基于资产经营平台的无边界动态资产盘活管理模式

柳林芳 楼 斌 张 羽 赵秀云 孙铁军

（中国联通山东省分公司，济南 250001）

摘 要：加强各项资源使用效益的精细化管理，是通信企业应对市场竞争、提升企业价值创造力的重要途径。本文结合山东联通搭建网络化经营平台，构建动态无边界资源管理和价值创造体系的案例，探讨了国有通信企业如何提高实物资产盘活和增值管理水平，以实现国有资产的保值增值。

关键词：网络化 经营平台 资产 增值

1 通信企业国有资产管理的背景

(1)实现通信资源价值最大化，是通信企业面临的重大难题

作为技术带动型行业，通信行业的新技术发展日新月异，新设备更新周期不断缩短，尤其是近年来互联网、3G、云计算、物联网等的应用、普及，导致传统网络资产的迅速退网和贬值，对原有资产运营管理模式构成了全新挑战。同时，高端客户对新技术的需求非常迫切，但原有产品无法满足其多元化、个性化、综合化的需求。为有效发展、保有这部分客户，做好新技术、新设备的更新换代，之前投入使用仅 2、3 年的技术和设备，就面临退网而带来资产损失。鉴于此，有效发挥传统网络资产的使用价值，就成为通信企业面临的重要课题。

(2)企业资产价值创造能力和 EVA 改善压力大

经过多年发展，国有通信企业形成了庞大的资产和网络，又承担了城乡普遍服务义务，在广大农村地区投资建设了通达县、乡、村镇的固话网络、长途 / 本地传输网络、宽带通信网络及营业服务网络，这部分资产占比大、创收能力低，在一定程度上导致企业总资产报酬率和 EVA 指标不高。

(3)国有资产保值增值责任重大，亟需提升价值创造能力

国有资产保值增值是维护社会简单再生产从而进行扩大再生产的必要条件，也是企业持续发展的前提。国有资产保值增值责任重大。

2 通信企业国有资产管理的难点

(1)企业资产规模大，分布广，涉及单位、部门、人员众多，难以实现完全的流程化控制。各系统相对独立，企业难以实时准确掌控全局实物资产信息和进行决策。

(2)资产管理缺乏有效的信息支撑手段，无法与企业 ERP 系统信息实时对应，闲置资产信息统计困难且工作量巨大，统计的信息也无法确保准确，大大制约了各级单位的资产增值管理工作。

(3)资产盘活和增值工作的实施效果难以实时准确统计和流程控制，导致绩效考核无法真正落实到位；而仅仅满足于资产管理定期盘点的被动管理，无法实现资产盘活和增值管理工作常态化。

3 山东联通资产增值管理的主要做法和实施效益

3.1 主要做法

3.1.1 对实物资产进行科学分类，分析各类资产特点，总结分析盘活、增值管理中的难点和不足

山东联通把实物资产分为网络资产、房地产、信

息化资产、ADSL 终端、库存物资五类,根据各类资产的现状和主要特点,分析各类资产在盘活与增值管理中存在的难点和不足。

3.1.2 搭建全过程、全方位企业资产经营平台

为有效支撑实物资产盘活与增值管理工作的开展,山东联通由财务部牵头,组织各专业部门深入讨论、合理分工,深入一线调研,在广泛征集各单位、各角色用户意见的基础上,通过与企业已有 ERP 系统、工程管理(PMS)系统建立接口,搭建了网络化资产经营平台,并在全省逐步推广,使全省资产经营能力和价值创造力得到有效提升。该平台涵盖全部实物类资产,覆盖省、市、县各级单位和各资产使用部门,解决了资产闲置、盘活信息更新难度大、效率低、缺乏信息化手段等问题,实现了网络化流程管理,分工明确,信息及时, 切实解决了资产盘活工作遇到的各种问题,有效促进了资产使用效益的提升。

(1)搭建网络平台,完善资产经营各项功能:将资产闲置和盘活流程在资产经营平台中进行固化;源头创新,拓展资产盘活方式;打开和突破物资盘活路径;各类统计分析报表自动出具。

(2)为网络化经营平台运行提供系统保障:建立专门的支撑保障团队;制度约束,流程固化;提升和加大专业线推动力度;采购环节刚性控制,保证平台使用效果;通报平台使用情况,考核资产盘活成效;传导资产盘活理念,推动资产经营平台的使用;以案例征集和经验推广等,推动平台的应用推广。

3.1.3 利用资产经营平台, 有针对性地做好各类资产的增值和盘活工作

资产经营平台上线前,各部门职责未进行流程化控制;闲置资产的信息是通过手工登记,信息无法及时更新、共享,也难以准确统计,各市分公司、各部门间信息不对称、不共享,制约了盘活工作的开展。盘活实施效果无法准确统计分析,难以调动各部门、各单位的积极性, 一定程度上制约了盘活工作的顺利开展。

资产经营平台上线后,平台相关信息自动从 ERP 系统和工程建设系统获取,各业务流程和信息流转均通过工作流的形式在平台内实现,资产经营平台各环节只需简单录入个别必要补充信息,即可完成本环节操作。山东联通全省各单位通过资产经营平台,创新了传统的实物资产盘活和增值管理模式,适时推进闲置、盘活、投资再利用等各项业务流程,及时进行各项数据统计分析, 纵向推动本专业盘活工作的开展,切实促进了资产盘活和增值管理工作。

(1)资产的闲置信息发布流程

1)各资产使用部门在实际使用资产过程中,或在网络优化、退网过程中,发现部分资产闲置,该部门资产管理员在资产经营平台中选择该批资产,录入闲置原因、建议利用方式等简要信息,提交该单据,自动发送至专业部门专业主管鉴定。

2) 专业主管收到单据后, 组织技术人员进行鉴定,确定设备完好情况,判断是否可再利用。对可在本单位继续使用的,审批通过,该批资产转入本单位闲置资源信息库, 本单位全部人员可以看到该共享信息;如在本单位无法使用、但在其他地市可以使用,选择省公司专业主管鉴定。省公司专业主管鉴定通过后,转入全省闲置资源信息库,全省人员可以看到该共享信息; 如判断在本单位无法使用或使用效率不高、但对外出租或处置价值较高(如房地产),选择财务部共同鉴定,鉴定通过后,转入本单位闲置资源信息库;对资产损坏应维修的,维修后在平台履行相应闲置流程; 对资产损坏且无法修复或不值得维修的,履行 ERP 系统相应报废流程。

(2)资产的再利用登记流程

1)建设部专业主管进行工程设计时,工程建设系统(PMS)自动发送项目信息到专业部门专业主管。专业主管根据项目建设需求,提供资产经营平台中符合需求的闲置资产清单给建设部专业主管。建设部专业主管在进行项目建设过程中优先采用这些闲置资产,此外再确定采购清单;对不使用的闲置资产反馈给专业部门专业主管。

2) 采购部在对建设部提供的采购清单进行采购前,须经本单位专业部门专业主管确认在资产经营平台确无同类可利用资产后,方可采购。

3)专业部门专业主管根据再利用设备情况,对已利用闲置资产进行再利用登记,更新资产经营平台信息。

3.1.4 实例:某市分公司利用资产经营平台,盘活 DSLAM 设备,全省共节约投资 1 千多万元

某市分公司在宽带提速项目建设中,退网了部分

DSLAM设备。省公司通过网络化经营平台,快速摸底全省 DSLAM 设备需求情况,判断该批 DSLAM 设备能满足全省一段时间内需求,于是决定暂时停止全省 DSLAM 新设备采购,鼓励各市分公司积极利用该批闲置设备。各市分公司从平台获知该信息,与该市分公司联系,在相关网络建设需求时充分利用闲置 DSLAM 设备。全省通过盘活闲置 DSLAM 板卡,共节约投资 1 千多万元。

3.2 实施效益

山东联通基于网络化经营平台的资产增值管理模式 2009 年底正式上线,成为中国联通企业资产管理领域的成熟范例,取得了显著的管理效益和经济效益。

(1) 该资产增值管理模式整合了企业内部 ERP 系统、工程建设系统等子系统,通过构建网络化的资产经营平台和流程控制管理,实现了对全省实物资产的实时掌控和价值增值管理,彻底解决了资产更新快、地域发展不平衡、资产闲置,以及盘活工作难度大、效率低、缺乏信息化手段等问题,为企业经营发展提供了准确的决策参考和系统支撑,有效促进了企业资产管理工作效率和国有资产效益的快速提升。一方面,专业部门可实时掌控实物资产信息,对通信技术更新换代的退网资产在不同地区及时调拨,实现了对闲置资产的充分利用;另一方面,保证了业务部门及时汇总、分析盘活信息和报表的准确、完整。

(2)山东联通对融合重组后原山东联通、山东网通的各类网络资源进行了全面摸底,对退网资产通过资产经营平台进行及时再利用,实现了两网融合与资产最佳配置,在资源使用效益方面实现了“1+1〉2”。

(3)企业综合资产使用效益持续改善,净资产收益率提升了 2%,EVA 指标提升了近 5 亿元。

4 对通信企业国有资产管理的建议

4.1 搭建网络化的综合性资产经营平台,为资产增值管理提供系统支撑

针对当前国有企业资产管理领域重管控轻增值、资产闲置和盘活难度大、效率低,以及资产经营能力不足等难题,通信企业应研发基于网络化的综合性资产经营平台,通过与企业内部 ERP 系统、工程管理系统建立接口,构建新颖的动态无边界资源管理方式和价值创造体系,消除传统国有资产管理中的区域范围、技术更新、专业领域等障碍因素,实现各单位、各专业领域资源的实时动态共享,创建多维度、多角色、多层次、全过程、全方位的资产价值管理体系,为企业经营发展提供准确的决策参考和系统支撑,推进国有资产的保值增值。

4.2 制定资产增值管理制度和流程,实现资产增值管理常态化

(1)建立常态化工作机制

制定本企业资产增值管理制度、实施方案和工作流程图,明确各部门职责分工,并将流程和职责分工固化在网络化经营平台中,实现资产增值管理工作常态化;发挥专业线优势,形成专业管理与财务导向齐抓共管、密切配合的工作局面,确保资产增值管理工作的稳步开展。

(2)制定资产增值管理激励措施

针对资产增值管理工作开展情况制定激励措施,以专项激励方式促进资产增值工作的开展,并根据资产规模、地域经济、增值管理成效等数据,采用科学的方法进行数据评比,保证考核的客观公正和有效激励。

4.3 传导资产增值管理理念,发挥全体员工国有资产保值增值的主人翁精神

通过多种形式,对基于网络化经营平台的盘活理念进行宣贯,传导到资产专业管理部门、使用部门,进而传导到全体员工,使资产增值理念深入人心,发挥全体员工国有资产保值增值的主人翁精神。强化全员参与意识,积极开展资产增值管理的案例征集、评比、推广活动,集思广益,广泛发动,充分挖掘基层单位的工作智慧,搭建有效的沟通平台,将资产增值管理先进经验进行及时推广。

基于物联网技术的“移动助学”公交系统及其应用

李 然 李林林

（中国移动山东公司济宁分公司,济宁 272000）

摘 要:“移动助学”公交系统利用物联网技术中的射频技术、无线视频监控技术、GPS 定位技术,成功地将移动信息化应用在校车上,助力校车安全运行。系统采用“终端+平台”模式,主要包括关爱信息发布、3G 无线视频监控两部分,可以将学生上/下车、到/离校信息及时发送到手机上,使家长、老师、公交公司及管理部门能通过移动终端、PC 客户端等实时掌握校车和学生的情况。

关键词:物联网 关爱信息发布 无线视频监控 GPS 定位

1 引言

为助力平安校车建设,济宁移动与兖州公交联合开展了“助学公交 多一点关爱给孩子”活动。济宁移动依托物联网等技术,将“关爱信息发布”、“无线视频监控”等信息化应用集成到“移动助学”公交系统上,使家长、学校、公交公司及管理部门能够实时掌握校车和学生的情况。

2 “移动助学”公交系统相关技术

2.1 物联网技术

“移动助学”公交系统采用 RFID 射频卡技术,在射频卡中存储学生的身份标识信息。在学生办理校车乘车卡时记录学生相关信息，并分配身份标识号,记录在学生乘车卡中；系统同时记录学生家长数据,包括手机号、姓名、关系等。当学生通过读卡终端刷卡时，中国移动 M2M 管理平台读取并识别信息后,将学生上、下车信息通过 GPRS 无线网络发送至预先设定的家长手机上。

2.2 3G 移动通信技术

基于中国移动 3G 无线网络,依托移动视频监控技术,车载移动视频监控设备通过点到点传输实时采集的校车内视频信息,借助移动无线网络上传至管理平台;管理平台对视频信息进行解析、压缩及传输编解码，解析压缩后的视频信息通过移动终端（手机、PDA）、PC 客户端等可以实时、流畅地查看。而且,通过移动终端、PC 客户端可以控制车载移动视频监控设备的云台进行上下、左右转动,全方位掌握校车内状况。

2.3 GPS 定位技术

“移动助学”公交系统采用 GPS 定位技术,结合短信息服务系统、GIS 地理信息服务系统，在校车上安装 GPS 定位终端,学校、公交公司及管理部门可以登陆校车智能管理平台或发送短信,实时掌控校车运行状况。

3 “移动助学”公交系统结构

系统采用“终端＋平台”模式。系统主要包括关爱信息发布、3G 无线视频监控两部分。关爱信息发布平台集成 RFID 射频技术,通过射频读卡终端识别学生信息,经过数据采集系统、业务支撑系统的数据分析、处理后,将信息上传到中国移动行业网关,实现信息的及时、准确发送,系统网络结构如图 1 所示。

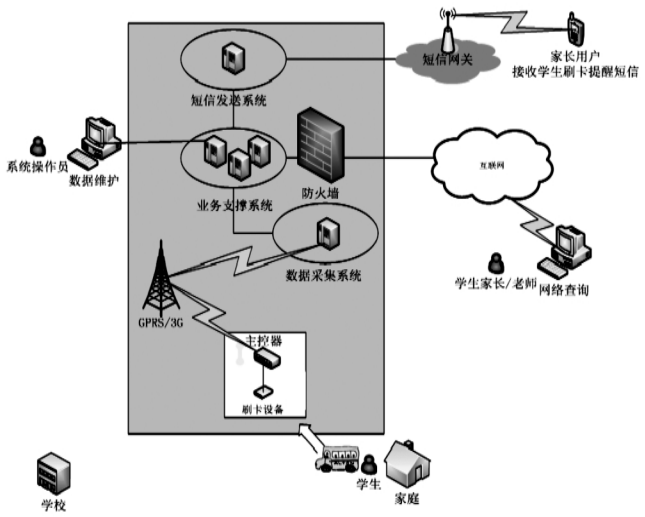


图 **1** 关爱信息发布模块网络结构

3G 无线视频监控通过搭建管理平台，经过视频信息采集、数据分析、端口传输、监控画面压缩上传等数据处理，以中国移动 3G 网络为数据信息传输通道,实现 WEB、WAP 两种模式的视频信息实时查看，系统网络结构如图 2 所示。

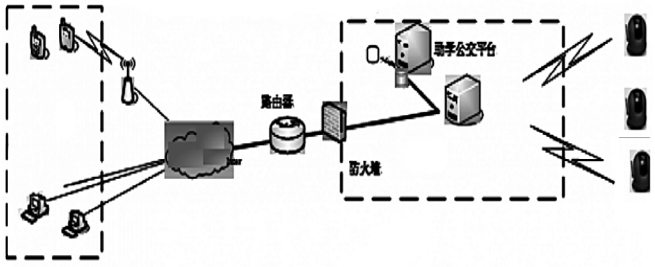


图 **2** 无线视频监控网络结构

4 “移动助学”公交系统主要功能

4.1 关爱信息发布

(1)上 / 下公交车短信提醒

学生上 / 下公交车刷卡时,读卡终端识别学生信息后,关爱信息发布平台自动将学生上 / 下车提醒信息及时发送到预先设定的家长手机上,包括刷卡学生姓名、上 / 下车时间、校车车号等。当校车因堵车及其它原因晚点时,家长、老师手机可收到晚点提醒、预计到达时间短信。

(2)到 / 离校短信提醒

学生到 / 离校刷卡时，读卡终端识别学生信息后,平台自动将学生到 / 离校提醒信息发送到预先设定的家长手机上,包括学生姓名、到 / 离校时间等信息。

(3)家校互动

通过关爱信息发布平台实现家长和老师的互动交流。老师可以将孩子在校的健康状况、学习成绩、日常表现、当天作业、学校动态和通知等信息直接发送到家长的手机上；家长可以登陆平台与老师互动,查询学生在校情况。

(4)关爱提醒

通过平台,公交公司和学校均可以向家长发送天气、路况、安全出行常识等短信,提醒家长、学生注意出行安全。

4.2 无线视频监控

(1)手机实时视频监控

通过手机终端，可以自动调节校车内的摄像头，全方位掌握车内情况。

(2)浏览器视频实时监控

家长、老师可通过浏览器,以访问网站方式查看孩子在校车内的情况。

(3)运动侦测,联动报警功能

校车停车落锁后,如车内仍有活动的学生,将触发告警短信,避免学生滞留在封闭的车内造成严重的后果。

通过灵敏度设置,无线视频监控一体机可以识别图像的变化,能检测到人或物体的细微运动而触发报警。

(4)全程数字录像

以数字编码录像方式对视频监控信息进行保存,方便后期管理、查询回放视频监控录像。

(5)人性化本地控制

驾驶员、管理人员可以实时查看车辆运行情况,也可以修改系统设置以启动 / 停止视频监控。

(下转第 **10** 页)

面向业务信息安全的风险评估

位 蓓 刘松森 王自亮

(中国移动山东公司,济南 250001)

摘 要:通过比较传统信息安全评估与业务安全评估,本文介绍了业务安全评估的概念、内容,给出了业务安全评估的相关流程,并以短信业务的恶意订购流程为例,对业务安全评估进行了说明。

关键词:业务安全评估 业务流程 数据流 数据处理单元

1 引言

传统的信息安全评估,是基于资产(IT 系统和信息)的评估,即评估资产所面临的威胁和存在的脆弱性,进而分析系统存在的风险。但是这种方法不能有效发现业务层面的安全问题,例如恶意订购、垃圾短信、业务冒用、业务欺诈等。本文在传统风险评估的基础上,以业务应用为切入点,考虑各部件之间的逻辑关联性,对安全功能在促进、保障业务应用流程价值创造中的实现状况进行评价,创新性地提出了一种面向业务信息安全的风险评估方法。

2 业务安全评估概述

业务一般是指提供给客户的、有价值的服务。一种业务通常面向特定的使用对象,由一系列相互关联的业务处理活动组成。保障业务安全,旨在保证业务服务的合法、合规、可控提供,保障业务的安全、稳定运行,避免对客户和企业权益造成损害。

在信息化时代,业务是由信息系统来承载和支撑的。离开了信息系统,业务将不能存在或高效运行。业务对信息系统有一定的依赖关系。随着业务的延伸,一种业务可能是基于多个信息系统甚至云计算系统的,同时,一个信息系统可能承载多个业务服务。多个信息系统由于业务需要,通过相应的服务接口而有机地组织在一起,而一个信息系统又承载着多个业务,所以系统间的接口和互联关系是非常复杂的。

业务安全评估,是面向业务及其承载系统的一种评估方法,是以业务为中心、以业务流程和数据流驱动的一种安全评估方法。针对评估对象的评估内容,同样是风险构成的三要素,即:业务(资产的一种)、威胁和脆弱性。面向业务的风险评估实施过程如图 1 所示。

