

第四章 IT 服务交付与支持

★ 必须的知识点

(IT Service Delivery and Support)

服务的等级（水平）管理实务；

运营管理最佳实务；

系统性能（效能）监控程序、工具和技术（网络分析器、利用率报告等）；

硬件和网络设备功能；

数据库管理实务；

操作系统、工具软件和数据库管理系统；

生产能力计划和监控技术；

对生产系统的应急变更和调度管理程序，包括变更、配置、发布和补丁管理实务；

事件/问题管理实务（如帮助台、呼叫中心等）；

软件许可和使用清单管理实务；

系统弹性工具和技术（容错硬件、单点失效的排出、服务器集群）

★ 可能的考试重点

物理体系运行（原计算机操作）

无人值守系统、输入输出控制功能、数据管理实务、作业记帐、日程安排、资源使用监控、

事故处理流程、问题管理（异常情况检测归档解决和报告）、支持/帮助台、程序变更控制、

程序库管理系统、库控制软件（可执行文件与源代码的完整性、源代码比较）、版本管理、

质量保证、信息安全管理

信息系统体系结构和软件（原第三章）

操作系统（软件控制参数、软件完整性、活动日志和报告选项）

访问控制软件

数据通信软件

数据管理（文件组织方式）

数据库管理系统（DBMS 结构、元数据结构、数据字典/目录系统、数据库结构、数据库控制）

磁带和磁盘管理系统

实用程序（系统工具）

软件许可

IS 网络基础设施（原第三章）

网络基础知识（基带与宽带）

企业网络架构

网络类型

网络服务

网络标准和协议

OSI 参考模型

OSI 模型在网络体系中的应用（局域网、城域网、广域网、无线网络、互联网）

网络管理和控制（性能度量、网络管理、管理工具）

网络环境的应用系统（C/S、B/S 技术，中间件）

★ 知识点摘要

4.2 信息系统运营

部分内容和第三部分第五部分是一致和重复的 **从体系上看交付和支持是开发的后续 交付和支持的 IS 是信息资产保护的内容**

信息系统的运营承担计算系统软硬件的日常支持工作。

库管员职责

问题处理程序

对资源利用的效率和效果的监控程序

4.2.1 信息系统运营管理

IS 管理层对 IS 部门的全面运行负全部责任。资源分配、标准和程序（符合总体业务战略和政策）、运营程序监控（不断改进处理流程）。

判断类是设施服务水平的标准是行业标准 benchmark

▲控制功能

确保信息系统处理无论在发生**较小**的或重人的中断后，均能及时得到恢复。

监控系统性能和资源情况，以实现计算机资源的最佳使用。

预测设备更换/容量，以保证当前**作业流量的最大化**并为**未来需求**制定战略计划。

4.2.2 IT 服务管理

提高服务质量，降低服务成本，以能满足企业**不断变化的需求**。

IT 支持服务包括服务平台、事件管理、问题管理、**配置管理**、变更管理和版本管理。IT 交付服务包括服务水平管理、IT 财务管理、能力管理、IT 服务持续性管理和可用性管理。

之间是**高度关联**：任何要求的变更，不管是源于解决问题、增强功能或任何其它原因，都必须经过**问题变更管理**。在变更被接受并得到批准前，要审核其**成本效益和可行性研究**。变更可能会涉及到一个或多个配置选项，此时变更管理就会调用**配置管理**流程。**德耳塔版本**中仅包含最近版本以后曾进行过修改的单元。

服务管理包含配置管理数据库(CMDB)，其中存放了每一项配置项目，ITSM 是一种基于**信息技术基础设施库(ITIL)**框架的方法。

▲服务水平

监控服务效率和效果的工具：异常作业终止报告、作业重启报告（job rerun report）、操作员问题报告、输出分发报告、控制台日志（比较复杂难以用作监控，需要 IS 管理层利用其他特定功能的日志）、操作员工作日程表。**服务水平协议(SLAs)** 审核外包的 SLA 时首先是判断是否基于业务需要、其次是成本是否合理、再次是审计权利、最后是安全条款

服务水平指标：风险、安全、控制指标以及效率和效益指标。

4.2.3 基础设施运营 infrastructure operation

▲无人值守 **Lights-out** 运行是重要计算机机房的自动运行，即在无人工干涉的情况下自动执行任务。 **减少系统错误和中断的次数**

▲输入/输出控制功能 • 保证批处理信息得到**准确**和**完整**的处理，且与 IS 管理部门的意图和**授权**一致。 **一对一的键入验证**(对大量数据录入不可行)、数据录入功能和数据录入验证的隔离。

▲作业记账 作业记账应用监控和记录 IS 资源的使用。计费和系统优化。

▲日程安排 高优先级的作业需要优先资源分配。

作业调度软件 一次设置作业，防止错误、保证作业独立性和控制作用先后顺序、控制生产数据访问，减少人工操作依赖，记录作业成功或失败情况。

4.2.4 资源使用监控 由于组织业务越来越依赖于计算机资源，对资源有效的控制很关键。

▲问题管理 意外管理

▲事故处理 意外（事故）管理和问题管理常常很相近，意外管理针对的是马上能够解决的问题，而**问题管理目的在于找出问题的根本原因**，解决问题，并避免以后再次发生。

▲异常情况的检测、归档、控制、解决和报告 出于控制的目的，追加**错误日志**应限制为授权的人员。职责分工则要求结束错误日志的人员应不同于开始记载错误条目的人员。

供应商直接拨入并修改配置和纠正问题的设备 只在**问题存在期间**给予权限

未解决问题缺乏关注的首要风险是可能导致**业务处理的中断**

4.2.5 支持/帮助平台

必须根据**组织的总体战略和政策**来建立技术支持人员执行全部任务时应遵循的程序。对问题根据程序规定的**优先顺序**逐级上报。

4.2.6 程序变更控制(PCC) 作业周转(Turnover)程序

4.2.7 程序库管理系统

4.2.8 程序库控制软件

程序库控制软件来**隔离测试和日常作业程序库** 由于测试版可能包括没有授权的代码或作弊代码，保证变更必须经过**授权**才可以到日常作业程序库

▲**执行码和源代码的完整性** 每个日常作业的执行代码模块应该有一相对应的原始代码模块。每当有更新的程序移入到**日常作业源代码库**，一个编译过的该程序的执行码版本就必须移入到**日常作业程序库**。源代码模块的时间戳不能晚于对应的可执行模块。 **必须特别审查终端用户**所开发的应用 可能不遵循组织的安全规定、技术问题存在 BUG。

▲源代码比较 源代码比较是追踪源程序代码变化的有效易用的方法。手工检查源代码变更是合理的，但不完全有效。

4.2.9 版本管理 软件版本管理是软件因用户的要求的变化而持续满足用户要求的软件变更过程的管理。一系列经授权的变更

4.2.10 质量保证 QA 质量保证人员验证系统变更进入发行前的授权、测试和实施是**受控的**。在库管软件的帮助下，他们也检查程序版本和源代码到目标代码的**完整性**。

4.2.11 信息安全管理 所有的 IT 运营过程中都要重视信息安全程序。内容：对信息资产实施**风险评估**、实施业务**影响分析**、经常进行安全评估、实施正式的漏洞管理

4.3 信息系统硬件

4.3.1 计算机硬件组成与结构 P14

▲处理部件 中央处理单元又由算术逻辑单元(ALU)、控制单元和内部存储器组成。

▲分类 大型机.具有基于内置硬件控制的系统隔离环境 **无盘工作站**是一种特殊的不含硬盘的微机，可连接网络并利用网络存储进行工作。

多任务(Multitasking) 多处理(Multiprocessing)共享相同内存的多个处理器同时执行程序
多用户(Multiusing>又称为分时共享 多线程(Multithreading) 优化处理器的运行，减少处理器的空闲时间

瘦客户机实施方案中尤其有用。将**应用和许可归并到服务器**中有利于集中管理并且更安全
专用设备

防火墙实施的效果取决于安全策略的质量，以及与最佳实务的符合性；

入侵检测系统(IDS)—监听所有的出入信息，以推断出**潜在的恶意连接**并报警；

交换机—是一种工作在**数据链路层**的设备，用于隔离和互连网段并有助于减小以太类网络的碰撞域。

路由器—用于连接两个或更多个**物理隔离**的网段。经路由器联接的各个网段可以保持逻辑隔

离并作为独立网段使用。

▲USB 设备 存储棒也带来了十分严重的安全问题,即任一拥有该设备的人均可以拷贝数兆字节的数据而不留下任何踪迹,期间**不需要任何登录过程来验证数据权限**,也无须任何许可即可装载第三方的驱动程序。某些**可引导的 USB 设备**则可以绕过安全检查并使系统彻底暴露。

无线射频识别(RFID)使用无线电波识别有限半径范围内的标记的目标。最大的问题 安全 数据泄露

4.3.2 硬件维护程序

确定已形成**正式的维护计划**并得到**管理层**的批准。IS 管理层应监视、标识和记录所有与供应商维护规格的偏离,并提出相应的理由。

4.3.4 能力管理 capacity management

能力计划应包括被以往经验所证实的预测,并同时考虑现有业务的潜在增长和未来业务的扩展。以**确保可用资源的有效利用和充分利用**。

能力管理的一个主要问题是把组织的应用系统分布到多个小的服务器上,还是**统一地安装到很少的大型服务器**上。对于后者来说,可以使得组织**更好的使用资源**,但是,从另一个角度看,一旦服务器维护或故障停机,会影响很多应用系统。

4.4 信息系统体系结构和软件 architecture and software 基础架构和软件 P20 eP27

计算机硬件 原语级功能 系统软件

4.4.1 操作系统

▲软件控制特征或参数

参数选择应适应组织的工作负载和控制环境结构。判断一个**操作系统的控制运行状况**的最有效的手段是检查其**软件控制特征和/或参数**。

▲运行模式 超级用户态(高风险的行为,必须受到严格控制。有时候一般户可能需要提升权限至超级用户) 一般用户态

IS 管理层负责实施适当的授权技术以避免**非授权用户获得执行权限**,进而控制整个机器。**审计和控制专业人员应检查系统控制选项及保存在系统目录中的参数**。

▲活动日志和报告选项 **保护日志要维护证据的可验证性**,日志应可以被法律和法庭采用。

4.4.2 访问控制软件

访问控制软件用于防止对数据的非授权访问、对系统功能和程序的非授权使用,以及对数据的非授权修改/变动,并预防对计算机资源的非授权的访问企图。

4.4.3 数据通讯软件用于将消息或数据从某点传送到另一点。数据通讯系统仅关心两个节点间**数据的正确传输**,而与传输信息的内容无关。所有的数据通讯系统至少有一个物理层和一个数据链层。

4.4.4 数据管理包括控制缓冲区、执行 I/O.和文件管理等操作,它是一类系统管理软件。

直接随机存取—可根据**非数据**相关的关键字(如记录编号)对记录进行单独的寻址。

4.4.5 数据库管理系统(DBMS) 主要功能包括**减少数据冗余**、**缩短访问时间**和建立对敏感数据的**基本安全措施**(记录、字段和事务级)..**DBMS** 包含一个**数据字典**来描述其数据元素(字段)、元素的特征及用途。**DBMS** 能够在以下级别上控制用户对数据的访问:..用户和数据库 . 程序和数据库 .交易和数据库 .程序和数据库 .**用户和交易** .用户和数据字段。可实现终端用户对**数据的特例(Ad Hoc)访问**,尤其是可通过设定的**查询语言/应用生成器**

▲ 定义一个数据库所需的数据元素称为**元数据(Metadata)**,这包括那些定义逻辑和物理字段、数据关系、查询等元素所需的数据。 **数据定义语言(DDL)** 提供外部和内部模式之间的映射,使得外部模式和内部模式是位置无关的..**数据字典(DD)**和**目录系统(DS)**用于存储外

部模式、概念模式和内部模式及相关映射的数据定义

▲常用的数据库模型:层次、网状和关系 P27 eP35 层次数据库模型会导致数据的冗余 网状只能适用于数据之间的依赖关系清晰且稳定的环境。层次和网状模型均不支持高级查询,用户程序必须通过操纵数据结构来获得数据。指针 关系数据库的一个关键特征是利用规范规则实现以最少的表数据来满足用户对数据库的结构化或非结构化查询。

▲数据库控制

4.4.6 磁带和磁盘管理系统

4.4.7 实用程序(系统工具) utility programs 许多实用程序可旁路安全控制系统,或不产生任何审计记录,因此对这些功能强大而敏感的应用程序的使用应进行严格的控制和限制。

4.5 信息系统网络基础设施

专用分组交换机(PBX) 电话总机

传输信号的方法可分为基带(Baseband)传输和宽频传输(Broadband)一在有效频带内划分不同的载波频率,每个频率均可以运载模拟信号就如同是一条单独的基带通道。

4.5.1 企业网络体系结构

4.5.2 网络类型 广域网(WAN)一地理上分散的网络,为局域网或其他网络段提供互连服务。存储区域网(storageareanetworks,SANs)是局域网的一种变种,专门用于高速连接存储设备和服务器(或其他计算设备)的网络。SANS 集中处理数据的存储和管理。

4.5.3 网络服务 目录服务 存储网络中各种资源的信息,并帮助网络设备定位这些资源。

4.5.4 网络标准和协议

ISO/OSI 参考模型 P32 eP40

ISO/OSI 参考模型的七个层次分别是:应用层、表示层、会话层、传输层、网络层、数据链路层和物理层。每一层的功能描述如下:

应用层一应用层提供一组应用程序与网络进行通讯的设施(如保存文件到网络、在网络打印机上打印文件、接收来自网络的数据),作为应用与网络间的接口。此外,它也将计算机的可用资源通告给网络中的其他设备。应用层不同于应用软件,也不应将其与应用软件相混淆。

表示层一表示层执行数据转换,以提供标准的应用接口和公共的沟通服务,如加密、文本压缩和重构(如将 EBCDIC 码转换成 ASCII 工码)等。这一层提供信息的表示,如格式、编码、转换和加密。表示层的作用是保证应用层所提交数据的格式符合可用的网络标准,如果不符合,则在移交给会话层之前将其转换为正确的格式。相反的,当表示层收到来自网络的数据时,它也评估该数据的格式是否符合应用层的要求,并在必要时进行转换。

会话层一会话层控制计算机之间的对话(会话)。它建立会话,引导数据的传送,并存数据传送完毕时终止会话。会话层制定检查点、终止和重启程序。

传输层一传输层提供两个端点间的可靠和透明的数据传输、端一端错误检测和流量控制(窗口控制)。其中流量控制的目标是将网络拥塞降至最低。传输层的职责包括:将一个消息分解为若干个称为数据包或数据分片的数据块;为数据包分配地址;运送数据包通过网络;回应数据包并将其重新组装成原始的消息。传输层的一个重要功能是分片排序,当传输层收到的数据分片已经不同于其发送次序时,可以对数据分片进行重排序。

网络层一网络层负责数据包在网络中的寻址和递送。这是通过像路由器这样的硬件设备来完成的,其依据是分配给每个网络的逻辑地址以及目标设备的服务地址。一个网络的地址不同于可能与之相连的任何网络的地址。网络层还提供网络管理(.路由、交换和流量监控)

数据链路层一数据链路层提供数据在物理链路路上的可靠传输。数据链路层上传输的是称为帧的数据块,帧中包含用于同步、位错检测/纠正控制和流控所需的数据域。数据链路层的一个独特的特征是通过介质访问控制(MAC)地址来进行物理寻址,以实现物理上连接在相同网络中的设

备之间的通讯。网络中的每个设备都有唯一的 MAC “硬件” 地址 **向前错误控制(Forward Error Control)** (确认错误已经发生, 而且能确定错误的位置甚至纠正该错误): **奇偶校验**; **块总计校验** (奇偶位组)、而**奇偶效验私!块总计效验均不能有效地检测出帧错误**; **循环冗余校验(CRC)** **反馈错误控制(Feedback <backward> Error Control)**只能确认错误但不能纠正错误 **前向差错控制**包含了传输每个字符或数据帧的额外冗余信息来检测或纠正(传输)错误。在**反馈差错控制**中仅仅传输足够使得接收者检测到差错发生的额外信息。**物理层** 该层负责所有建立、维护、操作和解除物理链路所需的二进制信息的发送和接受。只涉及与**物理介质**的机械、电子或过程的接口, 而**不考虑数据**的结构。**在链路层 头信息是最多的** 到达应用层协议控制信息都除去了。

4.5.6 osi 模型在网络体系结构中的应用

▲局域网 LAN 局域网工作在 os r 参考模型的物理层和数据链路层。

包到达所有目标前必须经过的路径又称为“碰撞域” 当因碰撞而导致网络效率下降时, 就需要给网络分段。

采用这种方法的设备对网络的访问是基于一种特殊的、环绕网络传递的帧, 称为**令牌**。网络设备除非持有令牌, 否则不会发送数据。令牌介质访问方法通常用于环型网络拓扑并称为令牌环。

▲LAN 网络拓扑是网络的逻辑结构, 常用的结构有:

总线型 BUS—所有设备(节点)连接到同一条通讯线路上, 传输信号可以被网络中的所有节点所接收。当流量增大到一定程度时网络性能可能大幅度下降。一个节点损坏整个网络瘫痪

环型 Ring—用于环型或 FDDI 网络。其所有站点(节)连接到 MSAU(多站点访问单元), 从而在物理上构成星型拓扑, 当这些 MSAU 连接到一起时就构成了环型配置。

星型 STAR—每个站点(节或线路交换来实现连接点)均连接到一个 HUB 或交换机, 由 HUB 或交换机通过消息。如果没有配置故障冗余设备, 则**中心 HUB 或交换机的故障**将导致网络瘫痪。

▲LAN 组件 network component ★★★★★

中继器 是一种物理层设备, 用来扩展网络的范围或将两个分离的网络连接在一起。中继器从一个网段接收信号并加以放大(再生)以补偿信号在传输过程中的衰减。

网桥是一种数据链路层设备, 用于连接 LANs, 或将**单个网段分隔成两个独立的 LAN 或 WAN 网段**以缩小碰撞域。分隔后的两个网段在 OSI 参考模型的数据链路层之下是两个不同的网络。但在数据链路层及更高层中则是一个逻辑网段, **能存储帧并作为存储转发设备**。

路由器 从连接两个物理隔离的网段上来说类似于网桥和交换机, 但经路由器连接的网段之间在逻辑上仍然是隔离的, 可以用作独立的网络。**路由器工作在 OSI 模型的网络层, 它通过检查网络地址(即 IP 包中包含的路由信息)来将数据包定向至其目的地址**。与链路层交换机不同, 路由器利用了网络的逻辑地址, 为其每个端口分配不同的网络地址/网段, 阻塞广播信息, 阻塞目的地址未知的流量, 并根据网络或主机信息来过滤流量。路由器是基于软件的, 而且需要检查经过的每一个数据包, 其效率不如交换机, 并有可能成为网络的瓶颈。因此, 在网络设计时需谨慎考虑路由器在网络中的位置, 应充分发挥交换机的作用, 并在各路由器之间建立负载平衡机制以获得最大的性能。

虚拟局域网(VLAN) 基于逻辑而不是物理的连接 设备实际处于不同的 LAN

网关 是用于协议转换的设备

交换机 是一种数据链路层设备, 能够分隔和互连多个网段以缩小以太网络的碰撞域。是一种数据链路层设备, 能够分隔和互连多个网段以缩小以太网络的碰撞域。此外, **交换机还基于第二层的源和目的 MAC 地址来存储转发数据帧**, 这和网桥和 HUB 所做的 T 作相同。但交

交换机通过利用专用集成电路(ASIC)实现的更为复杂的数据链层协议,可以提供比网桥更强健的功能性。这项技术使得交换机具有低成本、低延迟、高速度和端口数多等优势。

与TCP/IP协议套件相对应的标准			
ISO模型	参考	TCP/IP概念层	协议
7	应用层	应用层	文件传输协议 (FTP)
6	表现层		远程终端控制协议 (TELNET)
5	会话层		简单邮件传输协议 (SMTP) 命名服务协议 (NSP) 简单网络管理协议 (SNMP)
4	传输层	传输层	传输控制协议 (TCP) 用户数据报协议 (UDP)
3	网络层	网络接口	互联网协议 (IP)
2	数据链路层	LAN或WAN接口	以太网、令牌环网
1	物理层		点对点协议 (PPP)

