

ICS 03.240

M 81

备案号：16261-2005

YZ

中华人民共和国邮政行业标准

YZ/T 0115-2005

代替 YD 5042-97

邮政金融计算机网络系统工程 设计规范（储蓄部分）

Code for design of postal finance computer
network system engineering (saving part)

田 万方数据
WANFANG DATA

2005-06-10 发布

2005-06-10 实施

国家邮政局 发布

中华人民共和国邮政行业标准

邮政金融计算机网络系统工程
设计规范（储蓄部分）

Code for design of postal finance computer
network system engineering (saving part)

YZ/T 0115-2005

主编单位：中讯邮电咨询设计院

批准部门：中华人民共和国国家邮政局

施行日期：2005年06月10日



目 次

前 言	II
1 总 则	1
2 系统功能	3
3 系统方案	4
3.1 系统网络结构	4
3.2 各级节点系统结构	5
3.3 系统通信	8
4 网络管理	11
5 安全保密	13
6 设备配置及技术要求	15
6.1 设备配置原则	15
6.2 设备配置	15
6.3 设备技术要求	20
7 机房及设备安装要求	25
7.1 机房场地要求	25
7.2 设备安装要求	26
附录 A (规范性附录) 本规范用词说明	27
条文说明	28

前 言

邮政金融计算机网络系统工程设计规范（储蓄部分）（以下简称本规范）是根据国家邮政局国邮〔2004〕271号文《关于下达国家邮政局2004年第一批新技术开发项目计划（邮政标准类）的通知》（本规范计划编号为B200422），在参阅了邮政储蓄网络的技术方案、全国中心和部分省市工程设计的基础上，总结了多年来邮政储蓄计算机网络的建设经验，结合目前技术进步情况编制的。本规范是对原邮电部于1997年9月发布的《邮政金融计算机网络系统工程设计暂行规定》（YD 5042-97）的修订。

本规范包括总则、系统功能、系统方案、网络管理、安全保密、设备配置及技术要求、机房及设备安装要求等。主要修改了以下内容：

1 章节内容进行重新编排，增强了规范的系统性和条理性。

2 邮政储蓄应用系统由核心业务处理子系统、会计子系统、清算子系统、信息管理子系统和事后监督子系统组成。

3 根据目前邮政金融计算机网（储蓄部分）建设状况和发展形势，修改了邮政计算机网的网络结构，建设省中心、取消城市中心。账户数据存放在省中心并且业务处理由省中心完成。

4 全国中心、省中心、地县汇接点的局域网重新进行设计，增加了安全保密部分的内容。

5 根据业务发展需求和技术进步情况，重新提出了各级中心的设备配置标准和技术要求。

6 根据应用系统的需求，提出广域通信带宽的计算方法。

本规范附录A为规范性附录。

本规范由国家邮政局计划财务部提出。

本规范由国家邮政局科学研究规划院归口。

本规范由中讯邮电咨询设计院负责起草。

本规范主要起草人：周可记 李晓彤 吴季真 马雪鹏

1 总 则

1.0.1 为了满足邮政金融计算机网络系统建设的需要，更好地规范邮政金融计算机网络系统（储蓄部分）（以下简称邮政储蓄网）的工程建设，特修订本规范。

1.0.2 本规范适用于邮政储蓄网的可行性研究及工程设计。

1.0.3 邮政储蓄网的建设目标是：以先进的计算机技术、网络及数据通信技术为手段，建立以省（自治区、直辖市）为处理中心（以下简称为省中心），具有安全、可靠、高效、规范的邮政金融业务处理系统，使邮政储蓄网成为邮政金融业务处理的承载平台，通过数据的集中存储和应用的集中处理，实现信息资源的综合利用和共享，提高系统的可维护性、可用性，从而进一步提高邮政管理服务水平，增强企业的竞争能力。

1.0.4 邮政储蓄网在各省中心集中存放本省分户账并完成本省邮政储蓄业务的集中处理；跨省的交易通过全国中心进行，跨行交易通过本省中心连接银行卡区域中心或全国中心进行。

1.0.5 邮政储蓄网应具有较强的可扩展性，以适应未来的扩展。

1.0.6 邮政储蓄网的建设要认真总结分析现有邮政储蓄网的安全体系，结合邮政储蓄网的长远目标和当前的实际情况，制定切实可行的安全技术方案。

1.0.7 在邮政储蓄网的建设中，网络结构、软件设计和数据库设计是以省数据集中的模式进行设计，但应考虑多省集中的模式，为数据大集中奠定基础。

1.0.8 设计应符合工程设计文件质量特性（即功能性、可信性、安全性、可实施性、适应性、经济性及时间性）的要求，并应按照切合实际、技术先进、经济合理、安全实用的原则，进行多方案比较。

1.0.9 邮政储蓄网工程硬件系统应选择具有先进性、成熟性、稳定性，并拥有优良性价比的设备。软件系统的选择与开发应在满足业

务需求的基础上具有易改造、易升级、易操作、易维护等特性。

1.0.10 当本规范无具体规定时，应执行国家标准及邮政行业有关标准、暂行规定。

1.0.11 在特殊情况下执行本规范中个别规定有困难时，设计应充分论述理由，呈主管部门审批后变更执行。

田 万方数据
WANFANG DATA

2 系统功能

2.0.1 邮政储蓄网主要由核心业务处理、会计核算、资金清算、事后监督和信息管理等子系统组成。各子系统功能如下：

1 核心业务处理。在省中心主要实现对储户账户的账务性、非账务性的处理，并通过客户号对账户实现客户化管理；在全国中心主要完成本系统跨主机的交易转发，纵联跨行交易的转发。

2 资金清算。实现各清算账户的资金清算、省清算账户和全国中心的资金清算，省中心与区域银行卡中心的资金清算。

3 会计核算。完成相关的会计处理，实现权限管理、参数设置、会计事项维护、会计科目维护、往来款项的监控管理、重要凭证的管理等功能。

4 事后监督。事后监督数据的维护，包括联网网点数据与非联网网点数据，实现对交易的监督，存放、处理事后监督资料，实现人员管理、参数化的管理。

5 信息管理。完成各种信息管理，可以对信息管理子系统中的汇总信息进行查阅、修改、编辑等操作，负责对下辖各级信息管理子系统进行权限设定。

田 万万数据
WANFANG DATA

3 系统方案

3.1 系统网络结构

3.1.1 邮政储蓄网包括省际网络和省内网络。

3.1.2 邮政储蓄省际网应采用邮政综合网广域网作为通信平台连接全国中心和省中心，是实现异地储蓄业务处理及事务管理的网络。邮政储蓄省际网的网络结构如图 3.1.2 所示。