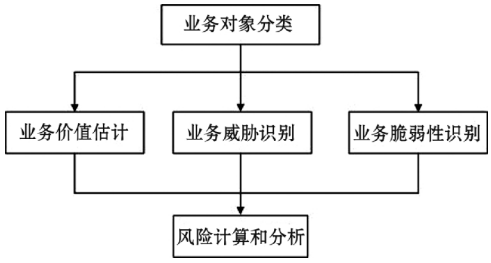


图 1 面向业务的风险评估实施过程

业务安全评估是传统安全评估的延伸和发展,包括传统安全评估的所有内容,并侧重于评估业务层面的安全风险,即关注业务流程、业务处理活动,关注业务恶用、滥用、盗用、欺诈威胁和风险等。业务安全评估与传统安全评估的关系如图 2 所示。

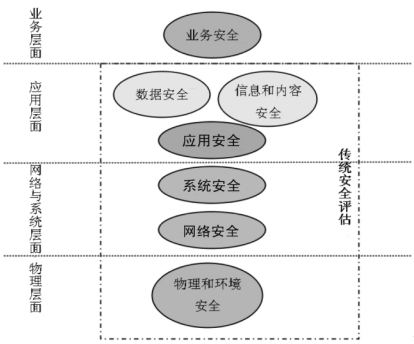


图 2 业务安全评估与传统安全评估的关系

业务安全评估以业务为中心,遵循业务风险导向的安全评估,其评估对象和内容有别于传统安全评估。

业务安全评估关注业务风险,其评估范围是:

(1)覆盖业务的全生命周期,包括业务设计与实现、业务运行与管理、业务间的接口和关联关系;

(2)覆盖信息系统的全生命周期,包括需求、设计、开发、测试、部署、运维、废弃等各个环节;

(3)覆盖业务与信息系统的承载关系,即业务在信息系统层面的数据流、数据处理活动及其关联关系;

(4)覆盖业务安全保障体系的各个方面,包括监控、保护、响应、审计等。

这些评估范围内包含了一系列的业务安全评估对象。按照业务层面,可分为业务流程、数据流和数据处理活动。其中,业务流程如彩信系统中的彩信发送流程、接收流程等,反映了端到端的业务逻辑;与业务流程并列的管理流程也是评估对象。数据流是业务流程在信息系统层面的反映,通常由一系列的数据处理活动单元构成,数据处理活动单元一般是技术评估的主要对象。按照信息系统的分层模型,可分为数据、应用、系统、网络、物理、信息和内容等。传统的安全评估侧重于数据的机密性、完整性、可用性,但对于业务安全而言,则还需要进一步考虑数据的可控性、可靠性。按照管控措施,可分为管理和技术两方面。管理方面包括业务流程、IT 管理流程、安全管理流程;技术方面包括扫描、监控、访问控制措施、审计日志等。

3 业务安全评估流程

业务安全评估的难点是理清流程,全面描述系统层面的数据流和数据处理活动单元,并对其进行深入的分析和评估。所以,其评估流程与传统安全评估稍有不同。业务安全评估流程如图 3 所示。

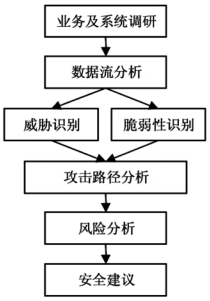


图 3 业务安全评估流程

3.1 业务和系统调研

(1)业务功能调研,业务对外表现为一系列的业务功能,因此,应首先进行业务功能的调研,即:从用户角度调研系统提供的功能以及支撑功能实现的一系列流程。例如:短信业务具有发信、收信、业务订购和取消功能,发信功能又可分为手机间发信、手机和SP间发信等。

(2)流程梳理,通常情况,广义的业务流程包括众多的业务流程、管理流程(含运维管理、安全管理),且流程间存在复杂的关联关系,需要进行梳理和分析,以便理清业务与业务流程的对应关系。

流程通常是一个端到端的服务过程,包括用户角色、活动、数据等内容。如图 4 所示。

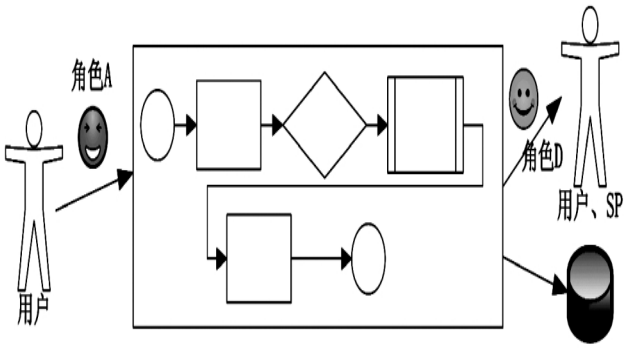


图 4 常见流程组成

明确业务与信息系统的承载关系。通常一个业务可能由多个系统承载,因此需要从业务角度出发,明确相关的信息系统,确定信息系统的调研范围。

(3)信息系统调研,主要是明确系统的组网结构、网络结构、系统结构,以及用户、访问途径、数据等构成要素。

3.2 数据流分析

(1)数据流梳理,基于业务流程,借助信息系统逻辑拓扑图,描述系统层面的业务数据流,并进行数据流的梳理,明确关键数据流。一个完整的数据流,包括访问主体及角色、访问客体、访问活动等。这些访问活动通常称为数据处理活动。

(2)数据处理活动单元分析,贯穿整个数据流,存在大量的数据处理活动,是无法在短期内高效、优质完成评估任务的,因此,需要对数据处理活动进行综合简化,即:以若干数据处理活动组合成的数据处理

活动单元作为评估的基本单位进行分析和评估。

一个数据处理活动单元，通常指完成单一功能的、密切相关的若干数据处理活动，这些数据处理活动一般存在高度信任关系。一个数据处理活动单元一般可以使用主体、客体、处理模块、参考监督模块等要素进行描述，如图 5 所示。

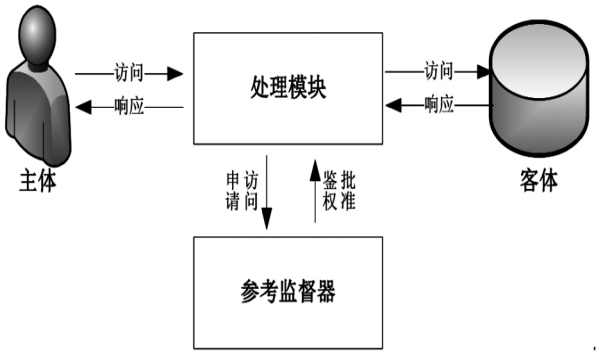


图 5 数据处理活动单元示意图

另外，还需明确每个数据处理活动单元与信息系统的对应关系，这是进行后续评估的基础。

3.3 威胁识别

在进行威胁识别时，要在业务流程、数据流、数据处理活动单元等不同层面，识别和分析业务面临的威胁。在业务流程层面，主要是流程不畅、流程失控、业务欺诈、用户假冒等威胁。在数据流层面，既要考虑正常数据流面临的威胁，也要考虑隐蔽的、非法的数据流对业务构成的威胁。在数据处理活动单元层面，主要考虑用户假冒、木马攻击、数据泄漏等威胁。

3.4 脆弱性识别

脆弱性识别是业务评估的重点和难点，主要基于业务流程、数据流、数据处理活动单元，对业务逻辑、系统自身和防护情况进行评估。

(1)基于流程和数据流的评估

基于业务流程和数据流，使用穿行测试的方法，检查业务逻辑在正常及异常情况下执行时所存在的问题。

(2)基于业务处理活动单元的评估

基于业务处理活动单元，可从业务、应用、系统、网络及数据等不同层面，分析系统存在的脆弱性。

业务层面的安全评估主要内容如图 6 所示。

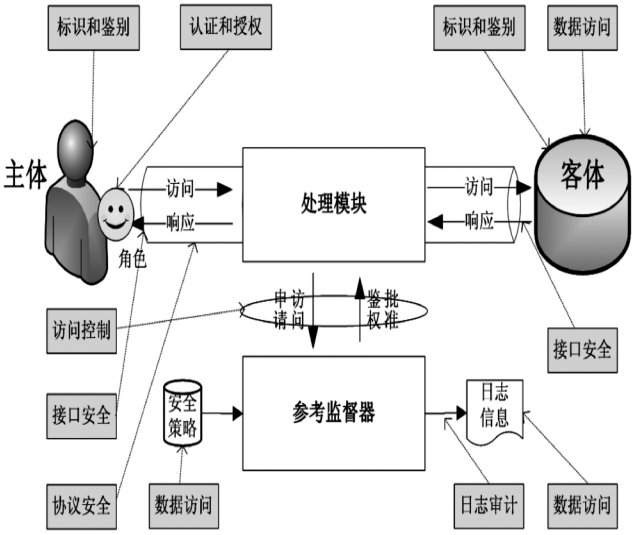


图 6 业务层面的安全评估主要内容

1)标识和鉴别：包括主体、客户及其安全等级的标识和关联；

2)认证和授权：包括鉴权绕过、鉴权失效、用户假冒、算法漏洞及角色授权等；

3)访问控制：包括权限边界、权限提升、权限制约(最小授权、分表分权)等；

4)协议安全：协议漏洞、算法漏洞等，如 WAP、GPRS 等协议漏洞；

5)监控和审计：活动的监督和批准、日志记录、数据处理活动与业务的关联分析等；

6)接口安全：如 Web Service、SOAP 等；

7)数据访问：包括服务器端、客户端的数据安全，以及内容监控检查。例如服务器端的数据创建、修改、删除、访问等，客户端包括 Cookie 修改等。

对于应用层面，安全评估的主要内容包括：系统配置(如用户管理、安全策略设置、协议配置等等)、编码(预防 SQL Injection、跨站脚本、缓存溢出等漏洞)、输入检查、错误处理等。

另外还有系统、网络等层面的评估。这些评估借鉴传统安全评估的方法和实践，以提高评估的效率和质量。

3.5 攻击路径分析

在威胁、脆弱性分析完成后,需要评估威胁与脆弱性的结合,即威胁能否利用脆弱性。如果能利用,则要深入分析业务被攻击的可能路径和危害。攻击路径分析的最终结果,必须明确是如何对业务构成影响的。为验证攻击路径假说是否存在及发生的可能性,可采用渗透测试的方法进行检验。

3.6 风险分析

与传统风险评估类似,风险分析可采用定性的方法,评估威胁所造成的客户损失、法律责任、经济损失、市场品牌损失等。

3.7 安全建议

根据发现的问题,提出相应的安全建议。例如:漏洞修补;切断攻击路径;加强审计,加强震慑;对业务运行情况进行实时监控等。

4 短信系统业务评估示例

4.1 业务和系统调研

短信系统具有的业务功能包括:发信、收信、订购、退订、计费等。

订购功能,可分为 MO 订购和 WAP 订购两种方式。MO 订购流程为:发送订购信息 > 服务商批价鉴权 > 生成订购关系 > 与 SP 订购关系库同步;WAP 订购流程为:访问 WAP 网站 > 提交订购信息 > 服务商批价鉴权 > 生成订购关系 > 与 SP 订购关系库同步。

短信功能依赖的系统包括:GSM 无线网、短信中心、短信网关,以及 GPRS、WAP 网关等。

4.2 数据流分析

基于系统的逻辑拓扑结构,其订购流程的数据流如图 7 所示。

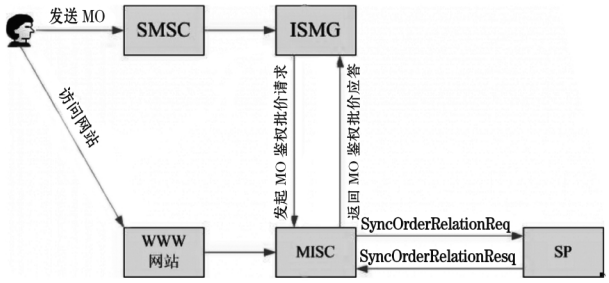


图 7 订购流程的数据流

贯穿订购数据流的数据处理活动可以采用流程图或者时序图描述,WAP 订购的数据流如图 8 所示。

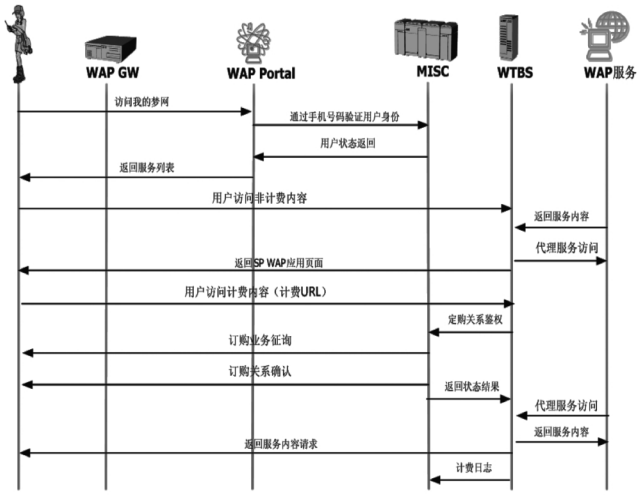


图 8 WAP 订购的数据流

分析发现,这些数据处理活动分属于不同的系统(这是由于该数据处理活动分析粒度较粗的缘故。当然,根据需要可以进行更细粒度的分析),信任关系较低,所以作为不同的数据处理活动单元进行后续分析。

4.3 威胁和脆弱性分析

订购业务的主要威胁包括:恶意订购、假冒订购等。系统存在的脆弱性包括:第三方人员具有超级用户权限、WAP 协议漏洞、终端软件控制等。

4.4 攻击路径和风险分析

(1)由于第三方拥有超级用户权限,可以上载木马、假冒用户建立业务订购关系,以谋取私利。

(2)WAP 协议漏洞，造成外部黑客可以攻击 WAP 网关,上载木马、假冒用户建立业务订购关系,

(3)客户手机终端被恶意植入木马,可以隐蔽地发起订购流程,并拦截二次确认信息,伪造确认响应,形成恶意订购关系。

5 结束语

业务安全评估是信息安全评估发展的一个重要方向,针对的是企业业务层面面临的一些安全问题。通过业务安全评估,企业能够全面、快速、有效地发现所面临的业务风险;明确风险控制策略,制定针对性的安全控制措施;推动信息安全保障体系的改进和完善。

在进行业务安全评估时,通过与传统安全评估相结合,并根据具体业务情况,对评估内容和流程进行调整和优化,可以有效提高评估的质量和效率。

参考文献

1 詹峰.一种面向业务的信息安全风险评估方法.广西科学院学报,2006(4)

2 NationalComputerSecurityCenter.Trustednetworkinterpretationofthe trusted computer system evaluation criteria[S],1987(7)

3 CarolineR.HamiltonRiskManagementandSecurity.Information Systems Security,1999,8(2):69-78

4 ChristopherJ.Alberts,SandraG.Behrens,RichardD.Pethia,WilliamR.Wilson.OperationallyCriticalThreat,Asset,andVulnerabilityEvaluation(OCTAVE)Framework[Version1.0].TechnicalReportofCarnegieMellonSoftwareEngineeringInstitute,Pittsburgh,1999.

5 ISO/IEC 15408: 2005 Information technology2 Security techniques-Evaluation criteria for IT security

(上接第 5 页)

4.3 动态信息实时掌控

实现对驾驶人员、校车的统一监控、调度和管理,提高工作效率,降低管理成本。

(1)定位监控

通过向车载终端发送呼叫指令,车载终端将定位数据进行回传、在 GIS 地图上显示,可实现对车辆的定位。定位数据包括经度、纬度、速度、方向、车辆状态等。

(2)实时调度及信息服务

监控座席可以通过电话对校车进行调度,也能向其发送调度信息。系统支持通过预设短信方式进行双向短信互动,车载终端可以上传预设好的信息至监控终端。

(3)超速报警

根据不同道路设定不同的限速值,也可实现一条道路不同路段的不同限速值。车辆超速时,系统自动报警并且以特殊标记显示超速车辆,中心及客户端都可以收到报警信息。

(4)区域报警和线路报警

校车进入 / 离开某一区域或者偏离正常行驶路线后,自动发出报警信息。该区域、行驶路线可在监控客户端设定,并且明显在地图上显示出来。

(5)遥控熄火功能

公交公司控制中心收到校车报警信息后,根据用户要求可对报警车辆下发遥控熄火命令、切断车辆电路或油路;确认报警解除后,根据用户要求或实际情况对车辆下发熄火解除命令。

(6)历史轨迹上传和回放

车载终端上存储的历史轨迹记录可以由控制中心通过无线方式按照时间段提取后存储下来,轨迹点可以在控制中心电子地图上回放以重现车辆行驶路线。

(7)手机查询

通过手机发送短信，查询指定车辆当前位置,系统将校车位置以短 / 彩信方式发回手机。

5 结束语

“移动助学”公交系统依托物联网技术、现代通信技术,将移动信息化应用在校车上,基于中国移动 3G 无线网络,利用 RFID、GPS 定位等技术,可以实时掌握校车和学生信息，为学生的安全出行提供重要支撑。

基于 BMA 安全模型的客户信息保护综述

田经师 李 斌

(中国移动山东公司,济南 250001)

摘 要:本文根据经典信息安全模型 **BMA** 模型(英国医学会模型),形成了电信企业客户信息安全保护模型,并从人员意识、保护策略、技术保障和内控体系四个方面提出了客户信息保护措施。

关键词:**BMA** 安全模型 流程优化 客户信息安全保护

1 引言

作为大众生活的重要组成部分,移动通信是私人信息传递的重要渠道之一,客户信息安全越来越受到人们的关注。目前,电信运营企业在客户信息保护方面面临着诸多挑战。本文研究的课题是客户在使用移动通信产品全生命周期过程中的客户信息保护模式:客户信息全生命周期包括入网、传输、存储、处理、消费、离网等闭环过程;以 1995 年英国医学会提出的 BMA 信息安全模型为框架,制定客户信息保护措施,分析客户信息保护的重要环节中应采取的措施,提出现阶段有效可行的客户信息保护解决方案。

2 BMA 安全模型

在许多国家,医疗资料也属于信息安全保护的范畴。个人健康信息包括一个人的健康状况、病历、治疗情况等。数据被关注并使用的可能性,取决于数据本身的价值和被访问人次,而将保存个人健康记录的数据库联网则加大了这种可能性。1995 年,英国医学协会(British Medical Association,BMA)针对国家健康服务(National Health Service,NHS)网络提出了攻击模型、安全策略和结构,从而形成了 BMA 安全模型的基础。后来由于其通用性,而在国际安全领域被定义为一种经典多边安全模型。

BMA 安全模型的主要原理,是客体同意主体可以有条件地查看并使用客体信息,并保证客体信息的完整性和可用性。

BMA 安全模型的主要规则包括:

(1)访问控制表:每一份病历记录都有一个访问控制表标记,用来说明可以读取、添加数据的人和组。

(2)打开记录:医生可以打开访问控制列表中与他有关的病人的病历,但需要经过病人委托。

(3)控制:在每个访问控制列表中必须有一个是可信的,只有他才能对病历进行写入。

(4)同意和通报:可靠的医生在打开病历时,应将访问控制列表中的名字、后续条件和隐私保密性等信息通知病人。

(5)持续性:除非已经过期,任何人都不能删除病历记录。

(6)日志:记录对病历的全部访问。

(7)可信计算:处理以上原理的计算机应该有一个有效的方法实现,实现方法需要由独立专家评估。

医疗行业保护包括纸质病历、电子病历在内的个人医疗信息的做法,是电信业客户信息保护工作的最佳学习对象;医疗记录安全保护 BMA 模型,自然适

用于指导电信业的客户信息保护。

3　客户信息系统

在电信企业中，客户信息主要包括客户基本资料、客户身份鉴权信息、客户通信信息、客户通信内容信息四大类。存储和处理客户信息的系统,包括支撑系统、业务平台、通信系统三大类。其中,与客户信息相关的处理环节包括营业、客服、营销、合作伙伴、互联网、统计分析、运行维护、开发测试等八个环节;可能接触到客户信息的人员,包括客户、内部人员、第三方人员等三大类。客户信息访问环节如图 1 所示。

