目标与约束:这是从技术角度分析未来网络的功能需求是不是已经满足用户的需求。

(2) 辨别商业目标和约束:理解网络商业的本质的关键步骤,它将贯穿我们整个网络设计的整个过程,需要明确用户的投资规模等。

(3) 刻画未来网络通信需求特征。

(4) 刻画现有网络的特征。

(二) 需求来源

进行需求分析,首先要收集需求信息,那么需求的来源大致可以分为政策上和技术上两个方面,把它细化可以分为:决策者的建设思路、国家/行业政策、用户技术人员细节描述、用户能提供的各种资料等。这里比较有直观效果的就是用户技术人员的细节描述以及用户能够提供的各种资料。

(三) 需求收集

需求收集从下面几个方面进行:

(1) 商业需求:商业需求需要注意几个方面:确定关键转折点、确定网络投资规模、预测增长率

(2) 用户需求:与用户群交流、列出服务需求、列出性能需求。通常我们是从用户的人员组织结构图入手,比如采用一些问卷调查、集中访谈等方式交流,交流过程中必须找出哪些功能和服务是用户完成工作所必需的,而网络设计中,需要对这些服务需求进行整理。这里需要注意的是,用户并不总是从技术角度描述需求,而是从一些使用性能上来反映。

(3) 应用需求,分为可靠性/可用率、响应时间、安全性、可实现性、实时性等。

(4) 计算机平台需求。

(5) 网络需求:首先需要知道当前的网络拓扑结构,其次还需要看看当前这个网络的网络协议,还有就是安全需求、网络设备和广域网连接的手段等。

每一个需求的收集都要形成文档,有了文档我们才能方便地完成后面一些工作。

(四) 需求分析整理

首先应该将当前的网络业务情况总结出来,然后再进行新网络建设思路的整理,包括线路的选择、三网合一、安全性、可靠性、扩充性和今后的业务范畴。

关键知识点 3:可行性分析

(一) 分析网络应用约束

商业的约束对网络设计影响较高,也需要认真分析。

- 政策约束;
- 预算约束;
- 时间约束;
- 应用目标检查表。

(二) 网络分析的技术指标

(1) 影响网络性能的主要因素:

- 距离;
- 时效;
- 拥塞;
- 服务类型;
- 可行性;
- 信息冗余;
- 一点决定整体。

(2) 网络性能参数:

- 时延;
- 吞吐量;
- 丢包率;
- 时延抖动;
- 路由器;
- 带宽;
- 响应时间;
- 利用率;
- 效率。

(3) 可用性(availability):指网络或网络设备可用于执行预期任务的时间总量(百分比),即

$$\text{可用性} = \frac{\text{运行总时间}}{\text{预期总时间}} \times 100$$



(4)可扩展性(scalability):是指网络技术或设备随着客户需求的增长而扩充的能力。主要包括的内容有信息点的增加、网络的规模、服务器的数量等。

(5)安全性(security):安全性设计是企业网设计的最重要方面之一,它能防止商业数据和其他资源的丢失或破坏。

(6)可管理性。

(7)适应性。

(三)确定网络的规模

(1)确定网络的规模即明确网络建设的范围,这是通盘考虑问题的前提。网络规模一般分为以下4种:

- 工作组或小型办公室局域网;
- 部门局域网;
- 骨干网络;
- 企业级网络。

(2)确定网络的规模涉及以下方面的内容:

- 哪些部门需要进入网;
- 哪些资源需要上网;
- 有多少网络用户;
- 采用什么档次的设备;
- 网络及终端设备的数量。

(四)网络拓扑结构分析

拓扑结构分析要明确以下指标:

- 网络的接入点(访问网络的入口)的数量;
- 网络接入点的分布位置;
- 网络连接的转接点分布位置;
- 网络设备间的位置;
- 网络中各种连接的距离参数;
- 其他结构化综合布线系统中的基本指标。

关键知识点4:网络工程设计方案

不管是作为售前还是售后,当拿到一个项目的时候,都必须要了解用户的环境,他当前的应用以及他期望的应用有哪些,还有他当前使用的网络产品和他期望使用的网络产品,这些对于一个售前人员或者是一个项目经理来说,都是必须事先要了解的,这样我们才可以给客户所谓定制化的、最优的网络设计方案。