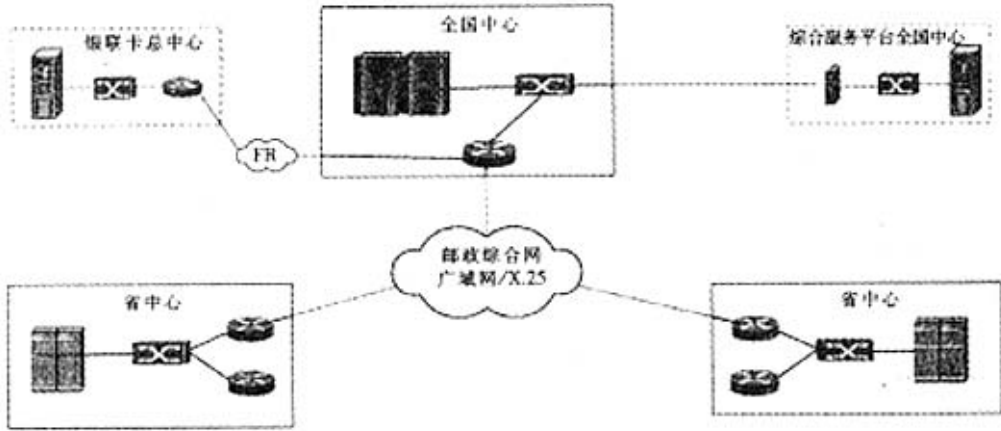


图 3.1.2 邮政储蓄省际网络结构示意图

3.1.3 邮政储蓄省内网是以省中心为核心，采用邮政综合网省内广域网或公用通信网连接地县汇接点，地县汇接点再连接营业网点，或省中心直接连接营业网点的集中式网络。邮政储蓄省内网的网络结构如图 3.1.3 所示。

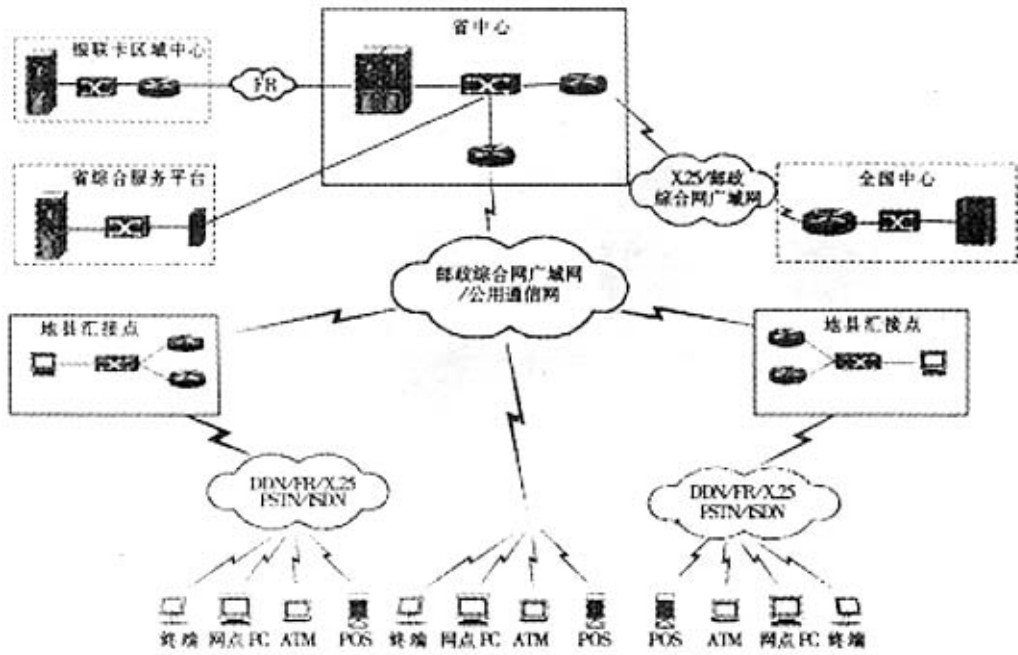


图 3.1.3 邮政储蓄省内网络结构示意图

3.2 各级节点系统结构

3.2.1 邮政储蓄网的节点包括全国中心、省中心、市（地、县、州）汇接点（以下简称市县汇接点）。

3.2.2 全国中心包含储蓄业务处理、会计、清算和信息管理等子系统。全国中心应用软件的业务、会计和清算等子系统在主机系统中运行。应用软件和数据库系统分别运行在两台主机上，两台主机互为备份。信息管理子系统运行在单独的 PC 服务器。全国中心存储系统采用存储区域网（SAN）结构，核心业务系统和信息管理系统共用 SAN 存储系统。全国中心网络结构如图 3.2.2 所示。

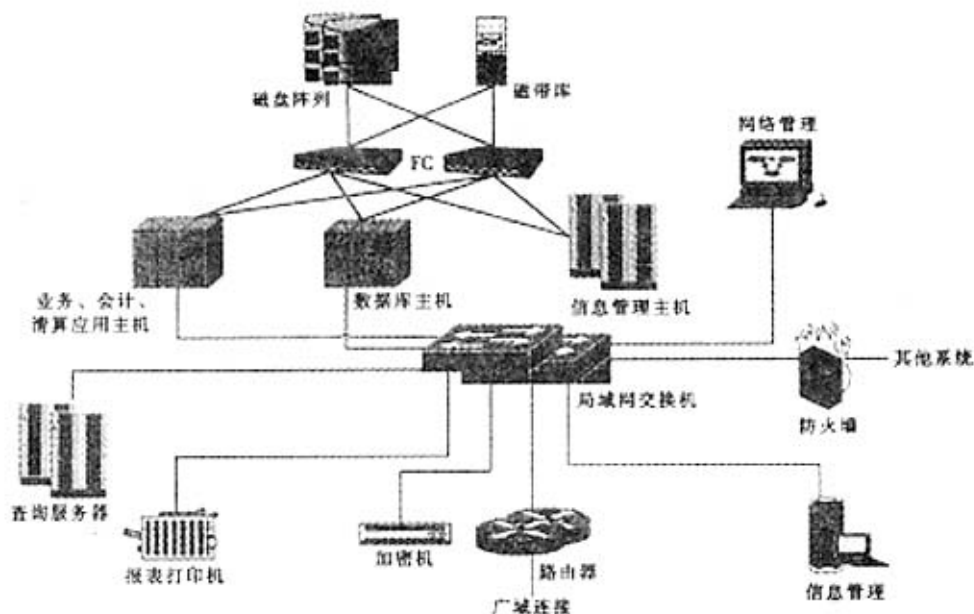


图 3.2.2 全国中心网络结构示意图

3.2.3 省中心包含业务处理、会计、清算、信息管理和事后监督等子系统。省中心应用软件的业务、会计、清算等子系统在主机系统中运行。应用软件和数据库系统分别运行在两台主机上，两台主机互为备份。信息管理子系统运行在单独的 PC 服务器上。事后监督子系统相对独立，运行在单独的 PC 服务器上。省中心存储系统采用 SAN 结构，核心业务系统、信息管理系统、事后监督系统、代理保险系统和电子汇兑系统共用 SAN 存储系统。省中心网络结构如图 3.2.3 所示。

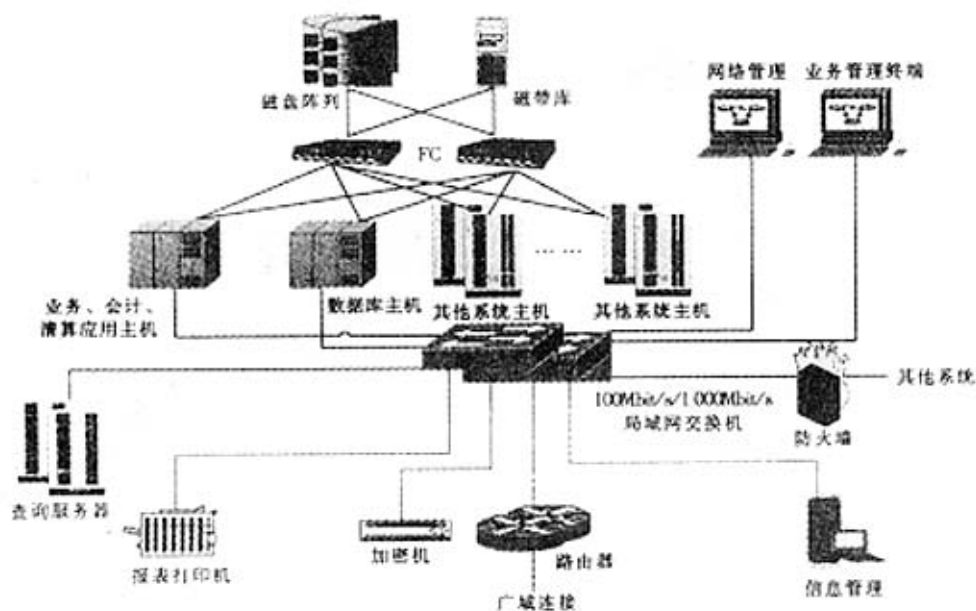


图 3.2.3 省中心网络结构示意图

3.2.4 市县汇接点配备信息管理、会计、清算、事后监督等客户端。客户端从省中心系统中得到本地需要的管理数据，并向省中心上传数据。网点服务器可放置在市县汇接点，每个网点服务器可连接多个营业网点。地县中心的信息管理、会计、清算、事后监督等客户端与省中心对应的服务器端联接，实现地市业务功能。地县会计客户端还负责接收和保存省中心信息管理子系统下发的报表等信息，便于随时查询。市县汇接点的系统结构如图 3.2.4 所示。

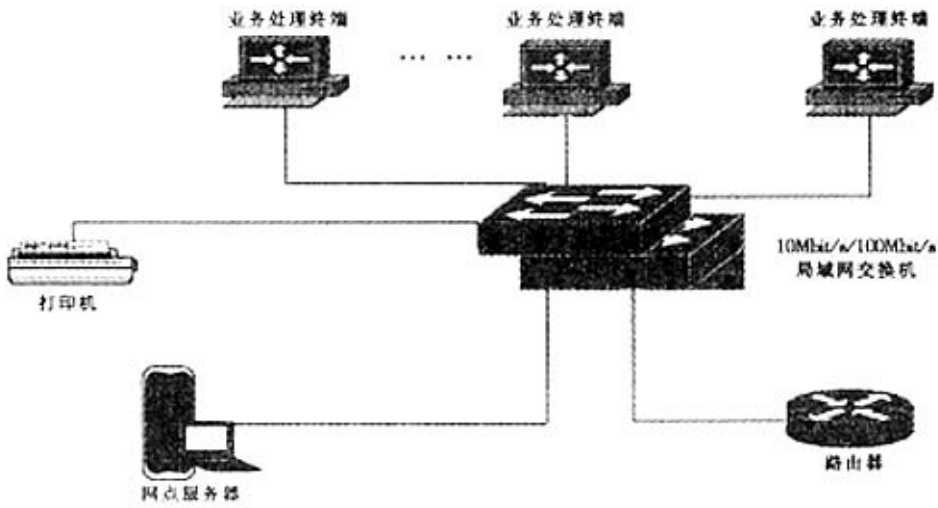


图 3.2.4 市县汇接点系统结构示意图

3.3 系统通信

3.3.1 邮政储蓄网应采用下列通信方式：

- 1 全国中心、省中心与市县汇接点连接时采用两条通信线路，两条线路互为备份。
- 2 省中心与营业网点、市县汇接点与营业网点间的连接方式可根据业务量和时限要求以及本地公用通信网的具体情况选取。
- 3 邮政储蓄全国中心、省中心与邮政其他业务系统及其他第三方的网络互联时采用对方要求的通信线路，同时应使用防火墙进行隔离。

3.3.2 网络通信协议应符合《中国邮政金融计算机网络通信协议 TCP/IP（暂行规定）》YDN 014-1996 的规定。

3.3.3 通信带宽测算应按下列方式确定：

- 1 邮政储蓄省中心系统包括省中心核心业务系统、事后监督系统和信息管理系统，在估算广域网带宽时，应分别对这 3 个系统所占的带宽进行估算。
- 2 根据各省核心业务的日均交易量可以测算核心业务所需的通信带宽。

省中心核心业务系统峰值时所占广域网流量按下式计算：

$$W_p = 8 \times (1 + q_1) \times L_1 \times \left[\frac{0.8 \times M_1}{3600 \times t_1} \right] \quad (3.3.3-1)$$

式中：

方括号内代表峰值期间内的每秒交易量；

W_p ——省中心业务系统峰值时所占广域网流量，单位为 bit/s；

q_1 ——冗余系数，对于网络带宽而言，通常取 50%，即允许网络内增加 50% 的突发流量；

L_1 ——数据包的大小，单位为 Byte（字节），取值为 2 500；

M_1 ——日均交易量，单位为笔；

t_1 ——交易量完成时间（全天交易量的 80%，在 t 小时的高峰期完成），单位为小时，取值为 3~4。

3 事后监督系统所占广域网带宽与“日均交易量”有关，估计事后监督系统的业务量占省中心业务系统的日均交易量的 25%~50%。

事后监督系统峰值时所占广域网流量按下式计算：

$$W_m = 8 \times (1 + q_2) \times L_2 \times \left[\frac{0.7 \times M_2}{3600 \times t_2} \right] \quad (3.3.3-2)$$

式中：

方括号内代表每秒交易量；

W_m ——省中心业务系统峰值时所占广域网流量，单位为 bit/s；

q_2 ——冗余系数，对于网络带宽而言，通常取 50%，即允许网络内有 50% 的突发流量增加；

L_2 ——数据包的大小，单位为 Byte，取值为 2 500；

M_2 ——日均交易量，单位为笔；

t_2 ——交易量完成时间（全天交易量的 80%，在 t 小时的高峰期完成），单位为小时，取值为 3~4。

4 信息管理系统采用 B/S 结构，系统的带宽与并发用户数量有关。

信息管理系统所占广域网带宽按下式计算：

$$W_g = \frac{8 \times N \times L_3}{T} \quad (3.3.3-3)$$

式中：

W_g ——信息管理系统所占广域网流量，单位为 bit/s；

N ——访问系统的并发用户数，单位为个，取值为 20~50；

L_3 ——数据包的大小，单位为 Byte，取值为 5 000；

T ——浏览页面的时延，单位为 s，取值为 3~10。

田 万方数据
WANFANG DATA

4 网络管理

4.0.1 网络管理的主要管理功能可分为性能管理、故障管理、配置管理、统计分析管理、安全管理、事件管理、资产管理、软件分发、数据库管理、存储管理、用户管理和应用程序管理。具体应包括下列几个方面。

1 性能管理：主机的负载量、CPU 利用率、磁盘占用量、网络资源利用率、通信端口吞吐量、网络系统响应时间；各种应用程序的状态；数据库的状态（空闲空间）；系统可用性，系统负载平均值，呼叫溢出，可用交换空间，邮件队列长度，异常中断的进程，登录的用户数。

2 故障管理：实时收集网络设备和主机设备的故障信息，处理完这些信息后，按照不同的严重程度发出不同的故障告警信息；能够对故障告警信息进行汇总，并可集中处理；能够对故障进行过滤和相关处理，以滤除无关的信息，并对多种事件的相关性进行分析，处理故障的根源，为故障的定位提供帮助；对各节点的故障可以进行远程诊断、恢复功能。

3 配置管理：检查网络拓扑；当网络节点发生变化时（如节点、线路增减），可以通过管理控制台得到信息；自动检查系统软件和硬件资源，建立资源库；当系统资源发生变化时更新数据库，通过管理控制台得到相关信息；网络设备的远程在线设置；设备端口配置检查，参数定义，虚拟网划分；应用软件远程安装、升级或删除。

4 统计分析管理：实时或定时向被管设备发命令；收集全网发来的统计信息；对全网的设备、网络、资源使用等信息按正常运行和故障情况进行分类汇总统计；将统计、汇总后的信息形成文件并存档，可根据需要随时打印输出。

5 安全管理：对访问资源的控制；对非法访问进行控制；建立网络安全日志，包括安全服务机制的创建、维护、删除以及与安全

相关信息的发布，并生成安全事件分析报告。

4.0.2 邮政金融计算机网网络管理采用 SNMP 协议。

4.0.3 网络管理应符合下列要求。

- 1 系统应能每天 24 小时不间断地工作。
- 2 定时查询周期应符合以下要求：
 - 1) 统计性数据应 30~60min 一次；
 - 2) 状态性数据应 3~10min 一次。
- 3 网管信息存储时限要求：
 - 1) 周期性业务数据和告警信息应在硬盘上至少连续保留 1 个月，待月底进行月统计处理后，再备份到磁盘上，脱机保存；
 - 2) 重大告警文件和告警统计数据至少应在硬盘上保留 3 个月，每 3 个月备份到磁盘上，脱机保存；
 - 3) 对人机命令及回显的信息至少应在磁盘上保存 2 个月，并根据需要转储到磁带上，磁带上数据至少保留 2 年。
- 4 网络管理应具有屏幕显示和声光告警。
- 5 网络管理应能显示文字、数字和图像。



5 安全保密

5.0.1 邮政储蓄网的安全保密应考虑物理安全、网络安全、系统安全和数据安全。

5.0.2 物理安全是以物理的方法和技术，保障主机设备、网络设备、通信线路和媒体的安全。

物理安全主要包括防范各种自然灾害（防火、防水、防雷击），防范各种人为入侵及盗窃，防止擅自操作和使用设备，防止储蓄信息的丢失、泄露和破坏等。因此需要从基础设施、网络设备、故障处理、电磁兼容及防电磁泄露发射等方面为邮政储蓄系统提供安全可靠的运行环境和条件。

5.0.3 网络安全是邮政储蓄网安全体系中的关键，应根据邮政储蓄网络结构情况，利用防火墙和路由器访问控制技术（ACL）、网络物理隔离和虚拟局域网（VLAN）等技术，保障邮政储蓄网各级中心之间、各级中心内部以及与第三方连接的安全。

为确保邮政储蓄网的网络访问安全，系统需要采用的安全手段主要有：访问控制（含 VLAN）、防火墙、线路备份、入侵检测及安全审计等，还应配置防病毒软件。

5.0.4 系统安全包括操作系统、数据库、中间件和应用系统的安全。

1 操作系统：操作系统的安全是邮政储蓄网系统安全和网络安全的基础。操作系统应提供用户身份认证、资源权限划分、访问控制和日志审计等手段，保护信息资源不被非法访问和使用；并提供操作系统的备份与恢复等功能。

2 数据库：邮政储蓄网目前全部采用 Oracle 数据库。Oracle 数据库系统符合 NCSC 认证的 C2 级安全标准，提供严格的数据库恢复和事务完整性保障机制；提供完整的角色管理和自主控制安全机制；支持软、硬件容错，逻辑备份与恢复，物理备份与恢复，在线联机备份和恢复等功能；并在配置相应的软硬件后，能保证在发生故障和灾难后能够很好地恢复数据库或重构数据库。

3 中间件安全：邮政储蓄网使用 TUXEDO 交易中间件。TUXEDO 中间件应采取安全保护措施（如用户管理、权限管理等），以保护中间件相关资源不被非法访问和使用；同时，应进行中间件软件安全漏洞信息跟踪并及时安装安全补丁。

4 应用系统安全应包括：数据报文加密；数据报文鉴别；数据校验；用户身份的鉴别；用户权限控制；应用系统的备份与恢复等方面。

5.0.5 数据安全主要包括数据加密和数据存放、备份等方面。

1 邮政储蓄网可采用基于对称算法的数据加密方法，密钥的管理要采取分级管理方式。

1) 数据传输加密：邮政储蓄网与综合服务平台、第三方系统之间要鉴定数据传输的有效性（即不可修改性）；邮政储蓄网全国中心与各省中心之间、网点服务器与网点终端之间、网点终端与密码小键盘之间都应考虑数据传输的加密问题；对交易敏感数据如用户的密码（PIN）等关键数据要采用加密传输方式，以密文形式出现。

2) 数据存放加密：对用户敏感数据如用户密码等要实施数据加密存放。

3) 密钥的管理：邮政储蓄网全国中心与各省中心的密钥分为三层，第一层为主密钥，第二层为次主密钥，第三层为数据密钥。其中数据密钥主要用于对数据进行加密和解密，它受次主密钥的保护，而次主密钥受主密钥的保护。数据密钥有 MAC 密钥、敏感数据密钥和关键数据密钥等。

2 邮政储蓄网数据存放、备份等方面具体内容包括：采用 SAN 存储系统存储数据，应用数据应采用 RAID0 方式保护；配置磁带库进行数据的联机备份，并且异地存放；历史数据存放在查询服务器上，以备查询；应建立异地数据备份中心，同步或异步备份生产数据；确保各种故障情况下系统均能快速重建并恢复，保证业务运行的连续性。

6 设备配置及技术要求

6.1 设备配置原则

- 6.1.1 应具有高的可靠性、可用性和可扩充性，以及完善的安全保密措施。
- 6.1.2 系统应满足邮政储蓄业务处理的要求。
- 6.1.3 设备配置应满足投产后3年期业务能力，并具有现场扩充升级的能力。
- 6.1.4 应具有功能强、性能好、符合国家标准或国际标准的开放式系统平台，并具有良好的完整配套性。
- 6.1.5 应具备系统管理和网络管理的功能。
- 6.1.6 系统响应时间要求：省内单笔交易响应时间不大于3s；跨省单笔交易响应时间不大于5s。

6.2 设备配置

6.2.1 处理中心核心业务主机配置应符合下列要求：

1 核心业务主机应采用双机集群，数据库服务器与应用服务器分离，以互备方式工作。

2 主机的配置应综合考虑联机交易复杂程度、联机终端总量、交易峰值等因素。

3 主机处理能力（TPMC）按下列公式计算：

$$P = \frac{m_1 \times \varepsilon_1 \times \varepsilon_2 \times K_1}{60 \times J_1} \quad (6.2.1-1)$$

式中：

P ——主机处理能力，单位为每分钟处理的交易量（TPMC）；

m_1 ——预测近期年的日均交易量，单位为笔；

ε_1 ——忙日集中系数，取值为2~4；

ε_2 ——忙时集中系数，取值为 0.2~0.25；

K_1 ——平均交易复杂度，取值为 8~10；

J_1 ——主机处理能力保留系数，取值为 0.7。

4 主机内存容量主要考虑因素应包括：操作系统运行开销；数据库运行所占用的内存；用户进程占用的内存；其他如网管和安全审计所占用的内存；内存容量（单位千兆字节<GB>）与 CPU 个数之比不小于 1:1。

5 主机内存容量按下列公式计算：

$$M=O+D+(N_1 \times n) + Q \quad (6.2.1-2)$$

式中：

M ——数据库服务器应配置的内存容量；

O ——操作系统占用的内存总量，单位为 MB（兆字节），取值为 150；

D ——数据库系统占用的内存总量，单位为 MB，取值为 300~500；

N_1 ——活动进程数量；

n ——每个活动进程平均占用内存数量，单位为 MB，取值为 3.4；

Q ——其他系统占用的内存，单位为 MB，取值为 150。

6.2.2 处理中心事后监督主机配置应符合下列要求：

1 事后监督采用高性能 PC 服务器，主机应采用双机集群，以主备方式工作。

2 事后监督主机的配置应综合考虑联机交易复杂程度、联机终端总量等数据。

3 事后监督主机处理能力按下列公式计算：

$$P = \frac{m_2 \times \varepsilon_3 \times \varepsilon_4 \times K_2}{60 \times J_2} \quad (6.2.2)$$

式中：

P ——主机处理能力，单位为每分钟处理的交易量（TPMC）；

m_2 ——预测近期年的日均交易量，单位为笔；

ε_3 ——忙日集中系数，取值为 2~4；

ε_4 ——忙时集中系数，取值为 0.2~0.25；

K_2 ——平均交易复杂度，取值为 4；

J_2 ——主机处理能力保留系数，取值为 0.7。

4 事后监督主机内存的配置，建议内存与 CPU 个数之比不小于 1:1。

6.2.3 处理中心信息管理主机应按照本标准第 6.2.2 条的规定配置。

6.2.4 处理中心存储系统的配置应符合下列要求。

1 全国中心和省中心应采用 SAN 系统，但在过渡期内或业务量比较小的省中心，采用主机直联磁盘阵列方式；

2 采用 SAN 存储系统的省中心，核心业务、事后监督、信息管理、代理保险等系统共用 SAN 磁盘阵列；

3 中心应配置联机备份软件和磁带库，进行数据备份和恢复。

4 历史数据应保存在查询服务器中以备查询。

5 核心业务所需的磁盘容量按下列公式计算：

$$S = \frac{(S_0 + S_1 + S_2 + S_3 + S_4 + S_5 + S_6 + S_7) \times J}{A} \quad (6.2.4)$$

式中：

S ——磁盘阵列容量；

S_0 ——操作系统空间，单位为 GB（千兆字节），取值为 4；

S_1 ——中间件软件空间，单位为 GB，取值为 0.4；

S_2 ——应用软件固定部分，单位为 GB，取值为 1.5；

S_3 ——应用软件变动部分（包括报表部分），单位为 GB，取值为 10~25；

S_4 ——数据库系统表空间，单位为 GB，取值为 6.5；

S_5 ——数据库应用表空间（含分户账、客户资料、交易日志），单位为 GB，计算方法为：（储户数×1K+储户数×0.8×1K+日均交易量×1K×保存天数×1.2）×1.5/(1024×1024)；

S_6 ——数据库归档日志，单位为 GB，取值为 10~50；

S_7 ——数据库 REDOLOG，单位为 GB，取值为 1~3；

J ——磁盘冗余系数，取值为 2；

λ ——磁盘利用系数，取值为 0.7。

6.2.5 处理中心交换机的配置应符合下列要求：

- 1 中心应配置核心交换机，用于局域网设备的连接；
- 2 核心交换机应采用冗余备份工作方式；
- 3 核心交换机应为插板式交换机；
- 4 中心可配置工作组交换机用来接入管理 PC；
- 5 交换机端口配置数量应大于需要连接的端口总和，并至少留有 30%的空余端口。

6.2.6 处理中心路由器的配置应符合下列要求：

- 1 中心应配置核心路由器，用于连接通信汇接点或网点；
- 2 核心路由器应采用冗余备份工作方式；
- 3 路由器应提供主用通信线路和备用通信线路所需要的连接端口；
- 4 省中心应配置上联路由器，用于连接全国中心。

6.2.7 处理中心防火墙的配置应符合下列要求：

- 1 中心配置防火墙，用于中心与外部系统之间的通信隔离；
- 2 关键节点上的防火墙应采用冗余备份工作方式。

6.2.8 处理中心加密机的配置应符合下列要求：

- 1 加密机的主要功能为存储密钥和进行加解密计算，其密钥存储能力和加解密计算能力要能满足业务的处理需要；
- 2 采用双加密机方式，以主备方式运行；
- 3 为便于扩充和共享，应采用网络加密机；
- 4 加密机的存储和处理能力应能通过扩容获得提高，具备可扩展能力；
- 5 加密算法应能适应现有的邮政储蓄系统，符合金融加密机的相关规定。

6.2.9 处理中心系统软件的配置应符合下列要求：

- 1 系统软件主要包括服务器操作系统、集群软件、数据库、中间件、系统管理软件；
- 2 中心业务主机采用随机的 UNIX 操作系统；PC 服务器应采用 Linux 操作系统；
- 3 主机和 PC 服务器应配置高可用集群软件；
- 4 数据库系统使用 Oracle 9I 以上版本；
- 5 中间件采用 TUXEDO 8 以上版本。

6.2.10 汇接点局域网交换机的配置应符合下列要求：

- 1 汇接点配置 2 台工作组交换机，互为备份；
- 2 交换机端口配置数量应大于需要连接的端口总和，并至少留有 30%的空余端口。

6.2.11 汇接点路由器的配置应符合下列要求：

- 1 汇接点应配置 2 台路由器，互为备份；
- 2 路由器汇接网点的通信线路与省中心连接。

6.2.12 网点服务器应根据服务器所连接的网点的数量配置不同规模的 PC 服务器或 PC 机。

6.2.13 网点终端宜选用网络终端，储蓄终端应具有连接 POS、密码键盘、中英文存折打印机、磁卡读写器和 IC 读写器的接口。网络终端数量应根据投产年的日平均业务量配置。每个台席配置 1 台终端。

6.2.14 网点打印机：每个台席配置 1 台票据打印机；每台管理 PC 配置 1 台激光打印机或报表打印机。

6.2.15 网点密码小键盘：每个营业台席配置 1 个密码小键盘。

6.2.16 网点磁卡读写器：每个营业台席配置 1 个磁卡读写器。

6.2.17 网点工作组交换机/集线路：网点可配置 1 台工作组交换机或集线器，用于网点终端设备的连接。

6.2.18 网点路由器：网点可配置 1 台路由器，用于网点终端的接入。

6.2.19 网点 Modem 设备：网点应配置 Modem，用于网点与中心的

通信。每条通信线路配置 1 台 Modem。

6.3 设备技术要求

6.3.1 处理中心核心业务主机系统技术指标应符合下列要求：

- 1 主机系统应达到设计年限要求的规模容量；
- 2 具有扩充 CPU、内存能力；
- 3 主机系统应配置镜像内置硬盘；
- 4 具备 Ultra SCSI 接口，在满足配置要求后应有一定的空余接口；
- 5 至少配置 2 块不低于 100/1000Mbit/s 的自适应网卡；
- 6 支持符合国际标准的 UNIX 系统；
- 7 主机系统应配置内置磁带机。

6.3.2 处理中心事后监督/信息管理主机系统技术指标应符合下列要求：

- 1 后督、信息管理主机系统应达到设计年限要求的规模容量；
- 2 支持多处理器、具有扩充内存、内置硬盘的能力；
- 3 具备 Ultra SCSI 接口，支持 RAID 0、RAID 0+1、RAID 5；
- 4 至少配置 2 块不低于 100/1 000Mbit/s 的自适应网卡；
- 5 支持符合国际标准的 Linux 系统。

6.3.3 处理中心存储设备技术指标应符合下列要求：

- 1 存储阵列的配置容量应达到设备满足年的规模容量；
- 2 光纤存储阵列和光纤存储交换机应支持 ESCON/SCSI/FICON/FC 等多种通道接口类型并兼容主流厂家的光纤通道卡；
- 3 存储阵列应支持多种 RAID 存储方式，包括 RAID 0+1 和 RAID 5 及混合模式（即 RAID 0+1 和 RAID 5 同时工作）；
- 4 光纤存储阵列的光纤接口采用多模光纤，带宽不小于 2Gbit/s；
- 5 存储阵列应配置冗余电源；
- 6 应配置备份设备（如磁带机/库或光盘机/库）；
- 7 主要存储设备（磁盘阵列、光纤存储交换机、光纤通道卡）

均应采用冗余配置。

6.3.4 处理中心交换机技术指标应符合下列要求：

- 1 中心核心交换机需支持三层交换和划分子网的功能；
- 2 交换引擎、电源、风扇应为冗余配置；
- 3 支持 100/1 000Mbit/s 的网络接口；
- 4 具备模块化扩展能力；
- 5 交换机配置的端口在满足当前需求后应有 30%的预留端口；
- 6 应支持简单网络管理协议（SNMP）。

6.3.5 处理中心路由器技术指标应符合下列要求：

- 1 中心核心路由器应采用多协议路由器；
- 2 具备模块化扩展能力；
- 3 支持 SDH、ATM 、DDN、Frame Relay、PPP 等广域网接口和协议；
- 4 可提供 100Base-T、E1、V.35 和 ATM 接口；
- 5 支持端口的信道化；
- 6 具有广播风暴隔离、虚拟网交换、端口过滤等功能；
- 7 交换引擎、电源、风扇应为冗余配置。

6.3.6 处理中心防火墙技术指标应符合下列要求：

- 1 基本技术要求应符合 YD/T 1132-2001 《防火墙设备技术要求》的规定，应具有 4 个以上的局域网端口；
- 2 防火墙工作在冗余备份方式时，每台应具备专门的 HA 口用于防火墙之间的通信。

6.3.7 处理中心加密机技术指标应符合下列要求：

- 1 提供局域网接口，支持 TCP/IP 协议；
- 2 支持 RSA、DSA、ECC、Diffe Hellman 等公钥算法，RSA 模长可选 512、768、1024、2048bit；
- 3 支持 DES、TRIPLE-DES、IDEA、RC2、RC4、RC5 等对称算法；
- 4 提供 PKCS#11、CDSA、X.509 等国际标准开发接口。

6.3.8 处理中心系统软件技术指标应符合下列要求：

- 1 所有系统软件的安全级别应达到 C2 级以上；
- 2 操作系统应与主流的数据库（Oracle、Sybase、Informix、DB2 等）和中间件（TUXEDO、CICS 等）兼容；
- 3 支持 GB 18030 中文标准及其它有关的国家标准；
- 4 中心服务器的操作系统应配置双机高可用集群软件。

6.3.9 汇接点局域网交换机指标应符合下列要求：

- 1 汇接点工作组交换机应支持不低于 10/100Mbit/s 的网络接口；
- 2 应具有插板扩展能力或堆叠式扩展能力；
- 3 应支持 SNMP 协议。

6.3.10 汇接点路由器指标应符合下列要求：

- 1 汇接点路由器应采用多协议路由器；
- 2 具备模块化扩展能力；
- 3 路由器应能够与现有网络设备互联互通。

6.3.11 网点服务器技术指标应符合下列要求：

- 1 网点服务器可根据连接的网点数量（终端数量）选择 PC 服务器或 PC 机；
- 2 具有扩充内存、内置硬盘的能力；
- 3 配置 100/1 000Mbit/s 的自适应网卡；
- 4 支持符合国际标准的 SCO UNIX 或 Linux。

6.3.12 网点终端技术指标应符合下列要求：

- 1 平均无故障运行时间应大于 15 000h；
- 2 应符合国家标准 GB 4943-2001《信息技术设备的安全》的要求；
- 3 应采用 16 点阵以上显示，16 或 24 点阵汉字打印；
- 4 显示速度应超过 3 800 字符/s；
- 5 应采用 GB 18030 字符集或 GBK 大字符集；
- 6 网络终端应支持多屏切换；