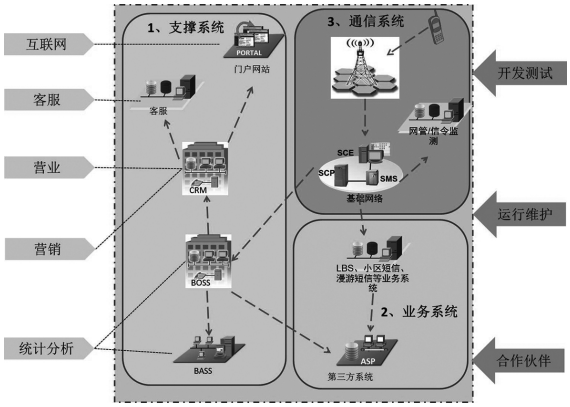


图 1 客户信息访问环节

4　客户信息安全保护模型

作为一个技术模型,BMA 主要规则集中在保护策略和技术保障的技术侧面。但是客户信息保护机制除了技术要素外,还必须考虑最关键的人员要素和建立机制的内控要素。BMA 模型与客户信息安全保护模型关系如图 2 所示。

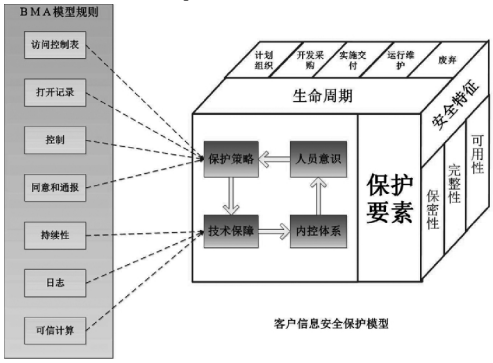


图 2 BMA 模型与客户信息安全保护模型关系

以下从人员意识、保护策略、技术保障和内控体系四个方面分别进行说明。

4.1　人员意识

(1)客户:对客户进行个人信息保密方面的培训和知识宣贯,使客户增强自我保护意识;通过营业厅、门户网站、短信、广告等多种渠道和方式,宣传企业在客户信息保护方面所做的工作,减少客户由于不明白所导致的误解、投诉等。

(2)内部员工:员工入职时,需要签订保密协议,明确员工对公司客户信息保密的法律义务;定期进行客户信息保密方面的法律法规培训和教育。

(3)第三方人员:在合同中,要与第三方厂家签订保密协议;第三方人员进入现场前,要进行相应的法律法规和管理制度培训。

4.2　保护策略

(1)访问控制

根据客户的不同类别，将客户信息进行分类;对不同类型的客户信息进行分级授权,授权依据职责分离和“知必所需”的最小化原则,将能够访问客户信息的人员范围缩至最小。

(2)信息操作原则

1)金库式管理:也称“双人操作”或“多人操作”管理。不管是前台的营业还是后台的系统维护、统计查询,对客户信息的批量操作都强制要求必须由两人或以上有相应权限的员工共同协作完成操作,通过相互监督、利益制约以确保关键操作的安全性。

2)客户授权知会原则:业务人员在访问与客户相关的详单、位置等信息时,必须事先获得客户的授权;访问后,应通过短信、邮件等方式通知客户。

3)模糊化原则:客户服务、营业办理等环节需要访问客户的基础信息时,应对显示的客户信息进行模糊化处理。譬如,对姓名,可模糊化最后一个字;对身

份证号码,模糊化后四位中的前两位。

4) 自动化原则：尽可能采用系统自动化处理方式,减少人为干预。

4.3 技术保障

技术保障主要是按照保护策略要求,有针对性地采取技术措施,限制批量操作和未授权操作,防止通过技术手段进行未授权操作或取得客户信息。

(1)物理安全:采用门禁、监控等手段,保证工作场所、客户纸质信息物理地点、客户信息相关系统物理机房的安全,严格控制出入,严禁将带有客户信息的纸质文档带离工作场所。

(2)网络隔离:对与客户信息相关的系统等进行安全域划分,并在网络边界加装防火墙、IDS 等设备,制定严格的网络访问控制策略。

(3)4A 系统：为限制非授权用户接触客户信息,原则上,涉及客户信息的支撑系统、业务平台、通信系统等应纳入 4A 系统进行集中管控。

(4)加密:数据在未授权用户可能访问的网络上传输或在不安全的系统中存储时,应该加密;关键客户信息如客服密码等在系统中存储、备份时,应该加密。

(5)数据防泄密:采用文档安全管理、终端安全管理、敏感信息监控等手段,防止文件形式客户信息的泄露,确保业务数据只保留在业务操作用的电脑上。

(6)应用安全:采用安全扫描、应用防火墙、代码检查等手段,确保应用系统的安全性,防御黑客对客户数据信息的攻击和窃取。

(7)数据脱敏:在外包时,如需把生产数据交给第三方,必须经过严格的数据脱敏过程,确保第三方拿到的数据里不包含客户的真实信息和交易记录。

(8)安全监控:通过自动化系统或人工方式,定期检查上述技术措施的有效性。

4.4 内控体系

为保证前三项控制措施的有效性,建立公司层面的内控体系,将客户信息保护工作纳入其中。

(1)规章制度:明确客户信息保密工作的范围、方法、人员职责,统一模板界面等。

(2)风险评估:定期对与客户信息相关的业务、系统等进行风险评估,梳理客户信息从登记、流转、分发到使用的数据流向及对应的业务流程,明确系统存在的风险,建立相应的控制措施,明确每个环节数据保护的责任人。

(3)外部审计:由公司审计部门或者聘请第三方专业机构，定期对公司及营业部内控情况进行检查,发现漏洞及时弥补。

5 结束语

参照 BMA 模型,建立电信企业客户信息安全保护模型;在人员意识、保护策略、技术保障和内控体系四方面制定针对性措施,严格限制接触客户信息的人员范围、数量和程度。通过技术、管理手段的综合运用,有效防止客户信息的泄露。

参考文献

1 (美)ShonHarris. CISSPAllinoneExamGuide(Fourth Edition). 科学出版社,2009

2 中国信息安全评测认证中心. 信息安全理论与技术. 人民邮电出版社,2003

3 李改成. 金融信息安全工程. 机械工业出版社,2010

MSC POOL 技术组网下局间 BICC CIC 的测算方法

尹 辉

（中国移动通信集团设计院有限公司山东分公司，济南 250001）

摘 要：本文介绍了在实际部署 **MSC POOL** 时一种计算局间 **BICC CIC** 的方法，其主要目的是防止实施 **MSC POOL** 后，由于局间 **BICC CIC** 设置的盲目性，网络资源不能得到合理利用的问题。该方法具有一定的通用性和实用性。

关键词：**MSC POOL BICC CIC** 话务模型

1 前言

1.1 BICC CIC 简介

BICC（Bearer Independent Call Control——与承载无关的呼叫控制）协议属于应用层控制协议，可用于建立、修改、终结呼叫，承载全方位的 PLMN 业务。BICC 协议是在窄带 ISUP 基础上发展起来的，应用在呼叫控制和业务承载相分离的水平网络上。核心网软交换设备 IP 化改造后，MSC Server 之间采用的协议是 BICC 协议，如图 1 所示。

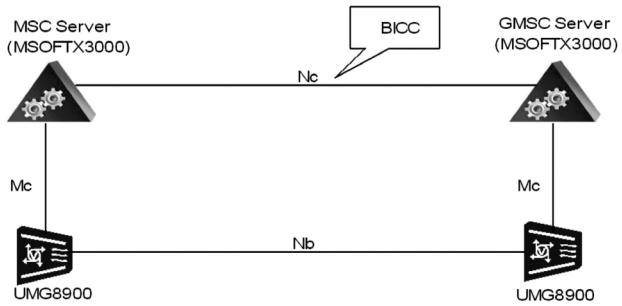


图 1 **BICC** 协议的应用

BICC 的消息格式和 ISUP 的消息格式基本相同，BICC 和 ISUP 消息中均有一个重要的参数——CIC。BICC 消息中称之为呼叫实例码，是局间呼叫关系对应的逻辑编号，指示该消息对应于哪一次呼叫实例；该 CIC 共 32bit，CIC 的最大取值 232 表示在 BICC 对等实体之间同时能够进行的最大理论呼叫数量。ISUP 消息中称之为电路识别码，用来在 ISUP 呼叫对等实体之间选择业务使用的电路；该 CIC 共 12bit，表示一条链路最多能够选择的电路为 4096 条。

1.2 MSC POOL 技术

MSC POOL 技术简称为 A - Flex (2G)或 Iu - Flex (3G)。MSC Pool 组网下，一个 BSC/RNC 通过 NNSF（非接入层节点选择功能）到 POOL 内每个 MSC Server 上信令可达，MSC Pool 中的每一个 MSC Server 共同服务于 MSC Pool 中的每个 BSC/RNC(图 2)。这种技术打破了以往 BSC/RNC 与 MSS 一对一的控制关系。

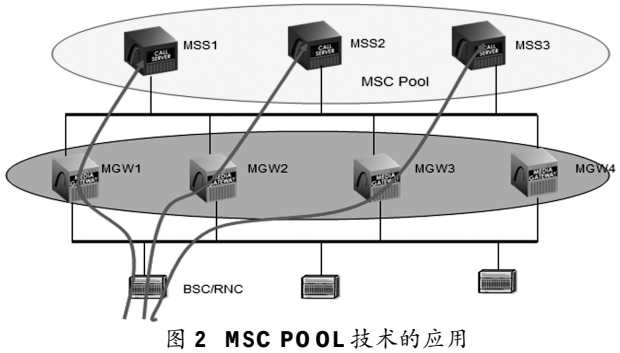


图 2 **MSC POOL** 技术的应用

MSC POOL 技术具有许多优势，譬如，由于局间切换和位置更新的减少，可以降低信令开销；端局之间实现了资源共享、负荷均衡；容灾备份保证了核心

网的安全;减少了潮汐效应的出现。

1.3 本文目的和意义

核心网设备软交换 IP 化之前,局间采用 TDM 的电路连接方式,根据话务量大小以及话务模型计算 TDM 电路的数量,从而确定 ISUP CIC 的数量。核心网设备软交换 IP 化之后,局间(MSC Server 间)信令由 ISUP 变为 BICC,移动通信本地网在设置 BICC CIC 时,一般是根据这两个局原来 TDM 所承载的电路数量通过一定转换关系进行配置,这种设置方法基本能保证话务的通畅以及网络资源的充分利用。

核心网设备 MSC POOL 技术的采用,使得局间话务量趋向于平均(话务量根据端局间的容量因子比例进行分配)。如果 BICC CIC 仍然保持组 POOL 前的值,势必造成网络资源的浪费或者话务的拥塞。BICC CIC 的设置值代表局间可以同时支持的呼叫数量:如果配置局数据时将其设置过小,当同时存在的呼叫较多时,会使新加入的呼叫无法顺利进行、多余的网络容量和带宽资源无法得到充分利用,无疑将造成浪费资源;如果设置过大,虽然可以建立呼叫,但当同时存在的呼叫所使用的资源达到设备或带宽上限时,将出现话务拥塞、用户掉话率增加的现象。

可见,MSC POOL 技术采用过程中,BICC CIC 值的设置至关重要。调研中了解到,本地网维护人员并没有掌握系统的科学设置方法,一般是根据局间的每线话务量进行设置,每线话务量超过 0.5erl 时就以 32(2 的 5 次方)作为步长增加 BICC CIC 的值,直到话务疏通正常为止。这种方法有很大的盲目性和滞后性,因此亟需一种科学的设置方法以保证局间话务的畅通。

本文着重介绍软交换核心网采用 MSC POOL 技术后对局间 BICC CIC 数量(局间呼叫数量)的影响,并对其进行测算。

2 BICC CIC 的测算思路和方法

2.1 分析话务呼叫流向

测算局间 BICC CIC 的第一步,是熟悉端局的话务流向。对于某个端局来说,其话务包括如下几个流向:

(1)本地移动的互通话务(A),其中包括本地端局间和本地端局内的话务。

(2)此端局的长途去话(B),包括外地移动用户和外地外网用户的话务。

(3)此端局的长途来话(C),只包括外地移动用户的话务。

(4)此端局的外网去话(D),只包括本地外网用户的话务。

(5)此端局的外网来话(E),包括外地外网用户和本地外网用户的话务。

综上,某个端局的话务可以归为如图 3~5 所示的 3 个模型。

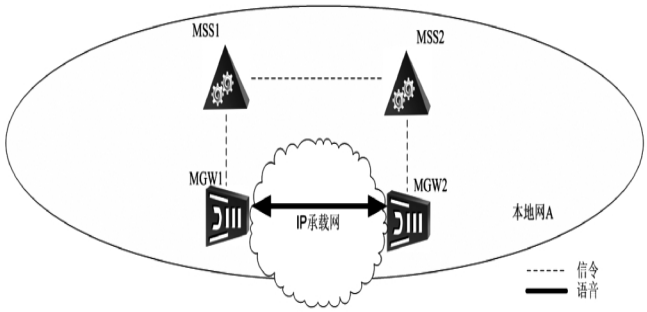


图 3 模型 1:本地移动的互通话务(针对 MSS1/MGW1,流向 1)

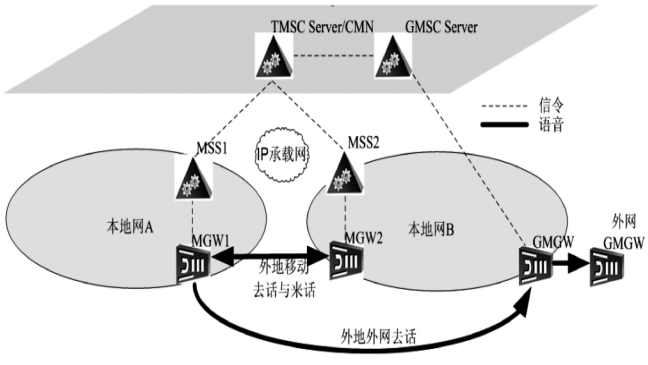


图 4 模型 2:MSS1/MGW1 的长途话务(涉及 CMN 和对端 GMGW,流向 2 和 3)

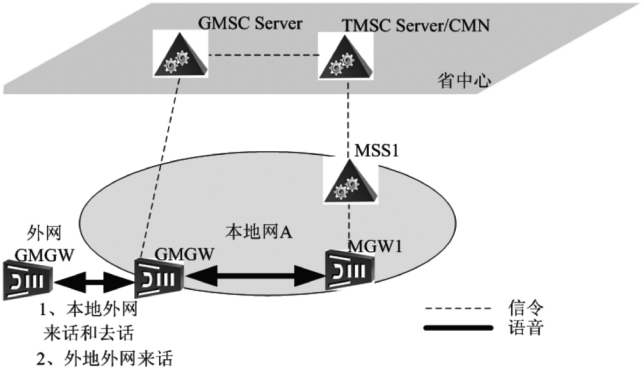


图 5 模型 3:MSS1/MGW1 的外网话务（涉及本地 GMGW,流向 4 和 5）

2.2 组 POOL 后的话务模型

实际上,组 POOL 之后,衡量话务模型的参数并没有变化,其中涉及呼叫比例的参数(其他参数不属本论文讨论范围)包括:(1)移动用户与移动用户间的呼叫比例;(2) 移动用户呼叫非移动用户的比例;(3)非移动用户呼叫移动用户的比例;(4)本地呼叫比例;(5)长途呼叫比例。组 MSC POOL 后,这些参数值将发生变化,分析这些参数的变化是计算 BICC CIC 的重要依据。首先根据 3.1 中的话务流向分析某端局的上述参数,再计算组 POOL 后的话务模型。

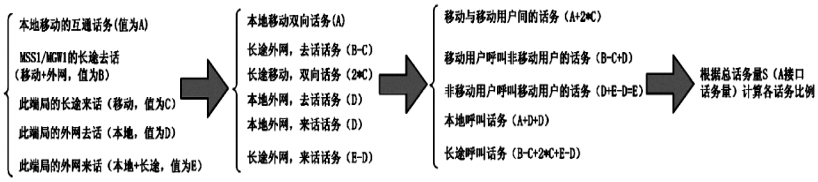


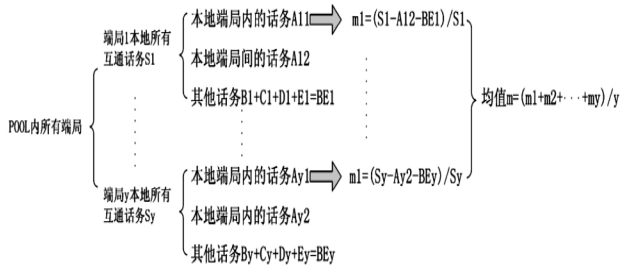
图 6 某端局的话务模型计算过程

图 6 中,A~E 的数值均可从维护人员的维护数据中直接得到。实施 MSC POOL 后,POOL 内所有端局的话务趋向平均,按照图 6 方式依次计算 POOL 内所有端局的话务模型,将所有端局的话务模型参数值求取平均值,即可得到此 POOL 的话务模型参数值。

2.3 BICC CIC 的测算

(1)中间参数需求

计算 BICC CIC 的过程中,涉及到 2 个重要的参数,其中之一是某个端局所有互通话务中其内部疏通话务的比例(设为 m),即 MSSy/MGWy 下互通的话务占其所有互通话务的比例;另外一个是 POOL 内本地移动话务量占本地移动总话务量的比例(设为 n)。根据现有维护平台中提取的数据,n 的计算较为简单,这里不再讨论;图 7 为 m 的计算过程。



注:Ay=Ay1(端局内部话务)+Ay2(端局与本地其他端局话务)

图 7 参数 m 的计算过程

(2)测算

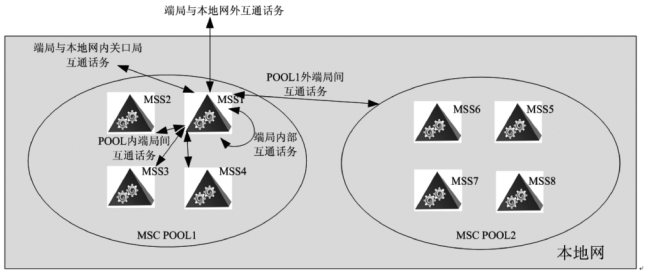


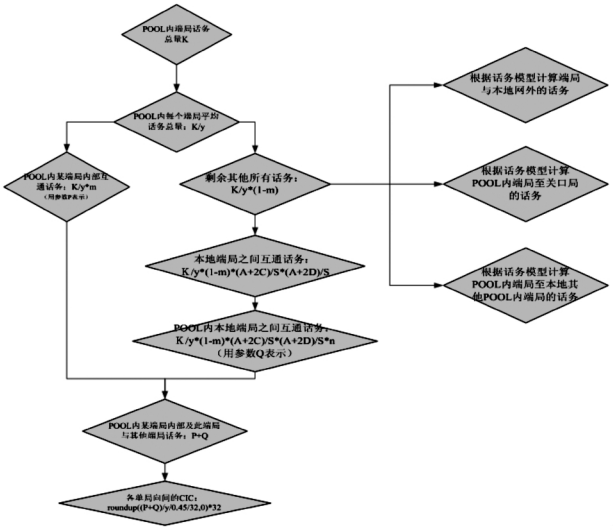
图 8 POOL 内某端局(MSS1)的话务流向

以图 8 为参考,为计算 BICC CIC,我们假设一个模型，设某本地网其中一个 POOL 内所有端局可支持的最大总话务量为 K,此 POOL 内端局个数为 y,所需要的数据参数如表 1 所示,组 POOL 后端局间 BICC CIC 测算流程如图 9 所示。

表 1 测算参数表

移动用户与移动用户间的呼叫比例	(A+2C)/S
移动用户呼叫非移动用户的比例	(B-C+D)/S
非移动用户呼叫移动用户的比例	E/S
本地呼叫比例	(A+2D)/S
长话呼叫比例	(B+C+E-D)/S
POOL 内所有端局的话务总量	K
POOL 内端局个数	y
端局内部话务与本地移动话务的比例	m
POOL 内本地移动话务与本地移动总话务比例	n