(一)企业网络的构成

对于一个企业来说,企业网络的构成,主要有下面6个方面:

(1)应用软件:指支持用户完成一些特定*作的软体,而对于应用软件来说,它根据工作方式的区分,分为单机模式和网络模式两种,不同的工作模式对网络会有不同的需求。



(2) 计算平台。

(3) 物理网络及拓扑结构:指从网卡到网卡之间位于网络之间的基础结构,包括电缆、连接器、插线板、集线器等。

(4) 网络软件及工具软件:网络软件是用来在客户端和服务器之间传输信息的协议栈,对于网络软件来说,最主要的就是网络操作系统。

(5) 网络互联设备:网络设备的选择在网络设计中是一个关键的决策。

(6) 广域网连接。

(二) 网络的生命周期

对于一个网络,从设计好到它生命的终止,主要分为4个阶段:

(1) 网络构思与计划阶段:必须明确网络结构体系,了解客户的需求,根据客户的需求来给客户设计一个最佳的网络方案,这个方案必须考虑到相关的设计目标和一些有可能的约束情况,如果没有正确的计划和对未来发展的考虑,这种实施和扩展网络都会变得非常的困难。

(2) 分析与设计阶段:这是网络生命周期中一个非常重要的步骤,这个步骤主要考虑公司的整个需求、考虑用户的需求、确定网络结构这几个部分,这个阶段还需要输出一些结果,比如用户的需求说明书、网络的逻辑图、网络物理连接图、网络地址的一些分配、物理设备说明、用户确认文件等,这些都可以作为我们网络实施的一些参考。

(3) 实施阶段:指定项目经理,指定实施工程师,然后根据设计和分析的结果完成网络的实施,

(4) 运行与维护阶段:一个网络实施好了如果没有很好的维护,那它的生命力是不会长的,因此实施过的网络必须要有一整套运营和维护的手段,这个阶段可能需要用户不断的投资来对网络做有关的维护、改造、升级、换代等工作,这样才可以保证我们一个网络的生命周期很长,但是这也导致用户针对网络的连续投资。