▲广域网 WAN P42

信道服务单元/数据服务单元(CSU/DSU)——工作在 OSI 参考模型的物理层,是**数字终端设备(DTE)到数据通讯设备(DCE)的接口**,用于交换式通信公司网络中。

帧中继是一种用于交换设备的数据链层协议,它采用标准的包封装技术来控制互连设备间的多条虚电路。其封装方法是用于同步数据链路的高级数据链控制(HDLC)协议。

虚拟专用网(VPN) 在互联网中建立虚拟连接,并采用**加密数据包(对原始数据进行加密和打包封装)**进行传输 **隧道加密模式**将整个数据包,包括报头都进行了加密,而**传输加密模式**则仅对包的数据部分进行了加密。最关注的是 **所有的接入机器都有最高安全等级的防护** 雇员或第三方家中的机器是检查重点。

▲无线网 ★★ IEEE 802.11 的**有线等效加密(WEP)采用了对称密钥**。这意味着末端用户的无线网卡(NIC)和访问点必须**拥有相同的密钥**,并陷入了必须定期为每块 NIC 更换密钥的困境。无线网卡(NIC) 如 **802.11i 和 WPA (Wi-Fi 保护访问协议)**,采用了**公开密钥密码学技术**来完成用户和访问点之间的**有效认证和加密**。

转换点——信息从无线网络转入有线网络的站点。•在这一点上,采用无线传输层安全的 WAP 安全模式所保护的信息需要被转换为由安全插座层来保护,此时信息首先需要解密然后再重新加密并在 TCP/IP 网络上传输。

▲互联网

跨界数据流动 法律保护 因为信息的传输路线是由路由器决定而不是固定的

▲网络管理和控制 可用于**监视和修改网络的软件应限制为只有网络管理员才能使用**。

反应时间(Latency)和**吞吐量(Throughput)**是度量网络性能的关键参数。

▲网络管理工具

简单网络管理协议(SNMP)——一种基于 TCP/IP 的网络管理协议,用来监视和控制网络中的各种变量、管理配置和采集性能/安全相关的统计信息。当有重要事件发生时 SNMP 的代理会产生一个**陷阱消息 trap message** 网络管理员使用 SNMP 管理网络性能,发现和解决网络故障,并计划网络增长。一个 SNMP 管理的网络包含三个主要部分:被管理设备、代理和网络管理系统(NMSs) managed devices, agents, and network-management systems (NMSs)。被管理设备使用陷阱命令向网络管理系统 asynchronously 报告事件。当一定类型的事件发生,被

管理设备向网络管理系统发送一个陷阱。其实就是一个符合条件的 *flag* 消息。

<http://blog.csdn.net/cnhairong/archive/2004/07/15/41841.aspx>

▲基于网络的应用系统:

三层体系结构由以下构件组成: 一个瘦客户机 一组(一个或多个)应用服务器, 主要运行应用逻辑 一组(一个或多个)数据库服务器。程序逻辑与其他代码分离; 从二层到三层意味着中间件的出现。

▲中间件

风险—中间件的目标是支持多个操作环境的并发交互, 导致数据或程序完整性的丧失。

4.6 系统和运行的审计 P57 eP65

▲操作系统

利用数据库管理系统使数据冗余度最小, 凡存在数据冗余的地方均已在数据字典或其他文档中进行了适当的交叉引用。

▲数据库

审计数据库时, IS 审计师应审核其设计、访问、管理、接口和可移植性。

关系-实体模型应和数据库的物理模式一致。所有用户的安全级别和角色应在数据库中加以标识、可移植性 应尽量使用结构化查询语言(SQL)

▲网络

必须了解如下内容 在开始检查:

网络拓扑和网络设计

重要的网络组件(如服务器和交换机)

网络的互连

▲运行审核 审计程序应包括对履行各自职责的 IS 人员的观察, 以确定是否有适当的控制来保证运行效率、对现有标准和政策的遵守、充分的监督、IS 管理层审查、以及数据完整性和安全。

无人值守设备对主控台的远程访问通常授权给可信赖的操作员用于处置紧急情况, 所以, 危险而又高能的控制台命令就暴露在通讯线路上。必须对通讯访问进行广泛的安全控制, 包括采用专用线路和回拨功能。