注:表中的 A—E 与图 6 中的有所不同,这里代表的是 POOL 内所有端局的平均值。



注:端局间的每线话务量不超过 0.45erl

图 9 组 POOL 后端局间的 BICC CIC 的测算流程

3 某地市 BICC CIC 的测算实例

(1)背景

某地市的端局均采用同厂家的设备,共部署了 2 个 MSC POOL,端局 GS1/2/4/6 归属于 MSC POOL2,端局 GS3/5/7/8 归属于 MSC POOL1。

(2)测算结果

根据上节提供的 BICC CIC 计算方法,测算出此地市所有端局间的 BICC CIC,并与原设置进行比较。表 2 列出了 MSC POOL2 内端局 BICC CIC 的计算结果。

表 2 MSC POOL2 内端局间 BICC CIC 的计算结果

局间 BICC CIC	实施 MSC POOL 技术之前								实施 MSC POOL 技术之后							
	GS1	GS2	GS3	GS4	GS5	GS6	GS7	GS8	GS1	GS2	GS3	GS4	GS5	GS6	GS7	GS8
GS1	-	1024	1024	1024	1024	1024	1024	1024	-	2144	1024	2144	1024	2144	1024	1024
GS2	1024	-	704	512	704	768	2560	2048	2144	-	704	2144	704	2144	2560	2048
GS4	1024	512	544	-	512	512	512	1024	2144	2144	608	-	608	2144	608	1024
GS6	1024	768	512	512	512	-	768	1024	2144	2144	608	2144	608	-	768	2144

(3)分析

1) 表中粗斜体数值是组 POOL 后 POOL 内端局间 CIC 测算调整后的结果。可以看出,实施 MSC POOL 技术之后,如果不对 POOL 内局间 BICC CIC 数量进行调整,局间互通话务将无法正常进行,势必造成不良影响。

2) 表中阴影部分数值是组 POOL 后不同 POOL 内端局间 CIC 测算调整后的结果。可以看出,若计算所得 CIC 数值比原数值偏小,原有数值可以不予调整;比原值偏大,则必须调整原值。(表中 POOL1 内和 POOL2 内端局间 CIC 应最小设置为 608。)

(4)验证

调查发现,大部分本地网维护人员是根据维护经验通过观察进行 CIC 数值的调整,其所设置的数值与上述方法计算所得的数值相差不大。运行 MSC POOL 后,端局间每线话务量的数值均在 0.2~0.4 之间,证明本测算方法合理有效,是一种科学的方法。

4 结束语

随着 3G 时代的到来,新技术的采用愈发多样化,客户对规划设计的依赖程度愈来愈高,为客户提高一种科学的维护管理方法是地市公司维护人员的必备技能。本文介绍的分析方法为地市维护人员提供了一种科学的设置 CIC 方式,在 MSC POOL 大规模实施阶段具有很好的推广意义。

参考文献

1 中国移动通信集团公司.中国移动 MSC POOL 技术规范,版本号:V1.0.0

2 张斌彬.交换协议的比较及发展趋势.科技情报开发与经济,2005

3 尼松涛.软交换协议在中国移动长途网的应用.现代通信,2006

4 侯颜平. BICC 协议及其在 NGN 中的应用.电信交换,2011

WLAN网络建设中的关键问题探讨

王少波 阎成刚 纪 芳 付宏志

（中国移动通信集团设计院有限公司山东分公司,济南 250001）

摘 要:近年来,随着数据业务的迅速发展和运营商之间的全业务竞争,**WLAN** 日益成为网络建设的重点。本文基于现网实际,对 **WLAN** 网络建设中的关键问题进行了探讨,以期为后续的建设提供参考。

关键词: **WLAN AP AC BRAS**

1 引言

随着手持智能终端和笔记本电脑市场的快速发展,无线上网客户增长迅速,宏网络面临越来越大的压力。而目前 TD-SCDMA 网络尚未充分发挥业务分流作用,因此需要寻找一种低成本接入方式以卸载流量。

WLAN 技术在高带宽、成本廉价和应用普及等方面具独有优势,特别是在全业务竞争环境下,一方面可以有效缓解宏网络扩容的压力，降低投资成本，另一方面能在一定程度上弥补中国移动有线宽带接入能力的不足,有利于宽带市场的发展。基于上述原因,中国移动开展了 WLAN 的大规模建设。

2 WLAN 网络架构

WLAN以无线多址信道为传输媒介,利用电磁波完成数据交互,实现传统有线局域网的功能。WLAN 主要由 AP 实现无线接入,AP 通过传输网络连接至 AC/BRAS，由 AC/BRAS 进行业务接入控制。随着 WLAN网络建设的展开，其标准和产品日见成熟，WLAN 正逐渐向运营网络方向发展，其网络架构如图 1 所示。

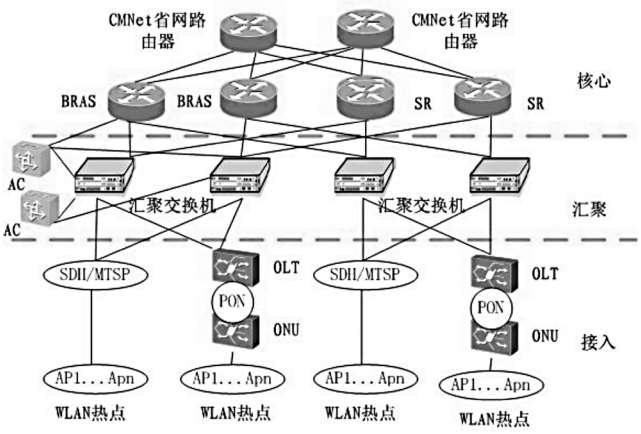


图 1 **WLAN** 网络架构

3 WLAN 网络建设中的关键问题

3.1 频率规划

在 WLAN 的网络建设中，频率规划是一个非常重要的环节。目前,中国移动 WLAN 主要使用 IEEE 802.11g 和 IEEE 802.11n 标准的设备进行组网。IEEE 802.11g 工作在 2.4GHz 频段，频率范围为 2.400GHz～2.4835GHz,信道宽度为 20MHz,最多有 3 个互不干扰的信道。IEEE 802.11n 工作在 2.4GHz 频段和 5.8GHz 频段，其中 5.8GHz 频段的频率范围为 5.725GHz ～5.850GHz，共定义了 20MHz 和

40MHz两种信道宽度,可以最多划分为 5 个互不干扰的信道。

2.4GHz 频段和 5.8GHz 频段的信道划分如图 2 所示。

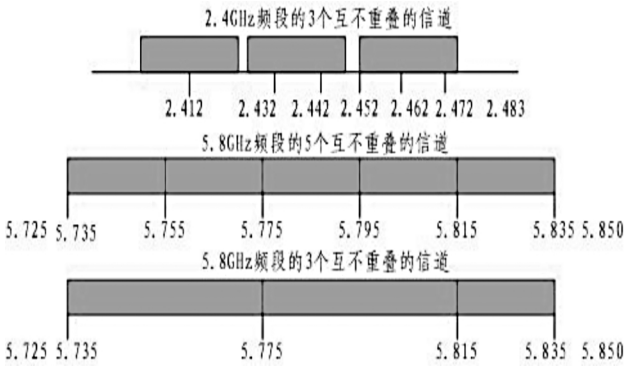


图 2 2.4GHz 频段和 5.8GHz 频段的信道划分

在 2.4GHz 频段，最多可以提供 3 个互不干扰的信道。考虑制式的兼容性,推荐频段为 1、6、11。为降低干扰源的影响,应尽可能将两个相邻放置的 AP 设置在频率不相交叠的信道上,当室内隔断不规则分布时,应依靠隔断物划分覆盖区域,减少同频干扰。

2.4GHz 频段和 5.8GHz 频段在我国是公共频段,所以干扰问题不可避免。功率较大的其他 WLAN 设备(如微波炉等)主要工作在 2.4GHz 频段,且 5.8GHz 频段的频谱资源远较 2.4GHz 频段丰富，因此就干扰程度而言,5.8GHz 频段明显小于 2.4GHz 频段。

为有效提高网络质量，提升市场竞争力,在 WLAN 网络建设中，特别是在 802.11n 的建设中,应重点考虑 5.8GHz 频段的使用。在干扰较少的区域,建议采用两个 40MHz、一个 20MHz 频段的组网方案;在干扰较大的区域，可以采用 5 个 20MHz 频段的组网方案。

3.2 AC 的建设模式

随着 WLAN 网络建设的不断拓展,AC 作为重要网络设备，其建设模式的选择对网络的影响越来越大。AC 主要有以下三种建设模式:

(1)小规格 AC,含简单认证功能。

(2)AC 与 BRAS 分别设置，实现 AC 与 BRAS 的专业化分层管理,AC 不含认证功能，由 BRAS 实现 WLAN 和宽带用户的统一认证、计费。

(3)BRAS 集成 AC,完全继承成熟的宽带业务。

AC 三种建设模式的比较如表 1 所示。

表 1 AC 的建设模式比较

	模式 1: 小规格 AC	模式 2: BRAS/AC 分设	模式 3: BRAS 集成 AC
优点	适合建网初期, 小规模组网	AC容量大, 适合大规模组网, 继承运营级 宽带业务	减少网络节点, 减少流量迂回, 符合网络扁平化 演进趋势
缺点	AC 数量多, 维护量大, 无法满足运营级 宽带业务要求	存在流量迂回, 较模式 3, 网络结构 略显复杂	现网改造大, AP 与 BRAS/AC 间 存在厂家壁垒

考虑到维护的工作量和网络的可扩展性，建议 AC 采用大容量、少局址方式进行部署,即采用模式 2 建设方式,同地市尽可能部署同厂家 AC 设备,最多不宜超过三家。至于模式 3,虽减少了网络节点,符合网络扁平化演进趋势，但由于 AP 与 BRAS/AC 间存在厂家壁垒,接口规范方面还需做进一步研究。

3.3 数据流向

WLAN 在转发数据时，分为集中转发和本地转发两种模式。采用集中转发模式时,用户数据都要通过 AC 进行集中交换;采用本地转发模式时,AC 只对 AP 进行管理和控制，本地用户数据无需通过 AC 进行转发。在网络建设中,选择何种转发模式是一个必须考虑的问题。

采用本地转发,最大的优势是减少了本地用户数据流量的迂回,但在用户漫游时,若用户 IP 归属到不同的网段,业务就会中断,势必影响用户感知。而采用集中转发,统一由 AC 来管理用户的网段,能够有效实现各种跨三层漫游的无缝切换。另外,集中转发模式下 AC 还可以对流量进行限速、计费、负载均衡等多种智能化处理,而且由于采用隧道技术,对用户 IP 的分配也更加灵活。因此,我们认为 AC 支持集中转发是电信级 WLAN 精细化业务控制的基础。

在 WLAN 现有网络中，由于厂家的支持情况不

同,同时存在集中转发和本地转发两种模式。在下一步的建设中,考虑到投资、维护等因素,建议现有网络的转发模式不变;对于新建的 WLAN 设备,优先采用集中转发模式。两种模式的数据流向如图 3 所示。

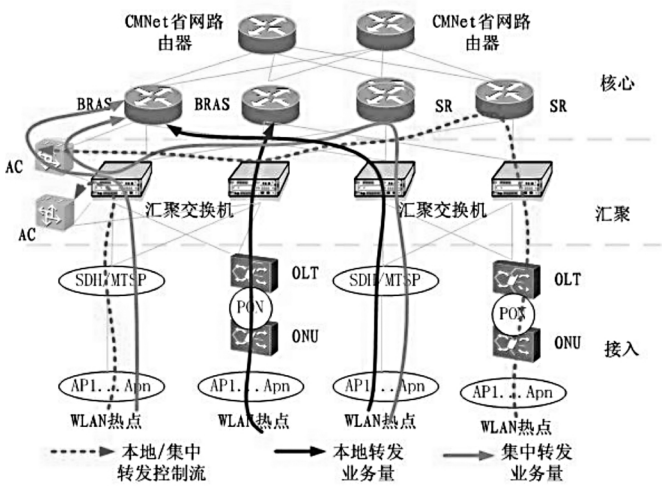


图 3 两种模式的数据流向

若汇聚交换机与 AC 位于不同的机房,之间没有直连线路,部分数据流需要进行转接。由于 SR 的投资要低于 BRAS 的投资,建议由 SR 转接汇聚交换机与 AC 间的数据流。

3.4 WLAN 与移动网络的融合

网络融合是现代通信网络演进的一个重要方向,WLAN 网络与移动网络的融合,可以有效加强用户管理,挖掘业务潜力,并充分利用 WLAN 网络的高带宽优势,实现对热点区域数据流量的有效分流,从而提高数据业务的投资回报比。WLAN 与移动网络融合也是近年来业界研究的一个热点。

WLAN 与移动网络融合可以分为统一认证、深度融合、业务连续三个演进阶段。网络融合中,终端适配是最大的一个问题,终端需支持 IPSec 等协议,需对现有协议栈进行改造。另外,现网中终端类型众多、数量庞大、标准不一,这些都为终端适配增加了难度。目前中国移动正在进行 LTE 试验网的建设,相应标准也日益成熟,建议以 LTE 建设为契机,重点加强 WLAN/LTE 融合终端的研究,制定系统的标准规范,切实解决终端适配的问题,从而真正体现网络融合的优势。WLAN 与 LTE 网络融合的目标架构如图 4 所示。

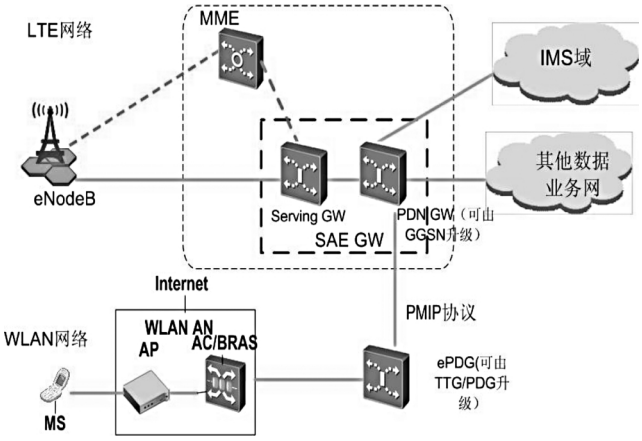


图 4 WLAN 与 LTE 网络融合的目标架构

4 结束语

WLAN 是中国移动“GSM+TD+LTE+WLAN”四网协调发展和“无线 + 基站光缆延伸 +IP+IMS”全业务网络发展策略的重要组成部分,是分流蜂窝网络数据流量和支撑宽带接入的有效手段。本文对 WLAN 网络建设中的频率规划、AC 建设模式、数据流向、网络融合等关键问题进行了探讨,并给出了相应建议。随着 WLAN 网络建设的不断拓展和 WLAN 技术的日益完善,人们必将越来越多地感受到它所带来的影响。

参考文献

1 马向辰,刘海平,于晓冰. WLAN 802.11n 组网规划相关问题研究. 电信工程技术与标准化,2011(04):1～6

2 戴伟霞,林璐. 电信运营级 WLAN 网络建设探讨. 广东通信技术,2011(03):50～55

3 3GPP TS23.236: Intra-domain connection of Radio Access Network (RAN) nodesto multiple Core Network (CN) nodes

3G 基站 PS 域上网业务 IP 化改造实施

白京春 戚均乐

(中国联通威海市分公司,威海 264200)

摘 要:本文介绍了采用 **IP** 承载网传送移动网 **3G** 基站 **PS** 域业务的实现原理,以期为 **3G** 基站网络部署和优化提供参考。

关键词:**3G** 基站 **PS** 域 **IP** 承载网 **VRRP** 主备保护

1 引言

某本地网最初几年的移动网 3G 基站规模建设,全部通过传输网承载。但随着业务发展,为解决 3G 基站的覆盖问题,计划规模布放室内分布(BBU)基站,需要按每台 3G 基站的上行带宽为 4*2M 捆绑方式(基站的无线带宽可达 28M)对本地传输网进行扩容,面临以下问题。

(1)传输资源不足

因传输网资源已经非常紧张,如接入大量的室分和新扩基站,势必要对现有的传输网(尤其是汇聚层以上网络)再次进行大规模扩容。而且随着 3G 用户的增多,现有基站上行带宽(8M)也会很快不能满足业务需求。带宽扩容是必须实施的。经过测算,按某本地网现有传输网络,必须再投资上千万元扩容,才能满足每个 3G 基站点 28M 的 PS 域传输带宽需求。

(2)RNC 和传输之间无保护

所有移动网 3G 基站的 PS 域业务,通过传输汇聚,汇总到多条 GE 上,再连接到 RNC。每台 3G 基站都与 RNC 的一个端口绑定,没有保护。当传输与 RNC 之间的中继出现故障时,所有 RNC 端口上所连接基站的 PS 域业务都会中断。

(3)网络扩展性差

3G 网络快速扩容和深覆盖需求,要求承载网具备良好的可扩展性,以支撑快速部署 3G 网络。传输网 SDH 技术作为底层电信级传输平台,侧重点是简单高速的数据传送和传输电路的保护,并且采用传统 TDM(时分复用)技术,因此无法满足 3G 网络快速发展的需求。

为解决上述问题,经多方论证,制定了 3G 基站 PS 域上网业务通过本地承载网实现 IP 化传送的方案。2011 年组织对现有 3G 基站业务传送网网络进行了 IP 化改造,历经半年多时间,将本地网 3G 基站接入全部调整为 IP 承载网传送。

2 IP 化改造方案

2.1 网络架构

如果本地承载网覆盖范围充足,可以将 3G 基站通过接入交换机直接上联至承载网。若承载网覆盖范围有限,以将 3G 基站经过边缘传输设备汇总后,再接入承载网的接入交换机。可以根据传输网络和基站分布情况,确定 3G 基站汇聚节点。将 3G 基站经就近

传输网络汇聚后,再接入本地承载网(图 1)。

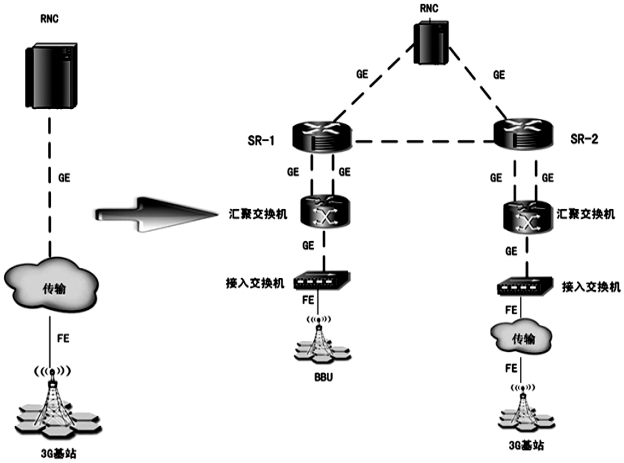


图 1　基站上联传送网改造前、后示意图

(1)确定汇聚节点,规划汇聚节点上联的本地承载网设备和端口,调度光路,完成网络架构规划和建设。需要规划所有基站的汇聚节点,并根据基站数量配置边缘传输资源。

(2)室内分布站,不经过传输设备接入,就需要确定室分站的汇接点,布放接入交换机汇总后,再就近接入到承载网上。

2.2　资源规划

对基站设备,采用每基站一个 VLAN、一个网管 IP 的资源分配方式。

(1)为传输网络的每个汇聚节点分配外层 VLAN;

(2)规划基站的传输端口和内层 VLAN;

(3)室分 BBU 节点,直接上连到承载网交换机上,分配内层 VLAN;

(4)通过 SUPER－VLAN 指定的方式,分配基站的 IP 地址。

2.3　基站带宽

若采用传输网传送,受资源所限,每个 3G 基站一般分配 4*2M=8M 带宽,并且从基站到 RNC 设备会占用传输网的全程带宽。而采用承载网改造后,每台基站的带宽可以达到 28M。

2.4　主备切换

为提高移动网络安全性,可以在无线网 RNC 和承载网业务路由器 SR 之间启用业务保护。以华为移动网 RNC 设备为例,可以采用 VRRP 的主备切换方案(图 2)。

(1)VRRP 主备切换方案

1)RNC 配置主备板卡保护;

2)2 台 SR 路由器配置 VRRP 组与 RNC 对接,VRRP 组配置采用主备方式;

3)因 RNC 主备板卡之间完全隔离,VRRP 心跳只能走在路由器之间;

4)2 台路由器之间应配置足够容量的链路,并配置跨板卡 LAG 保护。

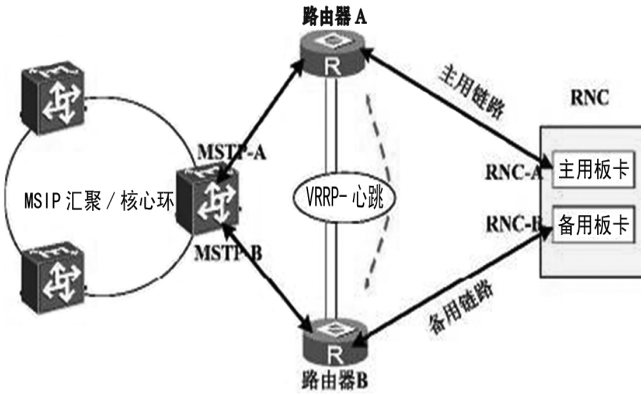


图 2　VRRP 保护方案示意图

如图 2 所示,当为移动无线网 RNC 设备配置 VRRP 时,需要对 SR 路由器与 RNC 之间的互联端口做 TRACK。

由于 SR 路由器需要配置静态路由指向 RNC,主备路由器上的静态路由都会发布到全网中(不是只发布主路由器的信息),有可能导致路由问题。

为解决主备路由器的静态路由同时发布问题,组织对 SR 与 RNC 之间 BFD 功能进行测试。将静态路由与 BFD 绑定,可以成功地避免此问题。但 VRRP 方式仍然存在下列潜在安全隐患:

1)协议可靠性低,存在因协议本身运行不正常而导致网络故障的风险;

2)存在两台 SR 之间的 VRRP 心跳链路发生故障,导致全部业务中断的重大风险。

(2)路由主备切换方案

深入研究华为 RNC 设备的主备机制后,在网络架构不变且不增加任何投资的情况下,提出纯路由的解决方案:

1)两台 SR 与 RNC 互联中继数据可以进行完全相同的配置,同时启用 BFD 协议,与指向 RNC 设备的静态路由做绑定;

2)正常情况下,RNC 设备备板因无数据配置,所以在 BFD 协议作用下,静态路由不会生效,不会导致路由混乱;

3)两台 SR 上互联中继的配置虽然一样,路由会同时公布,但因互联中继的 IP 不会被作为目的路由寻址,也不会影响业务;

4)经过测试,主备切换的时长在 1-10S 之间,完全满足业务需求。

2.5 改造后的优点

3G 基站 PS 域业务传送网实施 IP 化改造后,对网络安全产生如下良好效果:

(1)减轻核心、汇聚层传输网的带宽压力

可以避免核心、汇聚层传输网的不断扩容,并为宏基站承载更高速率数据业务提供了更大带宽,并且扩容非常便利。

(2)节省 MSTP 接入传输设备的资金投入

部分接入点的原传输设备不支持以太网业务传送。采用 IP 化承载后,可以直接开通数据业务,无需重建传输设备及相关配套投入。

(3)提高汇聚传输设备利用率

若通过原来的传输汇聚节点接入大量 3G 基站,汇聚机房的传输设备至少需要为每个基站提供以太网口,即传输设备需要配置大量以太网板卡,并且占用多个设备槽位,将严重影响可以下挂的环网数量,造成汇聚设备利用率极低。而采用 IP 化承载后,可以大大提高汇聚传输设备的利用率。

(4)优化 CS 域架构

可以节省传输设备,将有限资源用于 CS 域网络优化,进一步提高 3G 语音网的安全性。

3 技术创新点

本方案实现了移动无线网 RNC 设备和 IP 承载网 SR 业务路由器之间的路由自动主备切换。原来设备厂家提出的在 RNC 和 SR 之间采用 VRRP 协议的备份方案,容易导致网络配置复杂,引入新的故障点;并且在 VRRP 心跳线发生故障时,存在分组域全业务中断的重大网络隐患。本文所述 IP 承载网纯路由解决方案,可以在不增加更多投资的前提下,实现在 1-10S 之间(受限于 RNC 主备卡切换时间和 SR 的路由重收敛时间)的有效切换目标,大大提高网络健壮性和可扩展性。

4 结束语

随着 3G 移动网络的迅猛发展,数据业务的带宽需求、MSTP 传输网的扩容压力都将越来越大。本文介绍了移动网 3G 基站 PS 域业务 IP 化传送的可行性方案,并且在某本地网全面实施后,3G 基站带宽得到有效提升,网络健壮性也有了很大提高,预计可以节省上千万元投资,对于推动移动网络建设和优化有着积极的借鉴意义和参考价值。

CDMA网络山区模式的城区导频污染问题处理方案及实施

陈百鹏[1] 李 模[2]

(1 中国电信集团公司,北京 100010
2 中国电信临沂分公司,临沂 276000)

摘 要:本文以承德大桥导频污染问题的处理过程为例,介绍了单 **PN** 分析法、大电调天线、天线屏蔽罩等在 **CDMA** 网络优化中的应用,验证了优化效果,总结了山区模式的城区导频污染问题处理经验。

关键词:**CDMA** 山区模式 城区 导频污染 处理

1 引言

承德市区四面环山,以老城区为核心,逐渐南扩北延,形成了带状的城市空间结构布局;市区有河流穿过,地域特色显著。另外,市区分布较多的高山站,无线信号越区覆盖加上信号在水面的镜面反射,导致滨河路、跨河大桥区域出现了较为严重的导频污染。

本文选取承德市区导频污染问题最为严重的区域——承德大桥作为优化试点,探讨适合的导频污染问题处理技术手段,实施效果表明,可以在后期优化中推广。

2 承德大桥导频污染问题分析

承德大桥 CDMA 网络信号杂乱,周边基站的越区信号非常多,属于典型的导频污染。路测数据显示,该区域内导频强度小于 -12dB 的比例为 9.13%。针对城区高站多且有河流穿过的特点,我们确定了导频污染问题的处理思路:

首先,改造不合理的天线参数设置,根据射频覆盖区域的网格化,合理设置天线下倾角和方位角。

其次,通过电调天线和大电调天线的使用,减少因天线机械下倾角过大而导致的天线波形变形引起水平越区覆盖,减少因机械下倾角过大而导致的垂直上旁瓣越区覆盖。

最后,为基站天线增加隔离罩,改造天线波形,减少水平波瓣的宽度,消除水平旁瓣的影响,减少河面传播环境的负面影响。

3 承德大桥导频污染问题处理方案实施

3.1 常规 RF 调整,合理规划基站的天线参数

第一步,根据路测采集的数据,分析 Max_Ec/Io、Serving 或 Active_pilot 等指标,提取覆盖该区域的 PN 所对应的基站,主要有新华书店、承德宾馆、工商银行、卫校、乾阳酒店、新华园、天宇饭店等。

第二步,对以上基站进行现场勘查,发现部分基站的天线存在 2 扇区方位角夹角太小、俯仰角设置太大或太小等问题。对设置不合理的扇区现场都进行了整改,如表 1 所示。

表 1 承德大桥周边基站天线调整列表

基站名称	扇区	原方位角	原下倾角	新方位角	新下倾角	备注
新华书店	1	20	12			
	2	110	12		14	
	3	270	11			
工商银行	1	40	11	20		
	2	180	8	160		内置 6 度
	3	275	6	250		
卫校	1	65	14			内置 8 度
	2	170	11			内置 8 度
	3	305	13			内置 8 度
承德宾馆	1	5	15	345		内置 3 度
	2	70	12		15	内置 6 度
	3	125	15	200		内置 9 度
乾阳酒店	3	330	8		10	内置 3 度
新华园	2	175°	6		9	
天宇饭店	1	115°	4		7	内置 3 度

第三步,调整完成之后,对问题区域进行复测,显示:乾阳酒店 3 扇区、新华园 2 扇区、天宇饭店 1 扇区的信号得到了控制;而新华书店基站 2 扇区和卫校基站 1 扇区的越区信号仍然比较强。新华书店基站 60 米高,卫校基站是高山站、超过 100 米,由于这两个扇区的俯仰角都已经在 10 度以上, 所以为防止波瓣变形,不能再通过加大机械倾角方式来达到控制信号的目的。初步计划将新华书店 2 扇区天线更换为大电调天线,为卫校基站 1 扇区天线增加屏蔽罩以对信号进行精准控制。

3.2 大电调天线的应用

天线的波形不理想以及传播环境形成的传播模型对波形的改变,是射频优化中的最大困难。使用大电调天线(内置角度调整范围在 10 度到 24 度的电调天线)是种较好的优化方式。

(1)大电调天线的作用

使用大电调天线, 可以增大可调电子下倾角,减少大机械下倾角的使用,从而改善由于机械下倾角过大而产生天线辐射波形变形引起的水平越区问题;可以增大总下倾角,从而减少垂直越区。

(2)新华书店基站 2 扇区使用后效果

本次优化中,对新华书店 2 扇区使用了大电调天线。测试对比显示,大电调天线能够有效地减少和控制水平越区及垂直越区,提高导频的纯净度,如图 1 所示。

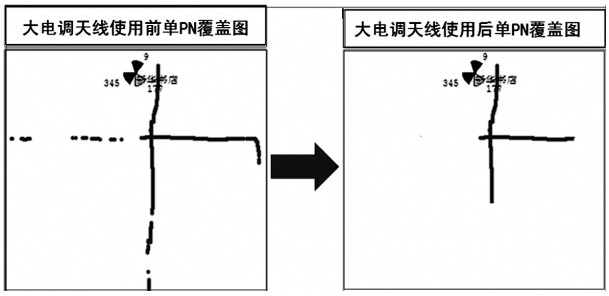


图 1 新华书店 2 扇区大电调天线使用前、后单 PN 覆盖图

3.3 天线隔离罩的应用

承德城区无线传播模型的特殊性,对现网的天线性能提出了更高要求。为有效提升天线水平波瓣的方向性性能,减少由于水平主瓣或旁瓣控制不好所导致的水平越区覆盖, 在现网中还没有成熟产品的情况下,尝试使用了天线隔离罩。

(1) 天线隔离罩的原理

当电磁波到达屏蔽罩表面时,由于空气与金属交界面上阻抗的不连续,对入射波产生反射。当金属网孔径小于电磁波长的 1/4 时, 电磁波较难穿透金属网。电磁波发射到天线隔离罩表面时,低电阻率的金属材料由于电磁感应作用产生涡流,形成对电磁波的抵消作用,从而达到吸收射频信号的效果,在移动通信中类似于对天线波形产生了隔离。目前 CDMA 网络使用的电磁波频段在 800~900Mhz 之间, 波长为 0.33~0.375m,所使用铁丝网的孔径约为 1cm 左右,远远小于电磁波波长,对该频段的电磁波有较好的屏蔽作用。

(2)天线隔离罩的使用

鉴于其他 CDMA 网络使用天线隔离罩中遇到的问题,决定使用双层不同尺寸的隔离网(表 2),为卫校基站进行安装。

表 2 天线隔离罩制作参数表

参数	内容
整体尺寸	长度稍微长于天线,宽度大约为天线支撑宽度的2倍
网线材料	角钢
外层网孔要求	10mm 镀锌网
外层网线尺寸	1mm
内层网要求	针眼不锈钢筛网
安装要求	紧贴天线,避免信号泄露;安装牢固;角度可调。针孔网朝向天线。
网线层数	双层

使用该种天线隔离罩后，隔离性能大大提升,水平方向的信号能够达到理想的控制范围内,如图 2 所示。

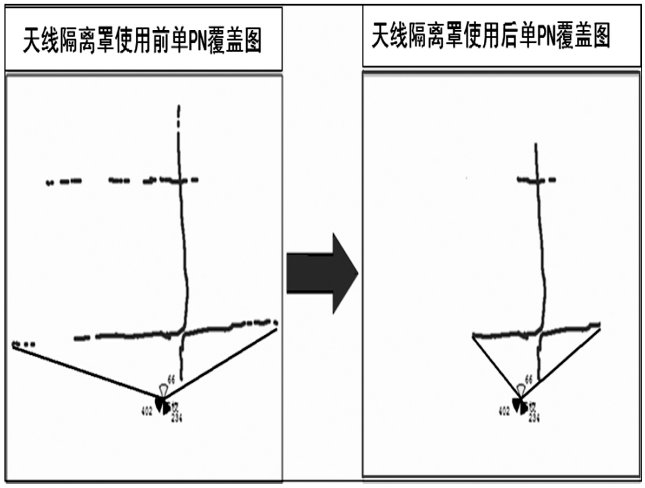


图 2 天线隔离罩使用前、后单 PN 覆盖图

通过试验,说明使用隔离罩能够改造天线的水平波瓣,抑制水平波瓣干扰。

(3) 总结

天线隔离罩可以使用在射频中由于天线水平波瓣受传播环境影响而导致的水平越区场景和控制天线信号水平覆盖范围的场景;要求天线安装平台有足够的容纳空间。

从本次试验看,天线隔离罩经过改造,性能得到了一定提升,说明天线隔离罩的合理使用能够对射频优化产生较好的辅助作用。另一方面,天线隔离罩的制作、安装等均还存在较大的改进空间。

3.4 处理方案整体实施效果

(1) 路测指标对比(图 3)

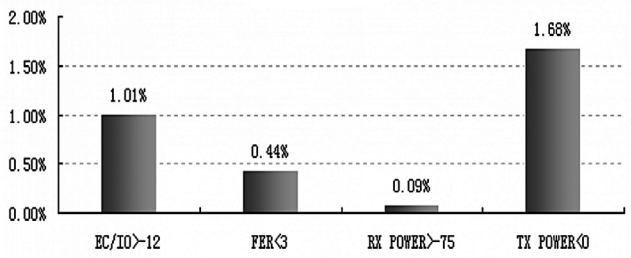


图 3 优化后路测指标提升情况

(2)KPI 指标对比(图 4)

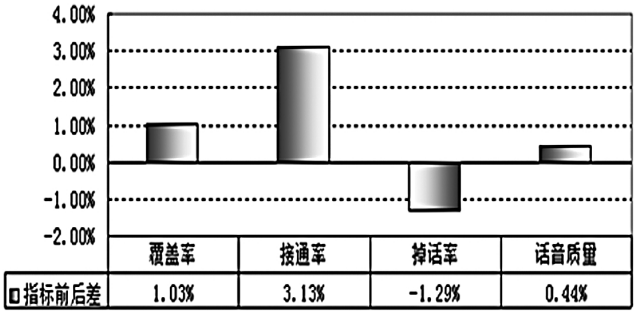


图 4 优化后 KPI 指标改善情况

4 结束语

借助单 PN 分析法开展了大量的射频优化工作,并应用了大电调天线、天线隔离罩等技术手段。优化后，承德大桥区域的导频污染问题有了明显改善,说明本次优化使用的技术手段在处理山区模式的城区导频污染问题时是有效的,可以在后期优化中推广使用。

参考文献

1 万晓榆等.CDMA 移动通信网络优化.人民邮电出版社,2004

2 华为技术有限公司.cdma20001x 无线网络规划与优化.北京:人民邮电出版社,2005

3 中国电信集团公司无限网络优化中心.中国电信 CDMA 网络高层导频污染优化方案,2009

山东联通档案管理系统信息安全研究

张 奎 宋秀梅

（中国联通山东省分公司，济南 250001）

摘 要：本文分析了涉及档案管理系统的信息安全风险，介绍了山东联通档案管理系统建设中加强信息安全防护的要点和措施，以期对档案管理系统建设及信息安全防护的深层次研究有所裨益。

关键词：档案管理系统 信息安全 数据存储

1 引言

档案信息的数字化、网络化和开放化，在为档案使用者带来快捷、便利的同时，也给档案管理工作构成了巨大的挑战。由于计算机网络的开放性和共享性，使计算机网络的接入变得十分容易，而电子档案对计算机及网络的依赖，使威胁档案信息安全管理的因素变得非常多。如何确保网络环境下的档案信息安全，是档案管理工作面临的重要课题。

目前，国内外档案馆的电子档案信息安全防护措施普遍存在手段单一的问题，大多是简单采用防火墙等有限措施来保护系统主机和网络安全。这些措施有很大的局限性，不能覆盖档案信息安全管理的各个层次和方位，档案管理人员无法了解系统潜在的漏洞和存在的风险，只能采取被动防御方式，而缺乏主动防御能力。

另外，随着我国电信体制改革的日益深化，企业内外部环境发生了一系列变化。从外部看，竞争愈发激烈，并逐步由单一化竞争向全方位竞争转变；从内部讲，企业的融合重组、机构人员的重新整合、工作流程的优化再造、项目建设的不断增加、协议合同的大量使用，都要求企业持续提升精细化管理水平。这些变化不仅为档案资源带来了种类、数量的激增，也给档案信息安全防护形成了新的挑战。因此，从全局高度、整体考虑档案管理系统信息安全防护就显得尤为重要。

2 山东联通档案管理系统概况

多年来，山东联通档案工作一直紧跟科技发展步伐，在档案管理信息化建设方面进行了有益的探索，取得了长足的进步。早在 1992 年，便开始在档案工作中引入计算机管理。1996 年，实现单机版档案管理系统。2001 年 3 月，启动基于网络的档案管理系统建设，并在 2005、2007、2009 和 2011 年，分别进行了四次较大规模的系统优化升级与安全加固，现已建成全省统一、基于企业内部承载网络（以下简称 DCN 网），覆盖省、市、县三级档案馆（室），集成文书、科技、会计、合同、声像、实物等资源的档案管理系统，实现了档案管理的数字化、标准化和网络化，有效促进了企业管理现代化水平和档案信息安全防护等级的提升。

2006 年，山东联通参与起草了《山东省数字化档案馆建设规范》、《山东省数字化档案室建设规范》等省内标准。2007 年，山东联通作为省内唯一企业代表，接受了国家档案事业发展综合评估组的评估检查，得到了评估组的充分认可。2008 年，国家档案局

调研组到山东调研,对山东联通的档案管理工作给予了高度评价。2010 年,山东联通《通信企业档案信息化管理体系的构建与实施》荣获山东省 2010 年度档案学优秀成果一等奖和山东省企业管理现代化创新成果一等奖。2011 年,《山东联通档案管理系统建设中信息安全研究》荣获国家档案局优秀科技成果二等奖。

山东联通档案管理系统由系统管理、核心功能与核心应用等三个子系统组成,其中,核心功能子系统包括档案数据采集与加工、档案数据存储与管理、档案数据查询和档案数据利用等功能模块。其网络拓扑图如图 1 所示。

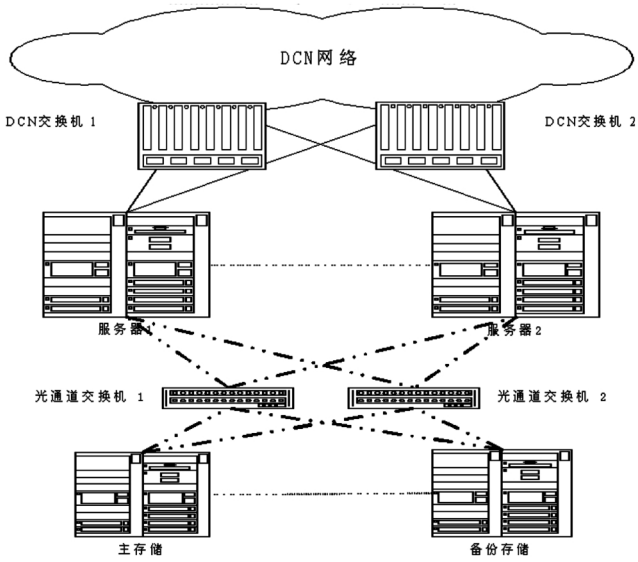


图 **1** 山东联通档案管理系统网络拓扑图

3 山东联通档案信息安全防护要点

按照 IT 信息系统的生命周期规律, 档案管理系统信息全防护涉及到系统的建设安全、使用安全和维护安全等生命周期各阶段。同时,作为系统管理对象,档案电子文件在处理、存储、传输和使用过程中,容易受到各种不确定因素的干扰,使电子文件信息遭到破坏或缺失。为有效提高档案管理系统的信息安全防护水平,山东联通档案管理系统建设注重了以下五个方面:

(1)遵循“统一规划、集中建设、规范使用、可靠运行”的原则,从档案信息安全的全局出发,统一设计和调配资源,减少了研究成本,提高了档案系统的安全防护能力。

(2)具有良好的技术支持团队。团队包括档案业务人员、系统开发设计人员、网络技术人员、存储技术人员、主机技术人员等。各方通力合作,既拓展了信息安全防护的深度和广度, 也有利于系统的可持续发展。

(3)系统具有较高的可靠性、开放性和先进性。山东联通档案管理系统实现了系统设备冗余互备和数据的多重备份, 并通过元数据管理和著录项管理,实现了与公文管理、合同管理、工程管理、新闻报送、财务审计等公司其它业务系统的有机衔接。

(4)严格控制系统版本变更。山东联通制定了《管理信息系统工程建设管理办法》、《管理支撑系统需求管理办法》、《信息系统运行维护管理规程》、《信息系统上线审批管理办法》和《档案管理系统系列规范》等规章制度,对系统的上线和变更需经过严格的全面测试和规范的上线审批, 以确保系统版本得到有效控制。

(5)实现了网络化部署和管理。建成的年报管理、目录上报、档案年检系统,实现了省、市、县分公司档案统计年报逐级上报、层次统计与汇总,保证了档案统计数据的准确性和年报的及时报送;目录上报系统实现了各市、县分公司年度档案整理目录向省公司的报送;档案年检系统实现了省公司档案人员可随时对各市分公司的档案归档、整理情况进行监督、指导,大大提高了工作效率。

4 山东联通档案信息安全防护措施

为实现档案管理系统的全方位安全保障,使之能够在统一安全策略保护下,免受因外部攻击、较严重自然灾害以及其它相当程度威胁所造成的信息丢失或破坏; 能够实时监控系统运行情况和安全事件,在系统崩溃或遭到损害后迅速恢复所有功能,山东联通主要采取了以下六项措施。

4.1 业务规范化与标准化

业务规范化与标准化的目的是为了规范档案业务管理人员的行为，确保电子档案在采集、处理、存储、利用过程中的信息完整、可用、可控和可靠。主要包括系统接口标准化、业务操作规范化。

(1)接口标准化：山东联通档案管理系统建立了电子文件归档的标准化接口，实现了与公文、合同、工程项目、新闻发布、财务等业务系统间、不同数据格式的电子文件的自动转换和可靠归档。

(2)操作规范化：系统实现了档案的采集、加工、借阅和利用等操作过程、操作方法的规范和统一，有效避免了因不同人操作而导致的数据不一致现象。

4.2 环境安全

环境安全是指档案管理系统及其存储介质应存放在安全可靠的地点，包括楼宇安全和机房安全。

山东联通档案管理系统位于通信枢纽楼的核心机房，楼宇和机房配有专业人员进行 7*24 小时值守，人员进出有严格的审批管理制度。机房除了配有门禁和指纹锁等安保设备外，还有完善的防水、防火、防电磁、防雷击、防偷盗破坏措施，以及电力保护和温湿度控制等设备。

4.3 设备安全

设备是档案管理系统的物质基础，主要包括系统主机、网络设备、存储设备、用户终端等。硬件设备故障是威胁档案系统和信息数据安全的主要因素之一，严重影响系统正常运行和业务完整提供，并可能导致电子文件的丢失、失密、完整性被破坏等情况的发生。

山东联通采用的安全防护措施主要包括设备冗余配置、漏洞补丁、身份鉴别、资源控制设备安全审计和用户终端标准化等。

(1)设备冗余配置：管理系统的主机、网络和存储设备均实现了双机冗余配置，其中主机采用 HACMP 技术实现双机互备，一台主机宕机后，另一台主机可自动接管。

(2)强身份鉴别管理：主机、网络和存储等设备的管理员由不同人员担任，各管理员帐号和密码分别保管，密码具有较高的复杂度并定期更换。系统主机只允许 root 和 notes 用户访问并自动记录访问情况。

(3)设备运行监控：专业工程师对各设备进行7*24小时现场巡检和维护，建有 IT 网管监控系统，自动监控设备运行情况，自动将设备告警信息通过手机短信及时发送给相关责任人。

(4)用户终端标准化：员工的办公终端全部实现了办公软件和防病毒软件的正版化，并实现了统一管理和补丁自动升级。

4.4 网络安全

网络安全是指建立能有效抵御利用网络协议对系统进行攻击的网络层防范措施。

在管理层面，山东联通建立了完善的网络安全防护体系，制定了多项规章制度，如《DCN 网外联管理办法》、《DCN 网络维护管理规范》、《DCN 网 IP 地址管理办法》等。在技术层面，采用了网络隔离、接入控制、漏洞扫描、入侵检测和安全审计等手段。

(1)网络隔离：管理系统承载在 DCN 网上，与 Internet 网实现物理隔离。在 DCN 网内，采用 MPLS VPN 技术，划分为不同的业务系统应用域以进行网络访问控制，最大限度地保障网络安全。

(2)接入控制：山东联通为下属各单位分配了不同的 IP 地址、域名、自治域号，实行 IP 地址和主机 Mac 地址绑定方式；通过不同 VLAN 的划分，对用户的网络访问进行授权，防止随意接入；关闭了档案管理系统服务器不需要的网络协议和通信端口，如 FTP、SMTP、POP3 等。

(3)安全审计：定期(每周)对 DCN 网内设备进行漏洞扫描、入侵攻击统计、病毒和蠕虫事件统计等，并按照不同风险等级进行分类整理，形成《内网信息安

全周报》下发相关责任人进行整改。

4.5 系统应用安全

系统应用安全是确保档案管理系统自身健壮性、可靠性的基本要求; 系统所提供的服务应具备高效、稳定、用户亲和性好的特点。

山东联通采取了权限控制、身份鉴别、高强度密钥技术、最小赋权原则、版本控制和健康检查等措施。

(1)权限控制:管理系统实施多层安全保证机制,各层中均可通过用户身份验证方式来限制用户对数据或资源的访问。用户只有经过多层次的认证与授权后,才能访问到想要访问的信息。

(2)身份鉴别:系统采用双因素身份认证技术。用户必须获得有效的数字证书和正确的密码,才能访问系统。

(3)高强度的密钥技术:系统采用 PKI 双钥非对称加密方式,对数字证书文件进行认证;采用网络信道加密手段防止网络侦听,保证信道传输安全。

(4)最小赋权原则:严格控制各级用户的访问权限, 普通用户的档案借阅须通过电子流程进行审批,并建立了借阅文件单独存放、超期自动归还、自动保留借阅痕迹等控制环节。

(5)版本控制:山东联通省公司本部统一负责全省各单位档案管理系统的需求和变更管理。在系统变更和新功能上线前,要经过严格的全面测试和规范的上线审批,以确保系统版本得到有效控制。

(6)健康检查:每年定期对系统软件进行健康检查,并对程序编码进行代码检查。

4.6 数据存储安全

数据存储安全是档案管理系统安全管理的重要内容,主要包括数据的安全备份和完整恢复;备份内容包括档案系统自身应用程序和档案数据信息。

在数据备份上,山东联通档案管理系统采用了本地存储备份、同城异地备份和异质多地备份等多种方式,并设置了合理的备份周期和备份作业计划,以确保灾难发生时能够快速、有效地进行数据恢复。在应用层面,实行年度分库保存方式,将各种类型、不同年度的数据分别保存在独立的数据库中。某年度档案整理方法发生改变时, 不会影响其它库中的档案数据;在进行年度档案整理时, 往年的数据不在当前库中,从而避免了损坏往年数据的可能,保证了系统档案数据的稳定性。

5 结束语

通过对业务操作、环境、设备、网络、应用和数据存储等方面的安全防护研究和实践,山东联通实现了档案管理系统全方位的安全保障。但是,任何安全体系都不可能一劳永逸地防范所有风险,档案信息安全防护是一个动态的、长期性的工作,网络环境下的档案信息安全防护是一项持续深入的研究课题。

参考文献

1 杨公之.档案信息化建设导论[M].北京:中国档案出版社,2001

2 马长林.档案馆信息化建设探论[M].上海:上海社会科学院出版社,2006

3 张晓霞.王宇晖.王萍.数字档案馆——21 世纪档案馆的新发展[J].兰台世界,2000(1)

4 王荣国.李东来. 数字图书馆的概念形态及研究范围[J].图书馆学报,2001(5)

5 李炎.数字图书馆——信息网络时代的战略选择[J].情报杂志,2000(5)

6 王宇晖.21 世纪数字档案馆发展之我见[J].档案与建设,2000(3)

重点客户组网 E1 故障处理探讨

段衍强 刘 淼

(中国联通泰安市分公司,泰安 271000)

摘 要:根据维护重点客户数字出租 **E1** 专线的多年经验,本文对 **E1** 线路在重点客户组网中的应用方式进行了分类,对故障处理经验进行了总结,为传输和客户服务维护人员提供了工作参考。

关键词:**E1 V.35** 以太专线 测试 定位 故障

1 引言

随着通信技术手段的演进和新业务的不断涌现,以金融、商贸业为主的服务型行业客户对专网通信的需求越来越多样化、带宽要求越来越高。但过去十年间,E1 专线成为运营商重点客户的主流组网方式,因此, 重点客户组网 E1 故障处理仍是目前重点客户保障中的重要工作。本文总结了重点客户组网 E1 故障处理经验,望能给同行提供参考。

2 E1 专线与用户的接口方式

(1)运营商 E1 专线直接为用户两端提供 G.703 E1 接口,用户设备包括 E1 接口路由器、语音交换机等。

(2)运营商 E1 专线为用户两端提供 G.703 E1 接口 +V.35 转换器,或者直接提供 V.35 接口。用户设备为 V.35 路由器,运营商提供 V.35 母头 DCE 接口,用户路由器提供公头 DTE 接口。

(3)运营商 E1 专线为用户两端提供 G.703 E1 接口 + 以太网转换器(俗称网桥),或者直接提供以太网接口。用户设备包括以太交换机、路由器、HUB、电脑等。

(4)有些用户总部一端使用 POS 接口路由器,分部一端使用 E1 或者 V.35 接口路由器,这样运营商就需要为用户总部提供 POS(E1 接口被集成在 POS 口内部,可视为 G.703 E1 接口的批量开放形式)光口,为用户分部提供 G.703 E1 接口或者 V.35 接口。银行、证券等业务汇聚型客户经常采用此类接口方式。

实际工作中, 有的用户要求一端使用以太接口、另外一端使用 V35 接口或者 POS 接口, 这样的组网接口要求由于涉及到以太网协议到 V.35 协议之间的转换,需要额外增加专用转换设备如 MSAP 等,否则仅用上述 4 类接口方式是无法完成组网的。

3 基本故障处理步骤

3.1 借助网管查询设备告警,进行预处理

如果提供 E1 组网的传输设备是可远程网管的 SDH、MSAP、PDH 设备,处理故障时,首先借助网管查看设备历史和当前告警,如掉电告警、光路告警、远端对告告警、E1 丢失告警、UP(DOWN) E1_AIS 告警等。根据这些告警,可以判定故障的大体段落,明确故障处理方向,而不必立即赶往用户端现场;即使去现场,通过这些操作也可以提供有效信息,提早准备需携带的工具、仪表等。

掉电告警、光路告警、远端对告告警、E1 丢失告警等是常见告警,维护人员比较熟悉,本文不做赘述,而是着重介绍经常被忽略的 UP(DOWN) E1_AIS 告警的用途,**E1_AIS** 告警示意图如图 1 所示。

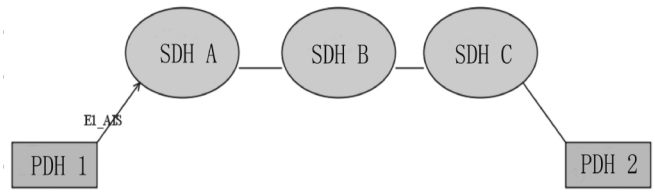


图 **1**　**E1_AIS** 告警示意图

很多 SDH 设备提供 UP(DOWN) E1_AIS 告警功能,即上游或者下游 E1 帧结构告警指示信号。如图 1 所示,假设 SDH A、B、C 三站具备 UP (DOWN) E1_AIS 告警功能,用户 A 和 C 之间 E1 线路发生故障时:

如果 A 站上报 UP(DOWN) E1_AIS,则意味着 PDH 1 设备发送给 SDH A 的 E1 信号(含二者之间的 E1 线缆)中断,故障点在 SDH A 站到 PDH 1;

如果 SDH B 站上报此告警,故障点则在上述基础上再追加 SDH A 和 SDH B 之间的 E1 接口线缆。

这样,根据网管提供的 UP(DOWN) E1_AIS 告警的分析,可以确定故障发生在图 1 所示 PDH 1、A、B、C、PDH 2 这些设备之间的某一段,从而有利于提高故障处理效率。

3.2　询问用户端设备告警情况,进行初定位

通过指导用户简单观察用户端设备,可以了解如下情况:

(1)用户端 SDH/PDH 传输设备、协议转换器本身故障

用户反映用户端 SDH/PDH 设备或者协议转换器本身运行指示灯或者电源指示灯不亮、指示灯频闪异常,可确定是这些设备本身发生故障。

(2)光路故障

用户反映用户端 SDH/PDH 设备上有光路(本端光丢失)告警。光路告警一般是光缆故障造成,这时可询问用户有没有整理线缆、附近有无装修、施工等,以确定光路故障。

还有一种情况就是光功率过强,超过该 SDH/PDH 设备的实际过载点,也会导致误码。譬如:一用户使用的 PDH 设备光功率过载点指标在 -8dBm,发光功率为 -5dBm。由于用户端和局端 2 台 PDH 设备之间的光缆距离很近,2 台设备之间光缆功率衰耗只有 1dBm。经计算,这 2 台 PDH 设备相互接收的光功率值为 -5dBm-1dBm(发光功率减去光缆衰耗)=-6dBm,超过该设备所能承受的光功率过载点指标 -8dBm,从而导致了 E1 线路误码。该类故障隐蔽性较强,如果进行 E1 通道测试时出现误码、但是看不到其他明显告警,此时应该优先考虑光功率过强的可能性。通过测量实际光功率、然后加光衰的办法,解决此类故障。

(3)用户端 SDH/PDH 传输设备对端故障

指导用户操作用户端传输设备上的按钮,通过用户侧 SDH/PDH 设备的对端告警灯 (对端丢光告警、对端掉电告警、对端 E1 信号丢失告警等)功能,以确定用户端设备对端的局端 SDH/PDH 传输设备故障。

(4)用户端线缆或者用户自有设备接口故障

指导用户观察用户端 SDH/PDH、V.35 转换器、以太网转换器的线缆接口指示灯,以确定线缆故障。指示灯包括 E1 接口告警灯、以太接口灯、数据发送 TX 和接收 RX 灯等。

SDH/PDH 设备 E1 接口告警灯报 E1 LOS 告警,而同时以太网转换器不告警,这证明是以太网转换器的发送、光端机的接收线缆故障;

以太网转换器的以太接口灯不亮灯,证明是以太网转换器自身故障或者用户与之接口的网线、交换机故障,可以指导用户自查内部设备和网线;

V.35 转换器数据发送 TX 灯不亮,一般是与之接口的路由器端口故障或者 V.35 转换器本身故障。

(5)用户自有路由器、交换机故障

指导用户对自有交换机、路由器进行简单观察,

如路由器的运行灯频闪、不亮灯,或者交换机的所有端口灯同频闪烁,一般是用户路由器故障或者交换机内部病毒攻击所致。

3.3 现场测试

主要包括以下几类:

(1)E1 通道测试;

(2)V.35 通道测试;

(3)以太 ping 测试;

(4)在线测试。

其中,第(1)、(2)类测试使用电信运营商常用的专业仪表,测试 E1 和 V.35 通道的性能,主要指标是误码率。但是用户对这两类专业指标不是很了解,没有感性认识,通常不太好接受测试结果。

第(3)类测试结果主要指标是线路丢包率和线路延时,用户容易接受。在用户许可的情况下,甩开用户局域网,用路由器的 WAN 口或者直接用笔记本电脑为用户做端到端的 ping 测试并提供结果。

第(4)类测试一般在运营商核心机房或者具备DDF的机房使用,主要测试仪表有误码测试仪、TTE 等,主要指标是误码率、AIS。测试时,仪表采用高阻跨接 DDF 形式,以避免在用户不允许的情况下造成用户业务瞬断。对于中断类、严重误码类的故障,通过该类测试得出的 AIS、误码等结果,可确定故障来的方向是 A 端还是 B 端;派单维修时,先考虑故障来的一端,从而提高故障处理效率。

3.4 替换法、配套设施排除法

进行上述常规观察、测试后,大多数故障都能得到解决,但是也有一些故障,测试正常之后仍无法解决,这就需要用替换法来排除:逐一替换 E1 线路、传输设备、用户自有设备等,确定故障是哪里引发,然后要求相关生产商分析具体原因,向用户做出答复。

4 疑难故障案例

有几类疑难故障不容易确定,如:设备之间不匹配、局域网病毒、环境干扰、设备性能指标下降等,其隐蔽性较强,又没有既定处理步骤,只能根据具体情况决定排查方向,下面通过几个案例加以说明。

4.1 传输通道、路由器匹配故障

(1)故障现象:某商场火车站总部至花园小区分部通信故障,用户某一程序无法使用,从用户路由器 WAN 口上进行 ping 测试,发现:分部到总部偶有丢包,端口有 CRC 错误包增长。

(2)基本处理方式:进行 E1 通道测试,测试结果正常,各类设备单独测试都没有问题;使用设备替换法,更换运营商提供的 PDH 设备和 E1 通道,故障依旧。

(3)故障解决:将花园小区分部路由器由华为公司路由器更换为 CISCO 公司路由器,所有故障现象消失。后观察数月,通信正常。

(4)故障定位:运营商提供的传输 E1 通道与用户自有华为路由器配合故障。

4.2 用户局域网病毒故障

此种情况下,进行常规 E1 通道测试、没有任何异常;加入用户路由器 ping 测试,出现丢包甚至不通,用户路由器 WAN 口可能会有 CRC 错误包增长。

如果用户 A、B 两端都具备以太网接口,且两端客户都能配合,首选是两端都用笔记本电脑甩开用户网络进行 ping 测试,如测试正常,即可排除运营商原因。

如果用户 A、B 不具备以太口直接测试条件,只有 B 端允许以太口测试,最好的方法是甩开 B 端所有用户,仅保留 B 端用户路由器的 WAN 口,在 WAN 口上 ping A 端路由器 WAN 口地址;如测试结果正常,可以排除运营商原因,转而配合客户检查局域网。

下面以某市法院至上级省法院、下级县法院 E1 线路通信故障案例说明此类故障处理过程。

(1)故障现象:从市法院路由器 WAN 口上 ping 上级省法院路由器测试,发现:大量丢包,市法院路由器 WAN 口为 E1 接口,端口有 CRC 错误包增长。

(2)基本处理方式:使用 E1 通道测试,市法院到省法院的通道无误码,测试结果用户认可,承认线路没问题,但要求协助其确定局域网内故障点。

继续测试中,发现笔记本电脑 + 串口线缆登陆用户路由器时,通信状态时断时续,因此怀疑用户路由器数据拥塞,导致运行不稳定。

(3) 故障解决: 经用户同意, 甩开用户局域网 LAN 口以下所有设备, 仅保留市法院路由器至省院 WAN 口, 此时笔记本电脑 + 串口线缆登陆用户路由器通信正常,路由器运行稳定;观察路由器 LOG 历史日志,CPU 使用率曾达到 97%以上,判定市法院局域网内有病毒攻击。逐一将用户电脑和服务器接入路由器,最终发现用户 1 台 web 服务器入路由器时,路由器 CPU 占用率由 7%立即升高至 97%,确定故障原因为该 WEB 服务器病毒攻击路由器, 导致路由器拥塞。

4.3 机房电源干扰导致的故障

按照通信机房建设原则, 机房应当实现信号线、交直流电源线的分离。而很多客户机房受条件所限,布线不规范,导致了疑难故障的发生。主要表现为交流电源、空调、大功率发射器等对 E1 信号线缆或通信设备形成干扰,或者机房接地不良,导致各类设备运行不稳定。

下面以某市邮政局至县局视频业务故障案例说明此类故障处理过程。

(1)故障现象:原来正常使用的电路突然间开始丢包。

(2) 故障处理: 传输通道测试正常, 用户端口 CRC 错误增加,情况极不稳定,没有规律可循。用替换法进行处理,更换了所有设备和通道,故障依旧。

经排查发现, 把传输 E1 线缆在用户机房地板下变换位置时,用户丢包现象立即消失。仔细观察,发现地板下用户电源线很多,主 220V 交流电源线和故障电路的 E1 线交叉, 应该是交流电源线对信号线形成干扰。经试验,证实这一推断。

(3)故障解决:整理用户线缆,把交流电源线进行金属套管隔离,使 E1 信号线和电源线距离保持 20cm 以上,故障消失,用户业务稳定。

4.4 传输 E1 接口性能下降或 E1 阻抗匹配导致的故障

实际应用中 E1 接口分 75 欧姆和 120 欧姆 2 种,可根据用户的不同需求进行灵活配置。有些用户同时对两种接口都有需求,而一套 SDH/PDH 传输设备只提供其中一种,因此很多维护人员习惯把两种接口直接相互替换, 而不是按规定增加 75/120 欧姆的转换器。在 E1 线缆较短的情况下, 最初业务不会发生问题;一旦设备老化、E1 接口性能下降时,就会出现丢包现象。而常规的 E1 通道测试不能发现误码,所以此类故障隐蔽性较强。

在处理某公安部门通信故障时发现,运营商提供的华为 SDH 设备与公安部门采购的 PDH 设备通过 E1 线缆直接进行对接的业务故障率很高。故障发生时, 电路测试有误码,SDH 支路板端口损坏,SDH 支路板接线处有烧焦痕迹。怀疑其自购 PDH 光端机的 E1 接口指标异常, 不能匹配运营商提供的 SDH 设备。要求其更换正规厂家设备后,故障解决。

5 结束语

近年来, 随着用户业务需求的变化,2M 带宽的 E1 专线已很难满足需求,速率更高、适应性更强的以太网专线业务浮出水面,成为大客户专网组网的主要方式。尽管用户组网形式发生了改变,但是重点客户故障处理的基本思路和步骤没有太大改变。本文提供的经验仍将在今后工作中发挥较好作用。

强化投诉分析 降低 GPRS 投诉率

孙 晶

(中国联通临沂市分公司,临沂 276000)

摘 要:本文从 **GPRS** 的投诉分析统计出发,找出用户投诉中的共性问题,分析原因并制定相应措施。措施实施后,及时通过投诉统计验证效果,保证了各项措施的针对性与实效性。

关键词:**GPRS** 分析 投诉率

1 引言

今年 1—5 月,某市电信运营企业 GSM 用户数迅速增长,GPRS 业务飞速发展。但随之出现的是后台资源的短缺、网上话务量的拥塞和用户服务质量的降低,GPRS 投诉不断增加。鉴于此,如何快速增强网络的业务提供能力, 满足不断增长的 GPRS 用户需求,成为维护部门面临的重要课题。

2 GPRS 投诉细分

5 月份 GPRS 投诉共 418 例。其中,反映无法上网的 400 例,上网慢的 2 例,出现掉线的 3 例,登陆网站正常而登陆 QQ 有问题的 12 例,下载音乐失败的 1 例。根据投诉产生的原因细分:

(1)用户自恢复:93 例,占 22.2%;

(2)用户手机设置原因:123 例,占 29.4%;

(3)HLR 执行位置更新后恢复:111 例,占 26.6%;

(4)基站语音话务忙或 BSC 处理能力有限:26 例,占 6.2%;

(5)基站障碍:23 例,占 5.5%;

(6)弱覆盖及干扰原因:18 例,占 4.3%;

(7)其他原因(QQ 版本问题或 WAP 网关问题):24 例,占 5.7%。

3 故障处理措施

3.1 用户自恢复类投诉:占比 22.2%

检查用户 GPRS 数据正常, 再次回访已自己恢复。这种情况占投诉总量的 22.2%。

(1)原因分析

用户所处的位置在上网时未能分配到空闲数据以传送信道(PDTCH,分组数据业务信道)而引起。

由于载频资源紧张,用户所能分配到的空中资源有限,而 GPRS 是叠加在 GSM 网络上的另一张网,这两张网共用一套无线资源,二者在容量配置上存在冲突,只能适当兼顾。而当用户话音和数据需求都比较大时,则按照语音优先原则将信道资源首先分配给语音业务,这时 GPRS 数据业务就会受到影响。

(2)解决措施

1)当网络没有保留 PDCH(Packet Data Channel,数据包信道),或保留的 PDCH 信道数量过小时,数据的传输速率都会降低,或直接连不上网。可以根据用户发展情况考虑,在特定地点、特定时间增加 PDCH 数据,或将动态 PDCH 修改为静态 PDCH。

2)合理设置各类定时器,调整 PDCH、AGCH(接入允可信道)上的信令负荷,使 PDCH、AGCH 上负载均衡,最大限度地提高 PDCH、AGCH 的利用率。

3.2　用户手机设置类投诉:占比 29.4%

用户无法上网,而周围用户可以。用户所处位置基站正常,GPRS 数据正常。更改用户手机设置后恢复。

(1)原因分析

关于GPRS业务的手机设置与检查一般包括7个方面:

1)检查用户手机的上网软件版本是否正确;

2)检查手机是否正确设置了上网参数;

3)检查用户网关地址及端口设置:如果手机发送的 APN(Access Point Name,接入点名称)错误、不是公用的 APN(UNINET、UNIWAP)或为空,那么,目前的公用 SGSN 会自动将用户请求的、HLR (归属位置寄存器)未签约的 APN 纠正为 UNIWAP;如果此时仍不能上网,则一般为用户网关地址设置错误或端口设置错误原因。另外,用户 GPRS 数据不完整也是导致激活失败的原因, 这主要是指 HLR 支持 GPRS 却缺少 PDP 定义所致。

4)检查手机设置的 QoS(服务质量)是否与 HLR 中的设置相匹配、是否设置了 IP 地址。因为系统不具备分配静态 IP 地址功能, 如果手机请求信息含有固定 IP 地址,那么激活请求会被 SGSN 拒绝。

5)检查用户行为

用户尚未完成激活时又重新发起激活过程,会造成激活失败; 或者用户在一个 APN 已经激活的情况下,尝试用另一个 APN 激活,因为部分设备目前不支持两个 APN 同时激活,所以也会造成激活失败。

6)检查手机本身设置

手机本身与网络的配合也是一个重要因素。GPRS 手机与 GPRS 核心网兼容性不好,可能会出现某些型号的手机在已经激活状态下又频繁发送 PDP 上下文激活请求消息,而导致上网失败。

7)清除手机上网缓存;检查手机内存空间剩余量。

(2)解决措施

1)检查用户申请的 APN 是否已授权给用户,检查用户手机中有关 GPRS 的设置、网关地址及端口的设置、APN 的设置是否正确,有无固定 IP 地址,QOS 配置是否正确。

2)加强与市场、客服部门的沟通,整理不同型号手机的设置规范提供给客服,便于其辅导用户,直接解决问题,减少派单量。

3)与客服部门之间开通绿色通道,一旦用户有类似问题立即响应,辅导用户正确设置手机参数、使用 GPRS 业务。

3.3　HLR 执行位置更新后恢复类投诉:占比 26.6%

检查用户 GPRS 数据正常; 让用户开关机或 HLR 执行位置更新后恢复正常。

(1)原因分析

1)如果用户在移动的过程中出现位置更新失败,用户的附着信息便会吊死在 SGSN 中; 当再次发起 PDP 激活时,SGSN 便会因为找不到用户标签信息而拒绝。这时通过位置更新,清除以前老的 SGSN 中的附着信息,便可以成功附着。

2)用户在同一 SGSN 内的或跨越 SGSN 之间的路由更新失败,也会使用户的路由信息发生吊死,再次发起 PDP 激活时将被 SGSN 拒绝。通过开关机重试即可解决。

3)在 HLR 中看到的“用户附着成功”可能是一种“虚附着”情况,即:SGSN 向 HLR 中鉴权成功后,将用户所附着的 SGSN 信息插入 HLR、更新 HLR 数据库,HLR 便认为用户附着成功。而此后 SGSN 还要通知用户所在的 MSC/VLR(拜访位置寄存器)发起一个位置更新消息,再向手机发送“Attach accept”消息;手机根据接收到的信息调整自身状态为 “Attach”,向 SGSN 发送“Attach Complete”消息后,这时附着流程才结束。不过有可能受无线环境影响,手机并没有收到 SGSN 发送的“Attach accept”消息,也就没有成功修改手机状态,从而也就没有附着成功。这时发起一个位置更新后,让手机重新附着,可能就会成功。

4)核心侧 SGSN 与 HLR 之间信令配合问题,导致 SGSN 至 HLR 中进行的鉴权过程及更新 HLR 数据库失败,致使用户附着不成功。

(2)解决措施

1)加强对用户正确使用 GPRS 业务的宣传,传授正确的使用方法和简单的故障排查方法。

2)跟踪用户出现路由更新失败的问题小区,通过以下措施进行排查: 重新开关小区的 GPRS 业务,重

新复位闭塞小区内的 BVC（BSSGP 虚连接），对 GPRS 的 BRP(BSSGP RLC/MAC，协议处理器)归属配置进行检查，合理调配 EBRP（增强型 BSSGP RLC/MAC 协议处理器)板的负荷均衡。

3)定期与公用 SGSN 侧核对小区数据，查看位置区、路由区设置是否与 SGSN 保持一致。

4)在 HLR 侧查看用户 GPRS 权限、APN 应用开放、速率设置及附着情况。如正常，则可联系 SGSN 侧通过跟踪信令共同查找原因。

3.4 基站语音话务忙或 BSC 处理能力有限类投诉：占比 6.2%

用户所处位置的基站话务忙或 BSC 中 PCU（分组控制单元)的 GPRS 容量满等原因所引发。

(1)原因分析

1)基站本身语音话务忙，如该小区只指配了动态 PDCH、没有指配静态 PDCH 的话，当语音忙的时候就会占用动态 PDCH 资源，导致用户发起上网需求时得不到分配的业务信道而无法正常连接。

2)BSC 中 PCU 单元 EBRP 板（处理 GRPS 业务的单板)处理 PDCH 信道的能力有限，致使用户需求被丢弃。

3)PCU 单元中 EBRP 板的信道配置不合理，使各个 EBRP 板负荷不均衡，也会导致不能正常处理用户的上网需求。

(2)解决措施

1)用新的 IBSC(综合基站控制器)替换老的 BSC(基站控制器)，将 GPRS 的处理能力由原来的 120 路信道提高到 400 路，相关的业务处理能力提高到 2 倍以上。

2)优化网络，将用户上网需求大的小区分配静态 PDTCH，使用户即使话音业务忙时也不会抢占上网业务信道。

3)合理设置、优化各类 GPRS 业务中的定时器，减少 PDCH、PDTCH 和 AGCH 等资源的浪费。

4)调整 PCU 上各 EBRP 板的信道配置，尽量做到业务均衡。

5)SGSN 侧实施软件升级与扩容。

3.5 基站障碍类投诉：占比 5.5%

(1) 原因分析：用户所处基站的话务统计中无 GPRS 流量，GPRS 信道有载频告警和信道无帧号告警，分别更换载频和联系传输部门解决。

(2)解决措施

1)每天进行 TOP5 小区分析，将 GPRS 流量分析加入每天的监测优化中，关注各项 GPRS 统计指标。如果发现 GPRS 流量为 0 的小区，第一时间派单至维护部门进行处理，并每天根据 PDCH 平均占用率及时进行优化和整改。

2)加大对网络告警、网络统计报表的分析力度，对指标不好的小区迅速排查故障，将维护工作做到用户投诉之前。

3.6 弱覆盖及干扰类投诉：占比 4.3%

(1)弱覆盖问题：提高服务小区的信号强度。

(2)系统内或系统外的干扰原因：检查是否存在同频干扰。如存在，则重新进行频率规划，调整干扰小区的覆盖，使干扰信号较低；或者调整服务小区的信号强度。

3.7 其他投诉类(QQ 版本或 WAP 网关问题)：占比 5.7%

上网正常但登陆 QQ 不成功，或登陆个别网站不正常。

(1)引导用户检查手机上网软件或 QQ 版本，有些版本与手机不兼容，也会造成登陆故障。

(2)检查 APN 的 DNS(域名服务器)查询是否有问题，防止用户使用正确的 APN 激活 PDP 后，不能根据 APN、号段信息所组成的域名解析出 GGSN 的地址，告诉 SGSN 下一跳是什么。

(3)针对登陆个别网站不正常的情况：在排除网站原因后，可检查 WAP 服务器的相关设置与状态。

(4)针对下载音乐失败的情况：下载数据量过大引起。避开忙时下载，一般即可解决。

4 结束语

本文措施实施后，移动网络各项考核指标不断攀升，用户投诉率不断下降：7 月份 GPRS 类投诉较 5 月份下降 48.9%，在为业务发展提供优质服务保障的同时，也为树立良好企业形象提供了重要支撑。

国际去话应答接通率异常原因超频呼叫的分析和探讨

陈 森 韩 萌

（中国移动通信集团设计院有限公司山东分公司，济南 250021）

摘 要：本文围绕国际去话应答接通率异常现象，对其产生原因——超频呼叫进行了定位和分析，并就解决途径进行了有益的探讨。通过实例，列举了修正异常指标值的具体方法。

关键词：国际去话应答接通率 超频呼叫 修正

1 引言

网络部门在制作每日网络运行 KPI 时，发现一个国际侧指标——国际去话应答接通率非常不稳定，有时低于 50%，有时又在 58—59%的高位。按照 KPI 审核参考标准，周一至周五工作日时段，国际去话应答接通率正常值应介于 50—55%之间；超出这个范围则为异常，需要分析具体原因并对指标进行修正。至于周六、周日，因受商务用户大幅减少等因素影响，48—49%也属正常。

由于电信运营商对国际去话应答接通率的波动较为敏感，为更直观地体现现网真实的国际去话应答接通率，必须对其异常原因进行深入分析，并设法屏蔽或消除不利因素，在剔除各种干扰项的前提下，将异常指标值予以修正。

2 超频呼叫原因分析和解决对策

2.1 问题定位与分析

（1）国际去话应答接通率偏低

对于国际去话应答接通率偏低的情况，在国际去话呼损次数表（表 1）中，主叫早释、振铃释放 2 种主叫用户行为造成的呼损次数最多，之和约为 11.7 万次呼叫 / 忙时，占总呼损次数的 86%，而振铃释放又占到了 70%以上（图 1）。

表 1 国际去话呼损次数表

时间	被叫拒接	被叫忙	接续不全	主叫早释	振铃释放
2011-XX-XX 18:00:00	1026	13434	4581	22327	94247

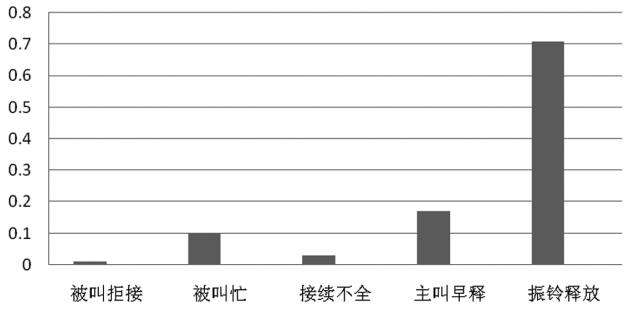


图 1 呼损比例图

进一步核查发现，这些振铃释放的呼叫记录里，有部分主叫号码呈现出短时频繁拨号、挂机的情况，呼叫地域一般为固定方向或呈离散态分布的国家或地区。以告警次数 100 次 / 小时为基准，呼叫大于 100 次 / 小时的主叫号码多半为自动接听；如果被叫用户回拨回去，听到的内容多为欺诈或者广告。

（2）国际去话应答接通率偏高

对于国际去话应答接通率偏高的情况，从呼叫业务 TDR 统计看，多为从京、沪、穗国际局出局的国际去话应答次数异常增加所致。例如，国际去话应答次数 125 万次，较日常值（假定 100 万次）增长 25%。依

照计算公式,国际去话应答接通率 = 国际去话应答次数 / 国际去话占用次数。因国际去话应答接通率<100%, 则国际去话应答次数小于国际去话占用次数。当分子(100 万次)对应的增量(25%)远超分母(假定 190 万次)对应的增量(13%)时,分子与分子的比值自然偏高,即国际去话应答接通率偏高。

进一步核查异常呼叫记录发现,存在大量通话 3 秒即挂断的情况。这些呼叫记录里,主叫号码为不规则连续号段,被叫号码为固定号段;呼叫地域一般为太平洋岛国方向。

上述两种情况引发的大量非法呼叫被称为超频呼叫。所谓超频呼叫,是指一个主叫号码在指定统计时间段内呼叫国际长途的次数超过指定门限值的呼叫。

2.2 对电信运营商的影响

从过往情况看,超频呼叫对国际去话应答接通率异常的影响最大。有些不法分子将办理的移动电话号码用特殊群拨设备进行自动拨号,一种情况是“响一声”骚扰电话,另一种则是大量代拨境外声讯台。

“响一声”骚扰电话占用大量的网络资源,会造成通信网络拥塞,影响正常客户的通话,并且使不知情的客户回拨后产生话费损失甚至上当受骗,其性质类似于垃圾短信, 给运营商的企业形象造成负面影响。而大量主叫用户拨打境外声讯台,使国内运营商跟境外运营商结算时会蒙受巨大的经济损失,也使不法分子套取结算费用有了可乘之机。同时不容否认的是,部分境外运营商受经济利益驱使,将大量闲置号码分配给声讯台,也起到了推波助澜的作用。

2.3 超频呼叫的解决对策

对于超频呼叫,网络部门可采用各种网管技术手段。譬如,利用国际局实时报表系统,以 15 分钟粒度对国际去话应答接通率进行监测; 若发现指标异常,则利用国际七号信监测系统,监测、分析超频呼叫的主叫号码, 定位超频呼叫被叫号码可能集中的区域。随后,网络、市场部门建立跨部门通告流程,网络部门发现超频呼叫后告知客服部门验证;如果客服部门验证情况属实、市场部门确认问题严重,则通知网络部门在国际局封堵被叫号段。同时,依照相关流程通知主叫号码归属地的省公司,对于明确为非法呼叫的主叫号码及时予以停机。

此外,对于少数唯利是图的国外运营商,国内运营商应加强与对方的沟通和信息交换,建立必要的共同打击超频呼叫的联系机制,晓以利害,使其能够配合清理乱分配闲置号码问题。

3 修正方法

3.1 一般流程

鉴于国际去话应答接通率偏低、偏高两种情况的修正方法较相似,笔者仅以国际去话接通率偏高为例进行介绍。

例如, 某日国际去话应答接通率达到 58.1%,较平时偏高。经查,为去往 A 国方向的非法呼叫导致。剔除被叫方向的非法呼叫后,其值修正为 53%。

具体查询和修正方法如下:

(1) 在国际信令监测系统 - 告警管理 - 非法呼叫预警中,查询 X 月 X 日全天国际去话(被叫)非法超频呼叫告警,可看到 345* 号段的非法呼叫号码最多。因无法确定是去往哪个国家方向的话务,需要查看具体信令。双击任意一个非法呼叫号码, 例如 345773967, 将该号码复制到呼叫查询被叫全号码前缀中,以 *345773967 进行查询,可看到为去往 A 国方向的非法呼叫。

(2)明确为 A 国方向非法呼叫后,开始确定此类非法呼叫的应答次数。以 00XX345 为被叫全号码前缀在呼叫查询中进行核查。(需注意的是,00 不可以用 * 代替,因为这会将 IP 长途呼叫次数计算在内。)在呼叫查询条件面板中选择 TDR 统计, 在新弹出的窗口呼叫业务 TDR 统计中, 将复选项统计指标里的呼叫结果横排勾上,点击统计,开始统计 X 月 X 日全天非法呼叫的应答次数,查询结果假定是 25 万次。

(3)在国际局性能管理系统中,打开国际及港澳台报表 -KPI 汇总表,选取日报,取出 X 月 X 日国际去话应答次数(假定是 125 万次)和国际去话占用次数 (假定是 215 万次)。

(下转第 42 页)

5ESS 双 GSM 改造方案探讨

宋景刚

（中国联通泰安市分公司，泰安 271000）

摘 要：本文介绍了在网络智能网化改造后，为提高端局中继负荷和信令处理能力而采用的将 5ESS 交换机由单信令点码改造为多信令点码的操作步骤和注意事项，该方案提高了 5ESS 交换机系统的安全性。

关键词：OPC GSM

1 双 GSM 业务概述

随着网络智能化改造的深入，市话局所有的话务（包括本局话务）都指向智能网汇接局，这样对中继负荷和信令处理能力的要求比以前就有了大幅度提高。

对于单信令点码的 5ESS 交换机而言，信令处理完全集中在全局交换模块 GSM 的 PSU 上。一旦 GSM 或该 GSM 的 PSU 发生故障，全局话务势必受到影响。因此，为克服网络智能化改造所带来的系统安全性降低的问题，有必要在话务量高的市话端局、汇接局、长途局上创建第二个 GSM，实现单交换机的多信令点码（OPC）功能。

根据原 GSM 的配置，为新 GSM 到相应对端局创建信令链路和中继群，对出局话务采用宏路由进行负荷分担，使负荷平均分配到两个 GSM 上的信令链路和中继群。采用普通的话务分担。当同一局向的信令链路或中继群出现故障时，该局向的话务将受到影响，影响的比例为设定话务分担时的比例。而采用宏路由，配合双 GSM 对话务进行负荷分担，可以实现在两个 GSM 正常工作时，按设定的比例负荷分担话务；当其中一个 GSM 的信令链路或中继群发生问题后，另一个 GSM 承担全部话务，大大提高了系统的安全性。

2 5ESS 实现双 GSM 前的准备工作

2.1 5ESS 上实现双 GSM 的安全原则：单 GSM 可以承载全局话务

（1）信令链路：新 GSM 上的链路群和链路数量要与原 GSM 的一样。

（2）中继群：为同一局向设定两个中继群，分别归属不同的 GSM。

（3）中继数量：到同一局向的两个中继群的中继数量尽量一样。当一条中继群工作时，其中继可以承载该局向的全部话务。

（4）QPH 数量：新 GSM 的 QPH 数量要与原 GSM 的 QPH 数量一样。

（5）资源分配：出于安全考虑，两个 GSM 应分别控制不同 LSM 上的信令链路和中继群，不得重叠。

譬如，5ESS 有 6 个 LSM2000，原 GSM 是 SM1，现将 SM6 改造为新 GSM。

GSM1 控制的信令链路和中继来自 SM1、SM2 和 SM3。

GSM6 控制的信令链路和中继来自 SM4、SM5 和 SM6。

2.2 资源要求

(1)硬件要求

1)新增的 GSM 类型应该是 SM2000 或 SM-XC,其负荷相对较低。

2)选定的 LSM 应配备 PSU 单元,该 PSU 单元空闲的协议处理器(PH3 或 PH22)资源可支持的信令链路数量应不少于原 GSM。

3)选定的 LSM 的 PSU 单元的空闲协议处理器(PH3 或 PH22)用作 QPH 的数量应与原 GSM 一样。

4)根据话务量和实际配置,决定是否需要为选定的 LSM 的 PSU 单元增加 PIDB 总线。

5)因为信令链路和中继群的重新分配,决定是否需要为个别 SM 扩中继电路板(DLTU、OIU)。

(2)其它要求

1)局方需为该局新 GSM 申请新的信令点码。

2)对新扩容的中继电路,协调相关部门,根据要求调整传输。

3)分析本局现有中继群,为新 GSM 分配通向直连局(市话局、汇接局和长途局)的中继,话务采用宏路由负荷分担形式。

4)分析本局现有信令链路,为新 GSM 分配通向信令转接点 STP 的链路。

5)5ESS 的对端局(市话局、汇接局、长途局)和 STP 都需要进行数据调整。

2.3 改造效果图

改造效果图如图 1 所示。

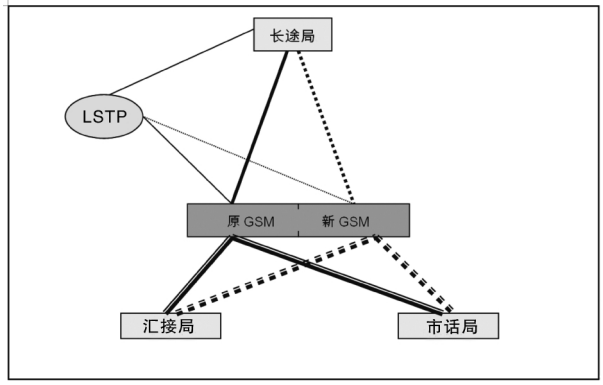


图 1 改造效果图

图 1 中,(1)实线表示原 GSM 到各局的信令链路和中继。其中,粗线表示中继,细线表示链路。

(2)虚线表示新 GSM 到各局的信令链路和中继。其中,粗线表示中继,细线表示链路。

(3)根据各局的实际情况配置,信令链路采用直连或准直连。

3 5ESS 实现双 GSM 的操作步骤

(1)根据原 GSM 的数据,在 RC/V40.1 CCGSM 中插入新的 GSM;

(2)在 RC/V9.4EUPSU 中设置新 GSM 的 PSU 中备份协议处理器的数量;

(3)在 RC/V99EUPHW 中定义信令处理器类型:PH3 或 PH22;

(4)在 RC/V13.11 QPIPE 中定义 QPH;

(5)激活 QPIPE;

(6)在 RC/V13.10EUQMH 中定义对应于新的 GSM 的第二个 QLPS 网络;

(7)在 RC/V13.12 QGCON 中定义与新的 QLPS网络相连接的 SM;

(8)在 RC/V40.2 CCLS 中加入由新 GSM 引出的信令链路组(LINK SET);

(9)在 RC/V40.3 CCPC 中定义相应信令路由;

(10)在 RC/V40.5 CCLNK 中定义该信令链路组中的信令链路;

(11)在 RC/V40.4CHGRP 中检查 PSUPH 的分配使用情况;

(12)在 RC/V4.1 TRGNR 中定义新 GSM 对应的中继群数据;

(13)在 RC/V4.3 TRKNR 中定义中继线数据;

(14)在 RC/V6.3 RTIND 中定义出局路由;

(15)为到同一局向的两条路由创建宏路由;

(16)激活信令链路,打开话务报告,进行呼叫测试。

4 5ESS 改造双 GSM 时的注意事项

(1) 在加 RC/V13.12 QGCON 表时,NONEGSM

LIST中应该包括 GSM 本身。

(2)在 RC/V40.5 CCLNK 加入信令链路前,应检查新 GSM 是否已经将 PSUPH 用于 CCS 的 IMAGE 加载。如果没有加载,就加 RC/V40.5 数据,系统会给出 MAJOR 告警,提示缺少相应 IMAGE。

1)检查 IMAGE 情况。如果没有 PH3AC、PH3IC 和 PH22S 的 IMAGE,继续 2)—4)。

2)扩 PH3 或 PH22 的 CCS IMAGE。下面命令结束后,用 1)命令检查,可发现 CCS IMAGE 已经扩好,但状态是 EMPTY:

<ST-GROW: SM=6, ODRID=PH3C; ← 如果使用 PH3 作为 CCS 处理

<ST-GROW: SM=6, ODRID=PH22S; ← 如果使用 PH22 作为 CCS 处理

3)将新 GSM 的 ODD 备份到硬盘:

<BKUP-NRODD: UNIT=6;

从 AM 硬盘中将 CCS IMAGE 的数据 PUMP 到 SM 内存(需要比较长时间):

<ST-NIPMP: SM=6, ODRID=PH3C

<ST-NIPMP: SM=6, ODRID=PH22S

4)重复 1)命令检查,确认 CCS IMAGE 的状态已经从 EMPTY 变为 NORMAL。

(3)在实施时,应首先选择一个局向、改少量中继进行测试,确认没有问题后,再逐步进行其它局向的改造。

(4)实验室测试结果

1)系统正常工作时,话务平均分配到中继群 196(GSM1)和 198(GSM6);

2)将中继群 196 置为 OOS 状态,出局话务全部转到中继群 198;

3)将中继群 198 置为 OOS 状态,出局话务全部转到中继群 196;

4)将 GSM 1 到 STP 的链路置为 OOS 状态,出局话务全部转到中继群 198;

5)将 GSM 6 到 STP 的链路置为 OOS 状态,出局话务全部转到中继群 196;

6)将 GSM 6 隔离,SM6 的用户和以 SM6 作为路由 SM 的用户无法出局,其它用户的出局话务全部转到中继群 196。

(上接第 **39** 页)

(4)剔除去往 A 国方向的非法呼叫后,修正值 = (125-25)/(215-25)≈ 53%。

3.2 修正方法流程图

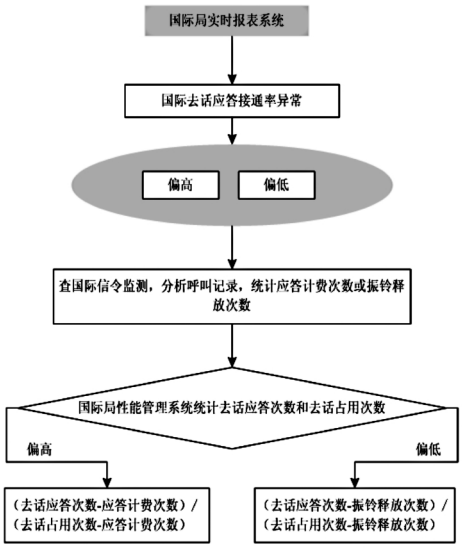


图 **2** 修正方法流程图

4 有关建议

分析国际去话应答接通率指标,电信运营商可以根据掌握的情况采取一系列针对性措施。譬如,对海外超频号段实施封堵,通过业务渠道停机处理非法主叫号码,配合公安机关清查打击非法窝点,同时探索非法呼叫拦截措施等。

5 结束语

对于超频呼叫问题,电信运营企业不仅要对症下药,更要标本兼治。本文所提各种应对措施可以有效地在源头上遏制超频呼叫,从而确保国际去话应答接通率的指标值处于稳定波动范围内。

提高基站断电告警准确率的措施及应用

林 垚

(中国联通威海市分公司,威海 264200)

摘 要:本文针对某运营商移动基站的断电告警状况做了调研,分析了基站断电告警不准确的原因,并制定了相应对策,实施后降低了基站断站率,提高了客户感知度。

关键词:基站动力环境监控系统 断电告警准确率 监控中心 监控设备

1 引言

随着移动网建设力度的加大,某市分公司年均新增基站数均超过 100 个,在网基站数量迅速增加。这些基站很大一部分位于野外无人职守环境中运行,环境相对恶劣,存在较大不可控性。而基站的高质量运行是建设、维护工作的重中之重,目前主要借助基站动力环境监控系统进行维护。基站动力环境监控系统主要由监控设备、网管服务器、告警平台等组成,对基站电源、空调、蓄电池等设备的运行参数及基站机房的物理环境(温度、湿度、火警等)以环境参量形式进行遥测、遥控;中心机房实施集中远程实时监测,用以指导诊断和处理故障。

在所有的监控参数中,基站停电是重要的告警参数之一。当基站供电异常时,开关电源监控模块采集到断电信息,上传到位于基站的监控设备,信息汇总至网管服务器,值班人员通过中心机房的监控中心告警平台发现告警后,通知维护人员现场确认和抢修。

基站监控系统停电告警的准确率至关重要,2010 年 1—3 月的断电告警准确率基本稳定在 97%左右,从数字上看已经不低,但仍有一部分停电事件因为告警不及时影响了处理,进而导致基站脱网。因此,提高基站断电告警准确率势在必行。本文针对某运营商移动基站的断电告警状况做了调研,分析了基站断电告警不准确的原因,并制定了相应对策,实施后降低了基站断站率,提高了客户感知度。

2 影响监控系统基站断电告警准确率原因分析及相应措施

经过分析、汇总,基站断站告警不准确的原因主要有两方面:一是监控系统不显示告警,二是监控系统显示错误。而造成监控系统不显示告警的直接因素,包括监控模块无备件、值班账号设置问题等八条;造成监控系统显示错误的因素,包括 IP 地址冲突、基站名称不一致、断电告警条件设置不完整等四条。逐条进行分析,最后确认导致监控系统断电告警不准确的主要原因有五个:

(1)开关电源监控模块无备件;

(2)某一特殊型号的监控设备硬件存在缺陷;

(3)断电告警条件设置不完整;

(4)网优平台站名调整,未通知监控维护人员;

(5)断电告警等级配置错误。

经测算,解决这些问题就能确保基站监控系

利用硅酸铝保护层对过桥涵洞管道进行隔热保护

曾兆涛 战连胜

（中国移动山东公司青岛分公司,青岛 266034）

摘 要:本文介绍了一种用硅酸铝保护层对过桥涵洞管道进行隔热保护的方法。与现有的 **PVC**、**ABS** 保护管相比,硅酸铝保护层可以节约业务成本,提高光传输网络的安全性。

关键词:硅酸铝保护层 管道光缆 隔热保护

1 引言

近几年,随着业务的飞速发展,通信管道沿桥梁、涵洞挂固的情况越来越普遍,这给管线维护带来诸多隐患,其中最严重的就是火灾事故明显增多。而现在采用的光缆保护管多为 PVC、ABS 管,阻燃、隔热效果一般。为避免因火灾烧毁管道所造成的光缆故障,我们采用了一种耐高温的非金属材质光缆保护层——硅酸铝保护层,显著增强了管道的阻燃性和隔热性,提高了线路安全水平。

2 利用硅酸铝保护层对过桥涵洞管道进行隔热保护的实施方案

2.1 硅酸铝材质可行性分析

硅酸铝是一种铝硅酸盐,无色晶体,不溶于水。主要用来制作耐高温防火隔音隔热棉、板、管、缝毡,防火隔热布,耐高温纸,耐火保温绳、带,防火保温针刺毯、砖,无机防火装饰板、卷帘等。与其他防火材料相

3 应用效果

某地市公司的基站监控系统为历年来多期工程投资所建,设备类型不同。因此,公司针对不同情况,根据制定的措施严格落实。2010 年 7 月至 9 月数据显示,公司基站断电告警准确率逐步提高至 99.8%以上(表 1),在全省相关指标考核中稳居前两位。

表 **1** 措施效果统计表

类别	2010年 7 月	2010 年 8 月	2010 年 9 月	合计
全区基站实际断电次数	617	638	702	1957
监控系统基站断电告警次数	616	637	701	1954
监控系统断电告警准确率	99.87%	99.84%	99.85%	---
平均准确率	99.85%			

4 结束语

基站断电告警准确率的提高,不仅带来了良好的经济效益,而且通过设备利旧等还节省了大量的工程投资。2010 年下半年,减少现场故障确认次数 76 次,减少基站中断 35 次, 产生维护效益 3.7 万元;通过自行研发和设备利旧,节约工程投资近 50 万元。

比,它具有高温隔热、保温、耐火、降噪、绝缘、轻质等优点,所以,硅酸铝是一种应用范围极广、开发前景极大的材料。

2.2 硅酸铝材质与 PVC、ABS 材质性能对比分析测试

硅酸铝材质与 PVC、ABS 材质性能对比分析测试,如表 1 所示。

表 1 硅酸铝材质与 PVC、ABS 材质性能对比表

	抗腐蚀性	耐热性	抗折性	电热绝缘性	使用寿命	工程及维护费用
硅酸铝	强	强	强	好	长	低
PVC、ABS	强	弱	弱	不好	一般	高

2.3 加装硅酸铝保温棉改造实施方案

(1)在新建光缆工程中,存在火灾隐患的光缆全部加装硅酸铝保温棉。

(2)对原有管道进行改造,达到保温棉完全覆盖管道、外观看不到原有管道的效果。

2.4 操作方法

(1)前期准备工作

查阅硅酸铝保温棉技术指标和规格,寻找合格的硅酸铝生产厂家定制样品;对样品产品、质量和强度进行测试、评估;达到设计要求后,按照需求批量订货; 技术人员对需要改造的管道进行实地考察和统计。

(2)使用材料及标准

材料:3.6 米× 0.05 米× 0.6 米硅酸铝保温棉、固定用铁丝等,以上皆符合现行材料行业标准。

(3)操作前准备

1)此项工作的主要工作量是加装硅酸铝保温棉,因为是在使用中的光缆上作业,因此需要熟练工人施工,确保施工过程中网络的安全运行。

2)施工专用车一台,保护栏 / 施工标志柱若干,手钳、不同型号铁丝若干,相应的水泥、沙子等辅助材料若干。

(4)作业步骤

1)检查作业现场,清除作业障碍,建立作业安全区。

2)加装硅酸铝保温棉的工作为:先小心地将管道与桥梁、涵洞或墙壁分离,检查施工过程中是否存在隐患;确认无任何问题后,找出保温棉介入的最佳位置,将硅酸铝保温棉小心地包覆在原有管道上,每隔 50cm 用铁丝绑扎固定,确保保温棉完全覆盖原有管道。

3 应用效果

(1)此方案在不影响光缆畅通的情况下,加装硅酸铝保温棉, 达到了保护管道免于火灾事故的效果,大大减少了光缆中断故障的发生。

(2)该方法最大的创新点在于,加装保温棉的过程不中断和影响在用业务,且硅酸铝材质阻燃隔热性能极佳,材质寿命长,使用更耐久。

(3)硅酸铝保温棉价格适中,如果使其量产化,价格还会下降,性价较高。

2011 年 1 月 15 日,青岛移动公司传输中心组织人员进行了一次通信管道阻燃、隔热试验,结果良好。在温度高达 400℃-800℃ 的火焰中经过 1 小时 30 分的测试,灭火后测量出硅酸铝保温层表内部温度仅为 60℃,而受保护的光缆表面温度更是仅有 18-19℃,阻燃隔热效果极佳。所以,维护人员于 1 月 16 日对青岛市李沧区黑龙江路(原 308 国道)一涵洞过桥光缆进行了防火保护;10 月底前,完成了对市区和县公司过桥、过涵洞及存在火灾安全隐患的移动光缆的改造工作,大大提高了青岛地区光传输网络的安全性,使网络质量达到了更高水平。

《山东通信技术》2011 年总目次

技术研究与应用

技术交流

管理经纬

业界观察

专　　稿