

金牌网管师（中级）



[金牌网管师（中级）_下载链接1](#)

著者:

出版者:

出版时间:2010-4

装帧:

isbn:9787508471648

《金牌网管师(中级)网络工程方案规划与设计》是“全国网管技能水平考试”(NMSE,“网管师”认证)中级考试和认证中，面向专业、综合的网络系统设计的指定教材。全

书共三篇，16章，前两篇(共14章)侧重于介绍企业网络中通信子系统、网络安全子系统的规划与设计，最后一篇介绍了在大型企业网络中才可能需要的网络存储子系统设计的基础知识。在通信子系统和安全子系统的规划与设计中，从最初的用户需求调查、拓扑结构设计等，一直到综合的网络系统方案设计与配置都进行了较为详细的介绍。

《金牌网管师(中级)网络工程方案规划与设计》是目前国内IT图书市场中唯一一本全面、系统、深入地介绍3个主要网络子系统规划与设计的图书，不仅可作为网络工程设计人员的自学教材，还是高校网络系统设计专业的最佳教材选择。

作者介绍：

目录: 第1章 网络工程设计综述 1

1.1 网络工程设计基础 2
1.1.1 网络系统集成概述 2
1.1.2 网络工程设计综述 3
1.2 网络工程设计的考虑 4
1.2.1 网络通信标准和协议的选择考虑 4
1.2.2 网络规模和网络拓扑结构考虑 5
1.2.3 网络功能和应用需求考虑 7
1.2.4 可扩展性和可升级性考虑 7
1.2.5 其他方面的考虑 8
1.3 网络工程集成设计的步骤和原则 10
1.3.1 网络工程集成设计的一般步骤 10
1.3.2 网络工程集成设计的基本原则 13
1.3.3 局域网系统设计的主要内容 16
1.3.4 广域网系统设计的主要内容 18

第2章 用户需求调查与分析 19

2.1 用户调查内容 20
2.1.1 一般企业状况调查 20
2.1.2 应用需求调查 22
2.1.3 功能需求调查 23
2.1.4 性能需求调查 25
2.1.5 管理需求调查 28
2.2 用户性能需求分析 29
2.2.1 接入速率需求分析 29
2.2.2 吞吐性能需求分析 32
2.2.3 可用性能需求分析 34
2.2.4 并发用户数需求分析 36
2.2.5 可扩展性需求分析 37

第一篇 网络通信子系统设计篇 41

第3章 网络拓扑结构规划与设计 42
3.1 网络拓扑结构 43
3.1.1 局域网拓扑结构 43
3.1.2 广域网拓扑结构 43
3.2 网络拓扑结构绘制 46
3.2.1 简单网络拓扑结构图元的获取 47
3.2.2 拓扑结构绘制 49
3.3 网络拓扑结构设计 57
3.3.1 小型星型网络结构设计示例 57
3.3.2 中型扩展星型网络结构设计示例 59
3.3.3 大型混合型网络结构设计示例 62
3.3.4 园区网络结构设计示例 65

3.3.5 无线局域网结构设计示例	69
3.4 广域网网络拓扑结构设计	70
3.4.1 小型企业互联网接入拓扑结构设计	71
3.4.2 X.25广域网接入拓扑结构设计	72
3.4.3 FR广域网接入拓扑结构设计	74
3.4.4 ATM广域网接入拓扑结构设计	76
3.4.5 光纤接入广域网拓扑结构设计	78
第4章 综合布线系统规划与设计	82
4.1 综合布线系统概述	83
4.1.1 综合布线系统的由来	83
4.1.2 综合布线系统的组成	83
4.1.3 综合布线系统的特点	85
4.2 综合布线标准	86
4.2.1 综合布线标准的发展历程	86
4.2.2 我国等效采用的综合布线标准	87
4.3 综合布线系统中的传输介质标准	88
4.3.1 双绞线综合布线标准	88
4.3.2 绞线布线标准中的参数测试规范	90
4.3.3 光缆布线装置	93
4.3.4 光缆布线标准	97
4.4 综合布线系统设计	99
4.4.1 综合布线系统设计的基本步骤	99
4.4.2 3个综合布线系统设计等级	99
4.4.3 综合布线系统的设计要领	101
4.5 综合布线系统设计要点	102
4.5.1 工作区子系统设计要点	102
4.5.2 水平子系统设计要点	103
4.5.3 垂直干线子系统设计要点	104
4.5.4 设备间子系统设计要点	106
4.5.5 管理子系统设计要点	107
4.5.6 建筑群子系统设计考虑	109
第5章 网络设备的选型	111
5.1 网卡的选型	112
5.1.1 有线以太网卡的选型	112
5.1.2 无线局域网网卡的选型	117
5.1.3 网卡的综合选型考虑	118
5.2 服务器的选型	120
5.2.1 服务器处理器架构的选型	120
5.2.2 服务器的综合选型考虑	122
5.3 交换机和无线AP的选型	124
5.3.1 交换机的综合选型考虑	124
5.3.2 无线AP的综合选型考虑	129
5.4 路由器的选型	130
5.4.1 边界和中间节点路由器的选型	131
5.4.2 宽带路由器的选型	132
5.4.3 企业级路由器的综合选型考虑	134
5.5 防火墙的选型	136
5.5.1 防火墙的选型	137
5.5.2 防火墙的综合选型考虑	138
5.6 UPS的选型与选购	142
5.6.1 UPS的主要作用和分类	142
5.6.2 主要UPS技术	143
5.6.3 UPS的综合选型考虑	145
第6章 网络体系架构规划与设计	147

6.1 两种网络架构模型	148
6.1.1 P2P网络架构模型	149
6.1.2 C/S网络架构模型	150
6.2 P2P工作组局域网架构设计考虑	151
6.3 域网络架构设计的基本考虑	153
6.3.1 域网络操作系统选择的考虑	154
6.3.2 林和域的规划基础	156
6.3.3 新建林、子域和域树的考虑	157
6.3.4 域命名空间规划考虑	159
6.3.5 域和林信任关系的设计考虑	163
6.3.6 多域环境下的访问控制策略规划与设计	166
6.3.7 域控制器和成员服务器的规划与设计	170
6.3.8 DNS服务器的规划考虑	172
6.3.9 DHCP服务器的规划考虑	174
第7章 企业网络通信子系统结构方案	180
7.1 小型SOHO办公室网络系统结构方案	181
7.1.1 小型SOHO办公室网络方案的特点与要求	181
7.1.2 Cisco小型SOHO办公室有线局域网方案	182
7.1.3 H3C小型SOHO办公室有线局域网方案	185
7.1.4 小型SOHO办公室的WLAN方案	189
7.1.5 小型SOHO办公室局域网的互联网连接	192
7.2 中小型企业网络系统结构方案	193
7.2.1 中小型企业局域网方案的特点与要求	193
7.2.2 Cisco中小型企业有线局域网方案	194
7.2.3 H3C中小型企业有线局域网方案	200
7.2.4 Cisco 1800的中小型企广域网连接方案	204
7.3 中型企业网络系统结构方案	210
7.3.1 中型企业网络方案的主要特点与要求	210
7.3.2 Cisco中型企业局域网方案	211
7.3.3 H3C中型局域网方案	215
7.3.4 Cisco中型企业网络的广域网连接方案	218
7.3.5 H3C中型企业网络的广域网连接方案	222
7.4 大中型企业网络结构方案	226
7.4.1 大中型网络方案的特点与要求	226
7.4.2 Cisco大中型局域网方案	227
7.4.3 H3C大中型局域网方案	232
7.4.4 Cisco大中型网络广域网连接方案	237
第二篇 网络安全子系统规划与设计	241
第8章 网络安全系统设计综述	242
8.1 网络安全系统设计基础	243
8.1.1 网络安全系统的发展	243
8.1.2 网络安全威胁综述	244
8.1.3 企业网络的主要安全隐患	246
8.1.4 常用网络安全防护策略	247
8.1.5 网络安全系统设计基本原则	248
8.2 OSI/RM各层的安全保护概述	250
8.2.1 物理层的安全保护	251
8.2.2 数据链路层的安全保护	252
8.2.3 网络层的安全保护	253
8.2.4 传输层的安全保护	254
8.2.5 会话层和表示层的安全保护	255
8.2.6 应用层的安全保护	255
8.3 网络安全系统设计的基本思路	255
8.3.1 安全隐患分析和基本系统结构信息的收集	256

8.3.2 调查和分析当前网络的安全需求	259
8.3.3 现有网络安全策略评估	259
8.3.4 设计细化的新网络安全策略初稿	260
8.3.5 方案的测试、评估和修改	265
8.3.6 方案定稿和应用	266
第9章 物理层安全方案	267
9.1 物理层的线路窃听技术分析	268
9.2 计算机网络通信线路屏蔽	269
9.2.1 选择屏蔽性能好的传输介质和适配器	269
9.2.2 屏蔽机房和机柜的选择	272
9.2.3 WLAN无线网络的物理层安全保护	273
9.3 物理线路隔离	273
9.3.1 主要的物理隔离产品	273
9.3.2 物理隔离网闸隔离的原理	276
9.4 设备和线路冗余	279
9.4.1 网络设备部件冗余	279
9.4.2 网络设备整机冗余	281
9.4.3 网络线路冗余	282
9.5 机房和账户安全管理	283
9.5.1 机房安全管理	283
9.5.2 账户安全管理	284
9.6 物理层安全管理工具	284
9.6.1 泛达综合布线实时管理系统	284
9.6.2 Molex综合布线实时管理系统	287
第10章 数据链路层安全方案及应用配置	289
10.1 典型的数据加密算法	290
10.1.1 基于“消息摘要”的算法	290
10.1.2 “对称/非对称密钥”加密算法	292
10.2 数据加密	294
10.2.1 数据加密技术	294
10.2.2 链路加密机	297
10.2.3 网卡集成式链路加密原理	299
10.3 WLAN数据链路层保护方案	301
10.3.1 WLANSSID安全技术及配置方法	301
10.3.2 WLANMAC地址过滤及配置	303
10.3.3 WLANWEP加密	304
10.3.4 WLANWPA/WPA2加密认证	306
10.4 无线AP/路由器的WPA和WPA2设置	309
10.4.1 个人用户无线AP/路由器的WPA.PSK或WPA2.PSK设置	309
10.4.2 企业级无线AP/路由器的WPA或WPA2设置	310
10.4.3 WLAN客户端第三方软件的WPA和WPA2设置	311
10.4.4 Windows XP无线客户端WPA/WPA2配置	314
10.5 MAC地址欺骗防护	316
10.5.1 ARP和RAP&协议工作原理	316
10.5.2 MAC地址欺骗原理	317
10.5.3 MAC地址欺骗源的查找和预防	318
10.6 Cisco设备基于端口的MAC地址绑定	320
10.6.1 基于端口的单一MAC地址绑定的基本配置步骤	321
10.6.2 基于端口的单一MAC地址绑定配置示例	322
10.6.3 基于端口的多MAC地址绑定配置思路	322
10.7 Ciseo设备基于IP地址的MAC地址绑定	323
10.7.1 一对一的MAC地址与IP地址绑定	323
10.7.2 一对多或者多对多的MAC地址与IP地址绑定示例	324
第11章 网络层Kerberos和IPSec安全方案及应用配置	325

11.1 身份认证概述	326
11.1.1 主要的身份认证方式	326
11.1.2 单点登录身份认证执行方式	327
11.2 Kerberos身份认证	328
11.2.1 Kerberosv5身份认证机制	328
11.2.2 Kerberosv5身份认证的优点与缺点	331
11.3 Kerberos应用原理与配置示例	332
11.3.1 利用kerberos进行本地登录的原理	332
11.3.2 利用Kerberos进行域登录的原理和示例	333
11.3.3.Kerberosv5身份认证的策略配置	337
11.4 IPSec协议	338
11.4.1 IPSec的两种使用模式	339
11.4.2 IPSec的AH协议	340
11.4.3 IPSec的ESP协议	343
11.5 IPSec协议应用方案设计与配置思路	346
11.5.1 IPSee策略规则	346
11.5.2 IPSee安全通信方案的主要应用	350
11.5.3 不推荐使用IPSec协议保护的应用方案	354
11.5.4 配置IPSec应用方案前的准备	355
11.5.5 配置IPSec安全应用方案的基本步骤	355
11.6 IPSec在Web服务器访问限制中的应用配置示例	356
11.6.1 创建两个筛选器操作	356
11.6.2 创建IP筛选器列表	359
11.6.3 创建和指派IPSec策略	363
11.7 IPSec的其他应用方案示例	367
11.7.1 IPSec在数据库服务器访问限制中的应用配置示例	367
11.7.2 IPSec在阻止NetBIOS攻击中的应用配置示例	367
11.7.3 IPSec在保护远程访问通信中的应用配置示例	369
第12章 网络层证书服务和PKI安全方案及应用配置	373
12.1 证书和证书服务基础	374
12.1.1 证书概述	374
12.1.2 证书的主要功能	375
12.1.3 证书的主要应用	376
12.2 Windows Server 2003系统PKI体系	380
12.2.1 WindowsServer2003系统PKI体系基础功能设施	380
12.2.2 WindowsServer2003系统PKI体系规划和部署的基本流程	381
12.3 定义证书需求	382
12.3.1 确定安全应用需求	382
12.3.2 确定证书需求	386
12.3.3 文档化证书策略和证书实施声明	387
12.3.4 定义证书应用需求步骤示例	388
12.4 证书颁发机构层次结构设计	389
12.4.1 规划核心CA选项	389
12.4.2 选择信任模式	398
12.4.3 CA层次结构设计中的其他步骤	401
12.4.4 CA层次结构设计示例	402
12.5 扩展证书颁发机构结构	403
12.5.1 评估影响扩展信任的因素	404
12.5.2 选择扩展CA结构配置	406
12.5.3 限制计划外的信任	408
12.6 定义证书配置文件	409
12.6.1 选择证书模板	410
12.6.2 选择证书安全选项	410
12.6.3 使用合格的从属来限制证书	413

12.6.4 配置证书示例	417
12.7 创建证书管理规划	418
12.7.1 选择注册和续订方法	418
12.7.2 将证书映射到用户账户	419
12.7.3 创建证书吊销策略	423
12.7.4 密钥和数据恢复	426
12.7.5 创建证书管理规划示例	427
第13章 传输层安全方案及应用配置	428
13.1 TLS/SSL基础	429
13.1.1 TLS/SSL简介	429
13.1.2 TLS与SSL的区别	430
13.1.3 常见的TLS/SSL应用	430
13.2 Windows Server 2003 TLS/SSL体系架构	432
13.2.1 安全通道SSPI体系架构	432
13.2.2 TLS/SSL体系架构	433
13.3 TLS/SSL在IISWeb服务器中的应用	434
13.3.1 安装CA	435
13.3.2 生成证书申请	436
13.3.3 提交证书申请	438
13.3.4 证书的颁发和导出	441
13.3.5 在Web服务器上安装证书	444
13.3.6 在Web服务器上启用SSL	445
13.4 WLAN网络中的传输层安全协议 WTLS	446
13.4.1 WAP的主要特点和体系架构	447
13.4.2 WAP架构与WWW架构的比较	450
13.4.3 WAP 安全机制	451
13.4.4 WTLS 体系架构	453
13.4.5 WTLS的安全功能	454
13.4.6 WTLS 与 TLS 的区别	455
13.5 SSH 和 SOCKS 协议	456
13.5.1 SSH 协议	456
13.5.2 SOCKS 协议	458
第14章 Web服务器安全系统设计与配置	460
14.1 Web服务器的安全威胁与对策分析	461
14.1.1 主机枚举攻击及防御策略	461
14.1.2 拒绝服务攻击及防御策略	464
14.1.3 其他攻击及预防策略	466
14.2 安全Web服务器检查表	467
14.2.1 程序修补和更新	467
14.2.2 安装IISLockdown	469
14.2.3 禁用不需要的服务	469
14.2.4 禁用不需要的协议	474
14.2.5 禁用或正确使用账户	474
14.2.6 正确配置文件和目录访问权限	476
14.2.7 删除不必要的共享和正确使用共享	477
14.2.8 限制端口	478
14.2.9 正确配置注册表	479
14.2.10 正确配置和使用审核与日志记录	479
14.2.11 正确配置站点和虚拟目录	481
14.2.12 正确配置脚本映射和ISAPI过滤器	482
14.2.13 正确配置IIS元数据库和服务器证书	483
14.2.14 代码访问安全性	484
14.2.15 HS Web服务器的整体安全检查表	485
第三篇 网络存储子系统设计篇	487