(三) 网络设计目标

(1) 最低运作成本。

(2) 不断增强的整体性能。

(3) 易于操作和使用。

(4) 充分的可靠性。

(5) 完备的安全性。

(6) 可扩展性。

作为投资方来说,它最关注的只有两点:成本和性能,如何能够达到最好的性价比就是我们的目标。

任务三 网络工程设计方法

【任务展示】

以网络设备实际物理地址为依据生成的拓扑图我们称之为物理拓扑,物理拓扑的生

成方式是根据 SNMP 协议扫描网络自动生成的。物理拓扑反映实际的物理网络环境。物理拓扑图如图 1-1 所示。

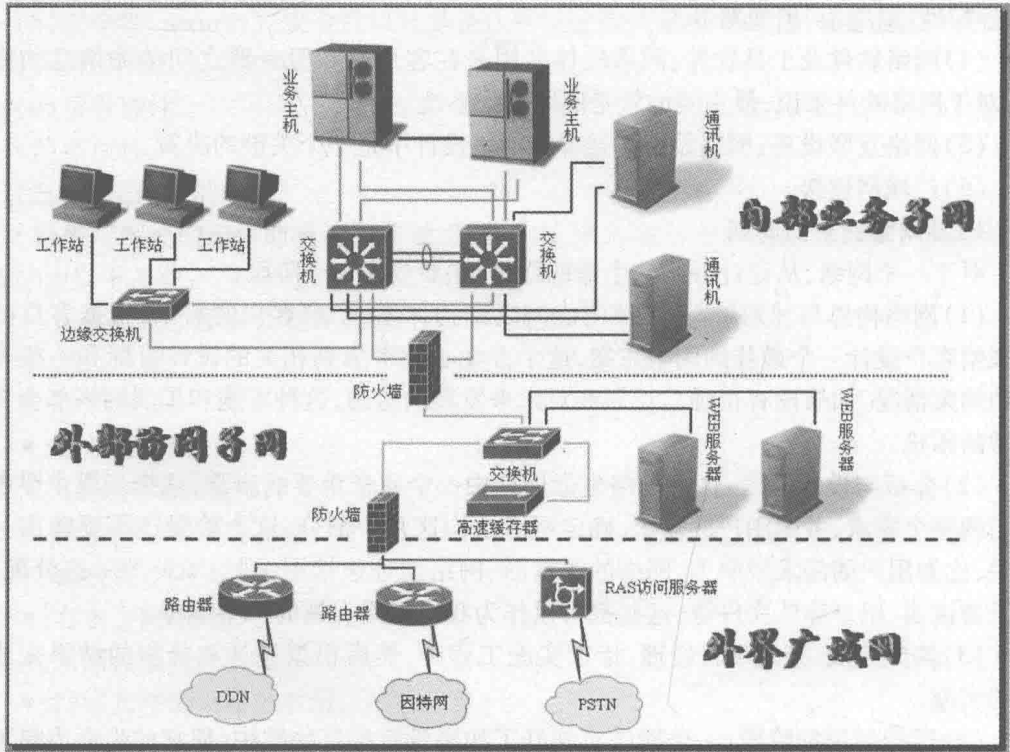


图 1-1 物理拓扑图

【任务知识】

关键知识点 1: 物理拓扑图

由于物理拓扑图是根据网络设备的实际物理地址进行扫描而得出的,所以它更加适合的是网络设备层管理,一旦网络中出现故障或者即将出现故障,物理拓扑图可以及时、详细地告诉网络管理者是哪一台网络设备出了问题。举个简单的例子,当网络中某台交换机出现了故障,通过物理拓扑图,网管系统可以告诉管理者在网络里众多的交换设备中是哪一台交换机的哪一个端口出现了问题,通过这个端口连接了哪些网络设备,便于网管人员进行维护。

对于物理拓扑图来说,由于它是基于 SNMP 协议自动扫描网络而生成的,在精确程度上需要我们仔细地进行检查。这是因为,网络设备品牌型号众多,如果想要生成精确的拓扑图就必须对不同品牌和型号的网络设备的内部 MIB 库有足够的了解。而网管系统厂商如果想把市场上所有的网络设备的 MIB 库掌握完全显然是不现实的,所以没有一家网络管理系统的厂商敢于保证他们的产品在每一个网络中都能生成 100% 准确的物理拓扑图。换句话说,物理拓扑图生成的准确与否是网管系统厂商长期积累的结果。同时,如果网络中的某些备用设备没有开启,那么在扫描生成物理拓扑图的过程中是无法发现这些