7 应支持透明打印、控制打印、拷贝打印、屏幕拷贝、格式打印、条码打印等，可支持各种 24 针打印机；

8 应至少具有 1 个主通信口，3 个辅通信口，辅口命令可仿真其他终端；

9 网络终端应采用以太网（TCP/IP 协议）通信方式，可同时具有 RS232 异步通信方式。

6.3.13 网点票据打印机技术指标应符合下列要求。

1 进送纸模式：单页纸应具有正向及反向进纸模式；连续纸应具有后进前出的送纸方式。

2 打印针数：24 针。

3 打印头寿命应不小于 2 亿点。

4 打印速度：西文高速打印速度宜不小于 120 字符/s，西文信函打印速度宜不小于 60 字符/s；中文高速打印速度宜不小于 90 汉字/s，中文信函打印速度宜不小于 45 汉字/s；

5 打印宽度不小于 80 列。

6 并口数应不小于 1。

7 应支持 GB 18030 大字符集。

6.3.14 网点密码小键盘技术指标应符合下列要求：

1 12 键或 14 键；

2 宜具有语音功能；

3 应具有 RS 232/TTL 接口、PS/2 键盘接口可选；

4 键体寿命宜不小于 2 000 万次。

6.3.15 网点磁卡读写器技术指标应符合下列要求：

1 接口应支持 RS 232、USB 等标准；

2 磁头寿命应大于 500 000 次（有效刷卡）；

3 划卡速度应大于 10cm/s；

4 读写标准应符合 ISO、ANSI、DIN 标准，并可通过拨码设置；

5 磁条读写标准应符合 ISO/ANSI、ISO7810/12/13 标准。

6.3.16 网点工作组交换机/集线器技术指标应符合下列要求：

1 端口数量应大于需要连接设备数量总和，并预留 20%~30% 的空余端口；

2 采用 RJ45 接口。

6.3.17 网点路由器技术指标应符合下列要求：

1 应具备至少 1 个以太网接口；

2 应具备至少 1 个同异步多串口模块；

3 应能够与现有网络设备互联互通。

田 万方数据
WANFANG DATA

7 机房及设备安装要求

7.1 机房场地要求

7.1.1 邮政储蓄网中心机房位置的选择应符合邮政行业标准 YZ/T 0042-2001《邮政综合计算机网信息中心机房场地要求》中 2.1 节规定，同时还应满足以下要求：

- 1 应与综合网其他系统合用机房场地；
- 2 不应建在雷暴多发区；
- 3 应满足通信安全保密、人防、消防等要求；
- 4 上述各条如无法满足，应采取相应的技术措施。

7.1.2 场地的组成和计算机机房的使用面积按邮政行业标准 YZ/T 0042-2001《邮政综合计算机网信息中心机房场地要求》中 2.2 节规定进行计算确定。

7.1.3 机房内温度、湿度、尘埃、照明、电磁场干扰等应符合邮政行业标准 YZ/T 0042-2001《邮政综合计算机网信息中心机房场地要求》中 2.4 节规定。

7.1.4 中心机房供配电应符合邮政行业标准 YZ/T 0042-2001《邮政综合计算机网信息中心机房场地要求》中 2.5 节规定。UPS 电源详细的技术要求应符合国家标准 GB/T 14715-1993《信息技术设备用不间断电源通用技术条件》的规定。

7.1.5 中心机房接地要求应符合邮政行业标准 YZ/T 0042-2001《邮政综合计算机网信息中心机房场地要求》中 2.6 节规定。

7.1.6 中心机房场地安全要求应符合邮政行业标准 YZ/T 0042-2001《邮政综合计算机网信息中心机房场地要求》中 3.1~3.5 节规定。机房的防静电技术要求应符合行业标准 YD/T 754-1995《通信机房静电防护通则》的规定。

7.1.7 中心主机系统应采用独立的空调系统，空调系统应符合国家标准 GB 50174-93《电子计算机机房设计规范》中第 5 章的规定。

7.1.8 消防应符合下列要求：

1 中心机房必须设置火灾自动报警装置和自动消防系统，并应配备灭火器；

2 中心机房内禁止使用自动喷沫装置；

3 在中心机房内、工作用房内、活动地板下和吊顶内应设置烟、温感探测器。

4 其他应按照 YZ/T 0042-2001《邮政综合计算机网信息中心机房场地要求》中 3.2 节规定执行。

7.1.9 中心机房的抗震设计应符合行业标准 YD 5059-98《通信设备安装抗震设计规范》的规定。

7.2 设备安装要求

7.2.1 设备布放应按照下列要求：

1 需要经常监视或操作的设备布置应便利操作；

2 两相对机柜正面之间的距离不应小于 1.5m。

3 机柜侧面（或不用面）距墙不应小于 0.5m，当需要维修测试时，则距墙不应小于 1.2m。

7.2.2 布线应按照下列要求：

1 在裁剪和布放通信电缆之前应进行路由核实和距离复核，按核实的具体距离裁剪电缆。

2 通信电缆与电力电缆应分别按不同的路由敷设，电缆转弯时最小弯曲半径不得小于电缆线径的 15 倍，如相互之间距离较近，也应至少保持 100ms 以上的距离。

3 电力电缆及通信电缆的敷设应符合行业标准 YD 5002-94《邮电建筑防火设计标准》中第 2 章的规定。

附录 A

(规范性附录)

本规范用词说明

A.0.1 表示很严格，非这样做不可的用词

正面词采用“必须”；

反面词采用“严禁”。

A.0.2 表示严格，在正常情况下均这样做的用词

正面词采用“应”；

反面词采用“不应”或“不得”。

A.0.3 表示允许有选择，在条件许可时首先应这样做的用词

正面词采用“宜”或“可”；

反面词采用“不宜”。

中华人民共和国邮政行业标准

**邮政金融计算机网络系统工程
设计规范（储蓄部分）**

YZ/T 0115-2005

条 文 说 明

田 万万数据
WANFANG DATA

编制说明

邮政金融计算机网络系统工程设计规范（储蓄部分）是根据国家邮政局国邮〔2004〕271号文《关于下达国家邮政局2004年第一批新技术开发项目计划（邮政标准类）的通知》（本项目计划编号为B200422），对原邮电部于1997年9月发布的《邮政金融计算机网络系统工程设计暂行规定》（YD5042-97）的修订。

随着邮政储蓄业务的发展以及计算机和通信技术的不断进步，原设计暂行规定已不能指导目前邮政储蓄计算机网络工程的设计。本规范是在参阅了大量的邮政储蓄网络的技术方案、工程设计，总结了多年来邮政储蓄计算机网络的建设经验，结合目前技术进步情况编制的。

本规范主要对邮政金融计算机网络系统（储蓄部分）的工程设计进行规范，包括邮政金融计算机网络系统的总体要求、系统建设方案、主机设备配置原则及标准等。主要适用于邮政金融计算机网络系统（储蓄部分）的方案规划、可行性研究及工程设计。

中讯邮电咨询设计院于2004年8月中旬接到任务后，立即组成项目组，根据国家邮政局业务主管部门对项目编写范围、深度、格式及时间进度的要求，明确了该规范的范围为：根据《全国邮政金融计算机网技术体制》和《邮政金融计算机网络系统储蓄应用软件统一版本工作技术方案》，制定出邮政金融计算机系统（储蓄部分）的设计规范，设计规范包括邮政金融计算机网（储蓄部分）的总体建设方案、网络结构、省中心（全国中心）、汇接点、网点的设备配置及相关技术要求。

项目组随后开始收集资料，并对河南、广东等省份的邮政储蓄计算机系统统一版本工程建设情况进行现场调研。至8月底前，项目组多次与国家邮政局、统一版本建设的省局、系统开发商及本项目的归口单位国家邮政局科学研究规划院等就本项目的相关工程技

术问题进行了交流，得到了上述部门与单位的多方协助，在此基础上，项目组初步完成了文本编制工作，经内部讨论和审核后进一步修改完善，最后形成了本规范的征求意见稿。根据邮政行业标准管理办法的要求，中讯邮电咨询设计院项目组将向国家邮政局计划财务部（科技处、计划处、工程管理处）、信息技术局、科学研究规划院邮政标准化技术归口办公室和河南、广东、江苏省邮政局以及北京市邮政管理局等单位寄送了征求意见稿。2004年12月，国家邮政局和各省邮政局对本规范的意见陆续返回，项目组根据意见对设计规范进行了修改，最终形成《邮政金融计算机网络系统工程设计规范》（储蓄部分）的报批稿。

本规范与原规范相比修改和增加的内容较多，无法按原规范条文顺序和内容进行解释和说明，现就修订后内容按新条文顺序作如下说明。

田 万万数据
WANFANG DATA

1 总则

1.0.7 在邮政储蓄网的建设中，网络结构、软件设计和数据库设计是以省数据集中的模式进行设计，但应考虑多省集中的模式，为数据大集中奠定基础。

目前，邮政金融计算机网（储蓄部分）是以省集中模式建设，但国内外的建设情况表明，金融网的建设最终都是数据大集中的模式，因此邮政金融计算机网在规划、设计时应考虑到以后数据大集中的模式。

3 系统方案

3.3 系统通信

3.3.3 通信带宽测算应按下列方式确定：

1 通信带宽的测算主要是计算省中心对汇接点之间的带宽，省中心对全国中心的广域通信主要采用综合网广域网，通信带宽一般采用 2Mbit/s。

2 根据日均交易量计算将依据以下条件：对于省中心业务系统而言，一笔交易由交易请求包和交易响应包两个交易包组成。其中，上传包（交易请求包）一般小于 1kbyte；下传包（交易响应包）中，50% 小于 1kbyte，一般是普通账务类的交易；30% 介于 1kbyte~1.5kbyte 之间，一般是单笔管理交易或普通查询交易；20% 大于 1.5kbyte，一般为多笔查询、打印类交易，如明细查询、流水查询，或者是报表、批量文件类的交易。综合考虑每日交易发生的频度及峰值情况，取数据包的大小为 (1+1.5) Kbyte。

3 计算事后监督系统所占带宽将依据以下条件：

1) 假设全天交易量花 6h 完成；

2) 对于事后监督系统而言，一笔交易由 2 个数据包组成，其中，上传数据包小于 1kbyte，下传数据包取其均值为 1.5kbyte，即 (1k+1.5k) byte。

5 安全保密

5.0.3 为确保邮政储蓄计算机网络系统的网络访问安全，系统需要采用的安全手段主要有访问控制（含 VLAN）、防火墙、线路备份、入侵检测及安全审计等。

1 访问控制：用于对邮政储蓄计算机网络系统资源的访问，防止未经授权而利用网络访问系统资源，利用已得到鉴别的身份或利用有关的信息，按事先确定的规则实施访问权的控制。

2 防火墙：一组计算机硬件和软件的结合体，在外部网与邮政储蓄计算机网络系统之间建立起一个安全网关，从而保护内部系统免受非法用户的侵害，同时具有 IP 地址转换功能，以便对外有效屏蔽网络内部 IP 地址，提高网络的安全性。

3 入侵检测：在网络安全管理中，除使用一般的网管软件和系统监控管理软件外，还应使用网络监控设备或实时入侵检测设备，以便对进出各级局域网的常见操作进行实时检查、监控、报警和阻断，从而防止针对网络的攻击与犯罪行为。

4 安全审计：在邮政储蓄计算机网络系统中，需设置对信息包及信息包内容监管的系统和设备，用以探测信息包的异常来源和去向，对信息包的内容进行检查。

5.0.5 数据安全主要包括数据加密和数据存放、备份等方面。

3 密钥的管理：邮政储蓄全国中心与各省中心的密钥分为三层，第一层为主密钥，第二层为次主密钥，第三层为数据密钥。其中数据密钥主要用于对数据进行加密和解密，它受次主密钥的保护，而次主密钥受主密钥的保护。数据密钥有 MAC 密钥、敏感数据密钥和关键数据密钥等。

1) 全国中心的密钥管理：全国中心主密钥由全国中心负责产生、保存和载入。全国中心到各省中心的次主密钥在全国中心产生，并由全国中心向各省中心分发。全国中心负责与其直接相连接的省

中心间的数据密钥的产生和分发。全国中心将根据需要定期或不定期地向省中心发送重置数据密钥的交易，并传送所产生的密钥；也可根据省中心发来的申请重置数据密钥的请求产生新密钥，并分发给省中心。

2) 省中心的密钥管理：省中心的主密钥在各省中心产生，次主密钥由全国中心分发。省中心负责与其相连接的地市、市县局和网点的密钥的产生和分发。省中心将根据需要定期或不定期地向地市、市县局和网点发送重置数据密钥的消息，并传送所产生的密钥。

6 设备配置及技术要求

6.2 设备配置

6.2.1 处理中心核心业务主机配置应符合下列要求：

3 主机处理能力 (TPMC) 按下列公式计算：

m_1 ——预测近期年的日均交易量，日均交易量应包括核心业务的账户业务和非账户业务、中间业务以及不成功的请求。

K_1 ——平均交易复杂度，取值为 8~10，根据各地的实际情况可做适度调整。

6.2.4 处理中心存储系统的配置应符合下列要求。

5 核心业务所需的磁盘容量按下列公式计算：

S_5 ——数据库应用表空间 (含分户账、客户资料、交易日志)，单位为千兆字节，计算方法为：

$(\text{储户数} \times 1K + \text{储户数} \times 0.8 \times 1K + \text{日均交易量} \times 1K \times \text{保存天数} \times 1.2) \times 1.5 / (1024 \times 1024)$

其中 1.5 表示除数据表空间外，还需索引等空间，故乘 1.5 的系数。

6.2.12 网点服务器可以放置在网点，也可放置在地县汇接点，根据各省的具体情况而定。对于网点服务器一般建议采用 PC 服务器。

6.3 设备技术要求

6.3.3 处理中心存储设备技术指标应符合下列要求。

存储设备：在全国中心或省中心配置的应采用 SAN 存储区域网，光纤交换机应配置 2 台，连接磁盘阵列。核心业务系统、事后监督系统、信息管理系统、代理保险系统、电子汇兑系统 (7 个一级中心局所在的城市除外) 共用 SAN 存储系统。