第15章 网络存储基础	488
15.1 3种主流的数据存储方式	489
15.1.1 DAS数据存储方式	489
15.1.2 NAS数据存储方式	490
15.1.3 SAN数据存储方式	491
15.2 SCSI接口	493
15.2.1 SCSI接口简介	493
15.2.2 SCSI设备连接	494
15.3 SATA接口	496
15.3.1 SATA简介	496
15.3.2 SATA的技术特性	497
15.3.3 SATA II标准	499
15.3.4 eSATA 规范	501
15.4 SAS 接口	502
15.4.1 SAS 接口简介	503
15.4.2 SAS 接口结构	504
15.4.3 SAS接口的设备连接	505
15.5 磁盘阵列 (RAID)	507
15.5.1 主要RAID模式	508
15.5.2 主要RAID模式比较	514
第16章 SAN网络存储	516
16.1 SAN基础	517
16.1.1 SAN的基本特性	517
16.1.2 光纤通道 (FC) 基础	518
16.2 FC体系结构和标准	520
16.2.1 FC体系结构	520
16.2.2 FC 标准	521
16.3 FC的3种主要拓扑架构	522
16.3.1 点对点架构	522
16.3.2 光纤通道仲裁环架构	523
16.3.3 交换式架构	525
16.4 光纤通进设备	526
16.4.1 光纤通道端口类型	527
16.4.2 FC-SAN 的主要设备	527
16.4.3 光纤集线器和交换机	528
16.5 IP SAN 存储基础	530
16.5.1 IP存储概述	530
16.5.2 IP存储的优势和面临的挑战	531
16.6 iSCSI-SAN	532
16.6.1 iSCSI协议基础	533
16.6.2 iSCSI协议栈和数据包封装	534
16.6.3 iSCSI-SAN应用方案体系架构	535
16.6.4 iSCSI-SAN 的优缺点	537
16.7 FCIP-SAN	538
16.7.1 FCIP 协议基础	538
16.7.2 FCIP协议栈和数据封装	540
16.7.3 FCIP-SAN 存储	541
16.8 iFCP-SAN	542
16.8.1 iFCP 协议基础	542
16.8.2 iFCP-SAN 存储	543
16.9 3种主要IP存储协议的比较	544
16.10 FCoE 技术	546
16.10.1 FCoE 协议概述	546
16.10.2 FCoE-SAN 所带来的好处	547

· · · · · (收起)

[金牌网管师（中级）](#) [下载链接1](#)

标签

计算机

评论

虽然说里面有不少东西缺乏新意，和其他类似的书没有大区别，但是有点是里面也有很多比较贴合实际的内容，也饱含了作者的实际经验，在同类书籍中还算是比较好的。但是里面涉及的范围和内容实在是过分追求大和全，想要完全掌握也不容易

[金牌网管师（中级）](#) [下载链接1](#)

书评

[金牌网管师（中级）](#) [下载链接1](#)