没有开启的备用设备的。

关键知识点 2: 网络系统层次划分

对于计算机网络系统这样一个十分复杂的系统, 分层是系统分解的最好方法之一。利用分层的思想, 可将计算机网络表示为图 1-2 所示的层次结构模型。

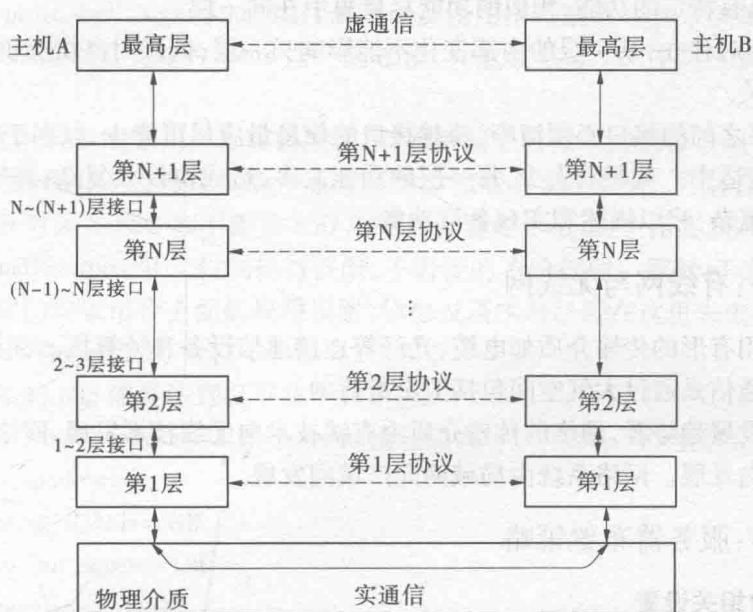


图 1-2 计算机网络的层次结构模型

(一) 网络层次结构的特点

- (1) 以功能作为划分层次的基础。
- (2) 第 N 层是 $N-1$ 层的用户, 同时是 $N+1$ 层的服务提供者。
- (3) 第 N 层向 $N+1$ 层提供的服务不仅包含第 N 层本身的功能, 还包含 N 层以下各层提供的服务。
- (4) 同一主机相邻层之间都有一个接口, 该接口定义了下层向上层提供的操作原语和服务。该接口中交换信息的地方称为服务访问点 (SAP), 它是相邻两层实体的逻辑接口, 即 N 层上面的 SAP 就是 $N+1$ 层可以访问 N 层的地方。
- (5) 除了在物理介质上进行的是实通信外, 其余各对等层实体间进行的都是逻辑通信 (虚通信)。除最低层外, 一台主机的第 N 层与另一台主机的第 N 层进行通信, 并不是同一层数据的直接传送, 而是将数据和控制信息通过层间接口传送给相邻的 $N-1$ 层, 直至底层。在底层再通过物理介质实现与另一台主机底层的物理通信 (实通信)。

(二) 网络层次结构中的协议

- (1) 不同主机同一层次 (对等层) 实体之间进行的通信。
- (2) 同一主机相邻层的实体之间进行的通信。

(三) 网络层次结构的优点

- (1) 各层的功能明确,并且相互独立。
- (2) 易于实现和维护。
- (3) 易于实现标准化。

(四) 网络层次结构的划分原则

- (1) 每层具有特定的功能,相似的功能尽量集中在同一层。
- (2) 各层相对独立,某一层的内部变化不能影响另一层,低层对高层提供的服务与低层如何完成无关。
- (3) 相邻层之间的接口必须清晰,跨越接口的信息量应尽可能少,以利于标准化。
- (4) 层数应适中。若层数太少,每一层的功能太多,造成协议太复杂;若层数太多,则体系结构过于复杂,难以描述和实现各层功能。

关键知识点 3: 有线网与无线网

有线网使用有形的传输介质如电缆、光纤等连接通信设备和计算机。在无线网络中,计算机之间的通信是通过大气空间包括卫星进行的。

从网络的发展趋势看,网络的传输介质由有线技术向无线技术发展,网络上传输的信息向多媒体方向发展。网络系统由局域网向广域网发展。

关键知识点 4: 服务器布置策略

(一) IIS 的相关设置

删除默认建立的站点的虚拟目录,停止默认 web 站点,删除对应的文件目录 c:\inetpub,配置所有站点的公共设置,设置好相关的连接数限制,带宽设置以及性能设置等其他设置。配置应用程序映射,删除所有不必要的应用程序扩展,只保留 asp、php、cgi、pl、aspx 应用程序扩展。对于 php 和 cgi,推荐使用 isapi 方式解析,用 exe 解析对安全性和性能有所影响。用户程序调试设置发送文本错误信息给用户。对于数据库,尽量采用 mdb 后缀,不需要更改为 asp,可在 IIS 中设置一个 mdb 的扩展映射,将这个映射使用一个无关的 dll 文件如 C:\WINNT\system32\inetsrv\inc.dll 来防止数据库被下载。设置 IIS 的日志保存目录,调整日志记录信息。设置为发送文本错误信息。修改 403 错误页面,将其转向到其他页,可防止一些扫描器的探测。另外为公开系统信息,防止 TELnet 到 80 端口所泄露的系统版本信息可修改 IIS 的 banner 信息,可以手工修改或者使用相关软件如 banneredit 修改。

对于用户站点所在的目录,在此说明一下,用户的 FTP 根目录下对应三个文件夹,wwwroot, database, logfiles, 分别存放站点文件、数据库备份和该站点的日志。如果一旦发生入侵事件可对该用户站点所在目录设置具体的权限,图片所在的目录只给予列目录的权限,程序所在目录如果不需要生成文件(如生成 html 的程序)不给予写入权限。

(二) ASP 的安全设置

设置过权限和服务之后,防范 asp 木马还需要做以下工作,在 cmd 窗口运行以下命令: